LANDTAG RHEINLAND-PFALZ
13. Wahlperiode

Drucksache 13/4836
18. 10. 1999

U n t e r r i c h t u n g

durch den Landesbeauftragten für den Datenschutz

Siebzehnter Tätigkeitsbericht nach § 29 Abs. 2 Landesdatenschutzgesetz – LDSG – für die Zeit vom 1. Oktober 1997 bis 30. September 1999

I n h a l t s v e r z e i c h n i s

		Seite
1.	**Vorbemerkung**	17
1.1	Zum Charakter des Tätigkeitsberichts	17
1.2	Fünfundzwanzig Jahre Datenschutz in Rheinland-Pfalz – ein Rückblick	17
1.3	Zur aktuellen Situation des Datenschutzes und des Datenschutzrechts	19
2.	**Zur Novellierung des Bundesdatenschutzgesetzes**	20
3.	**Datenschutz in Europa**	21
3.1	Nachholbedarf bei der Umsetzung der EG-Datenschutzrichtlinie	21
3.2	Die unmittelbare Wirkung der EG-Datenschutzrichtlinie vom 24. Oktober 1995	21
3.3	Novellierungsbedarf des LDSG aufgrund der Vorgaben der EG-Datenschutzrichtlinie	22
3.4	Vereinbarung zum Datenschutz zwischen der Europäischen Union und den Vereinigten Staaten in Sicht	23
3.5	Datenschutz innerhalb der Gemeinschaftsorgane und -einrichtungen	23
3.6	Zugang der Öffentlichkeit zu staatlichen Informationen	23
3.7	Entwurf einer Ratsentschließung zur Überwachung der Telekommunikation vorerst gestoppt	25
4.	**Meldewesen**	25
4.1	EWOISneu	25
4.1.1	Gesetzliche Grundlagen von EWOIS und Folgerungen für EWOISneu	26
4.1.2	Löschung und Aufbewahrung von Daten	26
4.1.3	Meldedatensatz	27
4.1.4	Auskunftssperren	27
4.2	Erklärung über steuerliches Getrenntleben	27
4.3	Vorsicht bei Müllgebühren	27
4.4	Meldescheine von Beherbergungsstätten	28
4.5	Übermittlung von Meldedaten an politische Parteien	28
4.5.1	Nutzung des Melderegisters für Zwecke der persönlichen Ansprache von EU-Ausländerinnen und -Ausländern	28
4.5.2	Beschränkung der Auskunft auf bestimmte Altersgruppen	29
4.5.3	Widerspruchs- oder Einwilligungslösung?	29
4.6	Erteilung von Melderegisterauskünften duch die Wegzugsbehörde	29
4.7	Meldedaten von Transsexuellen	30
4.8	Auskunftssperre nur für Volljährige?	30
4.9	Alters- und Ehejubiläen	30
4.10	Namensverwechslungen	30

Dem Präsidenten des Landtags mit Schreiben vom 18. Oktober 1999 zugleitet. Der Bericht wurde in der Sitzung der Kommission beim Landesbeauftragten für den Datenschutz am 28. September 1999 nach § 26 Abs. 3 Satz 4 LDSG vorberaten.

Druck: Landtag Rheinland-Pfalz, 3. Dezember 1999

Seite

5. Polizei ... 31
5.1 Allgemeine Tendenzen im Sicherheitsbereich ... 31
5.2 Überprüfungen bei der Polizei ... 31
5.3 Datenschutzrechtliche Schwerpunkte bei der automatisierten polizeilichen Datenverarbeitung ... 32
5.4 Überprüfung von POLIS/INPOL-Speicherungen ... 32
5.5 Internet-Fahndung durch die Polizei des Landes ... 33
5.6 Presse- und Öffentlichkeitsarbeit bei der Polizei ... 33
5.7 Ergänzung des Polizei- und Ordnungsbehördengesetzes; verdachtsunabhängige Personenkontrolle ... 33
5.8 Polizeiliche Datenverarbeitung auf europäischer Ebene; Europol ... 34
5.9 Einsichtnahme in das Pass- und Personalausweisregister ... 34
5.10 Wie privat ist ein „Privates Fach“? ... 35
5.11 Zusammenarbeit zwischen Bundeswehr, Polizei und anderen Behörden der Gefahrenabwehr ... 35
5.12 Zentrale Datei zur Erfassung von Verdachtsanzeigen nach dem Geldwäschegesetz ... 35
5.13 Zusammenarbeit von Staatsanwaltschaft und Polizei bei der Bekämpfung der Geldwäsche ... 36
5.14 Datei „Ringalarmfahndung“ ... 36
5.15 Vorsätzliche Verstöße gegen Datenschutzvorschriften durch Polizeibedienstete ... 37

6. Verfassungsschutz ... 38
6.1 Novellierung des Landesverfassungsschutzgesetzes ... 38
6.2 Befugnisse des LfD im Bereich von Abhörmaßnahmen nach dem G-10-Gesetz ... 38
6.3 Landessicherheitsüberprüfungsgesetz ... 39
6.4 Scientology und Verfassungsschutz ... 39
6.5 Erfassung einfacher Mitglieder von extremistischen Personenzusammenschlüssen durch die Verfassungsschutzbehörden ... 39 / 40
6.6 Örtliche Feststellungen im Bereich des Verfassungsschutzes ... 40

7. Justiz ... 40
7.1 Grundsätzliches zum Verhältnis Datenschutz und Justiz ... 40
7.2 Gesetzgebung im Justizbereich ... 41
7.3 Telefonüberwachungsmaßnahmen – neue Techniken, alte Probleme ... 41
7.4 Parlamentarische Kontrolle von Lauschangriffen in den Bundesländern ... 41
7.5 DNA-Analyse in Strafverfahren ... 42
7.6 Täter-Opfer-Ausgleich und Datenschutz ... 44
7.7 Anspruch eines Geschädigten auf die Bekanntgabe der Berufs-Haftpflichtversicherung eines Rechtsanwaltes durch die Rechtsanwaltskammer ... 45
7.8 Die datenschutzrechtlichen Ergänzungen des Strafvollzugsgesetzes ... 45
7.8.1 Defizite des Gesetzes aus datenschutzrechtlicher Sicht ... 46
7.8.2 Folgerungen für den LfD ... 46
7.9 Eingaben von Strafgefangenen ... 46

8. Schulen, Hochschulen, Wissenschaft ... 47
8.1 Schulen ... 47
8.1.1 Elternbefragung zur Errichtung einer Regionalen Schule ... 47
8.1.2 Zahngesundheitspflege in der Grundschule ... 47
8.1.3 Antragsverfahren für Lernmittelgutscheine ... 48
8.1.4 Was darf in die Schülerakte? ... 48
8.1.5 Diagnoseangaben auf Entschuldigungsschreiben ... 49
8.1.6 Schülerausweise ... 49
8.1.7 Präsentation von Klassenfotos und personenbezogenen Daten im Internet ... 50
8.1.8 Videoaufzeichnung des Unterrichts ... 50
8.2 Hochschulen ... 51
8.2.1 Gesetz zur Änderung des Verwaltungsfachhochschulgesetzes und des Landesgesetzes über die Zentrale Verwaltungsschule Rheinland-Pfalz ... 51
8.3 Wissenschaft ... 51
8.3.1 Krebsregister ... 51
8.3.2 Allgemeines zu Forschungsvorhaben im Schulbereich ... 52
8.3.3 PISA-Studie ... 52
8.3.4 Civic Education-Studie ... 53
8.3.5 Befragung von Schulkindern zur Lebensqualität ... 53
8.3.6 Multikulturelle Gesellschaft, Ernährung, Fitness, Aussehen – eine Frage der Einstellung? ... 53
8.3.7 Fremdenfeindlichkeit, Antisemitismus und Rechtsextremismus und deren Hintergründe ... 53

Seite

8.3.8 Erhebung zur Jugendhilfeplanung . . . 54
8.3.9 Katamnese-Studie zum rheinland-pfälzischen Maßregelvollzug . . . 55
8.3.10 Evaluation von Erhebungs- und Messmethoden . . . 55
8.3.11 Was macht die rheinland-pfälzische Elite? . . . 56
8.3.12 Befragung zu Karriereverläufen und Mobilitätsprozessen von Wissenschaftlern . . . 56
8.3.13 Absolventenbefragung . . . 56
8.4 jugendschutz.net . . . 56

9. Umwelt . . . 57
9.1 Einzelfragen zum Umweltinformationsgesetz . . . 57
9.2 Die Århus-Konvention: Erweiterung des Informationszugangs im Bereich der Umwelt . . . 58
9.3 Fragebogen zur Freistellung von der Überlassungspflicht für Bioabfälle . . . 58

10. Gesundheitswesen . . . 59
10.1 Neuordnung des öffentlichen Gesundheitsdienstes . . . 59
10.1.1 Arztpost auf dem Schreibtisch des Landrats . . . 59
10.1.2 Online-Zugriff eines Landrates auf die medizinischen Daten des Gesundheitsamtes . . . 60
10.1.3 Eingliederung des Sozialpsychiatrischen Dienstes in das Gesundheitsamt . . . 60
10.2 Warnmeldungen der Gesundheitsämter . . . 60
10.3 Tonbandaufzeichnungen bei Prüfungsgesprächen . . . 61
10.4 Neufassung der Berufsordnung für Ärzte in Rheinland-Pfalz . . . 61
10.5 Vernichtung von ärztlichen Unterlagen . . . 61
10.6 Besuchskommission nach § 29 PsychKG; Berichterstattung an den Stadtrat oder Kreistag . . . 62
10.7 Sanitätsdienst in Justizvollzugsanstalten . . . 63
10.8 Datenschutz im Krankenhaus . . . 64
10.8.1 Zugriff des Landesrechnungshofs auf Patientendaten . . . 64
10.8.2 Informationen zum Datenschutz; Heft 4 – Datenschutz im Krankenhaus . . . 64
10.9 Patientenchipkarten; Modellversuch Neuwied/Rhein . . . 65

11. Sozialdatenschutz . . . 65
11.1 Gesetzliche Änderungen im Sozialgesetzbuch . . . 65
11.1.1 Gesundheitsreform 2000 . . . 65
11.1.2 Änderung des § 68 SGB X durch das Medizinproduktegesetz . . . 65
11.2 Sozialhilfe . . . 66
11.2.1 Was lange währt, ... 66
11.2.2 Übermittlung von Sozialdaten an die Staatsanwaltschaft . . . 67
11.2.3 Fragebogen zum Vorliegen einer nichtehelichen Lebensgemeinschaft . . . 67
11.2.4 Arbeitsunfähigkeitsbescheinigung bei der Verrichtung gemeinnütziger Arbeit . . . 68
11.2.5 Die Einholung von Bankauskünften im Sozialleistungsverfahren . . . 68
11.2.6 Missbrauchskontrolle bei der Gewährung von Sozialhilfe . . . 69
11.2.6.1 Der Datenabgleich nach § 117 Abs. 1 bis 2 a BSHG . . . 69
11.2.6.2 Sozialhilfedatenabgleich nach § 117 Abs. 3 BSHG mit der Kfz-Zulassungsstelle . . . 69
11.2.6.3 Sozialhilfeermittler . . . 70
11.2.7 Rechnungsprüfung und Begleichung ambulanter und stationärer Krankenhilfeaufwendungen . . . 71
11.2.8 Datenübermittlung im Rahmen der Kostenerstattung bei Umzug (§ 107 BSHG) . . . 71
11.3 Jugendhilfe . . . 72
11.3.1 Rechnungsprüfung im Jugendamt . . . 72
11.3.2 Einkommensabhängige Erhebung von Elternbeiträgen für Kindertagesstätten . . . 72
11.4 Wohngeld . . . 73
11.4.1 Unaufgeforderte Datenübermittlung der Wohngeldstelle an das Sozialamt . . . 73
11.4.2 Landesweiter Datenabgleich im Wohngeldverfahren . . . 73
11.5 Krankenkassen, Kassenärztliche Vereinigungen . . . 74
11.5.1 Eingeschränkter Zugriff auf Versichertendaten bei landesweiten oder überregionalen gesetzlichen Krankenkassen . . . 74
11.5.2 Anforderung von Behandlungsunterlagen durch Krankenkassen . . . 74
11.5.3 Auskünfte an Versicherte . . . 75
11.5.4 Briefzustellung durch Privatunternehmen . . . 75
11.5.5 Datenschutzprobleme bei der Umsetzung des Psychotherapeutengesetzes . . . 76
11.6 Dialogverfahren der Rentenversicherungsträger . . . 76
11.7 Datenerhebung und -verwendung bei der Kontrolle von Heimen . . . 77

Seite

12. Datenschutz im Ausländerwesen ... 78
12.1 Einführung von Asyl-Cards ... 78
12.2 Ausschreibungen zur Einreiseverweigerung im Schengener Informationssystem ... 78
12.3 Verpflichtungserklärung vor Visum an ausländischen Gast ... 79

13. Finanzverwaltung ... 79
13.1 Outsourcing in der Steuerverwaltung – Versand von Steuervordrucken durch Private ... 79
13.2 Arzt und Fahrtenbuch oder der Patient als Geschäftspartner ... 79
13.3 Bekämpfung der Korruption in der öffentlichen Verwaltung ... 80

14. Wirtschaft und Verkehr ... 80
14.1 Grundsätzliches zur Auskunftserteilung über Gewerbeanzeigen ... 80
14.2 Zugriffe auf den Datenbestand des Gewerbeamtes ... 80
14.3 Weitergabe von Gewerbedaten an den Ausländerbeirat ... 81
14.4 Weitergabe aller Firmendaten an einen Online-Dienst ... 81
14.5 Datenerhebung bei Stundungen ... 82
14.6 Privatisierung von Tätigkeitsbereichen ... 82
14.7 Datenschutzrechtliche Aspekte bei der Beteiligung Privater an der kommunalen Geschwindigkeitsüberwachung ... 84
14.8 Künftig Kraftfahrzeugzulassung über das Internet? ... 85
14.9 Halteranfragen von Privaten ... 86
14.10 Erteilung der Betriebserlaubnis und Ausstellung eines neuen Fahrzeugscheins durch den TÜV bei Änderungen an Fahrzeugen – Modellversuch in ausgewählten Zulassungsbezirken ... 86
14.11 Tilgung von Datenspeicherungen in Führerscheinakten ... 87
14.12 Gesetz zur Änderung des Straßenverkehrsgesetzes und anderer Gesetze ... 87
14.13 Die Fahrerlaubnis-Verordnung und das Problem mit den Führerscheinakten ... 88

15. Landwirtschaft, Weinbau und Forsten ... 88
15.1 Datei der Rindfleischerzeuger zur Bekämpfung von BSE ... 88
15.2 Datenverarbeitung zum Zweck der Bodenkunde und des Bodenschutzes ... 89
15.3 Behördliche Auskünfte und Akteneinsichtsrechte im Zusammenhang mit der Einräumung eines Wasserrechts ... 89

16. Statistik ... 90
16.1 Alle Jahre wieder – Fragen zur „Kleinen Volkszählung“ (Mikrozensus) ... 90
16.2 Volkszählung light? ... 90
16.3 Die Volkszählung und das Melderegister ... 91

17. Personaldatenverarbeitung ... 91
17.1 Mitteilung von Gehaltspfändungen durch die Zentrale Besoldungs- und Versorgungsstelle an die personalverwaltende Stelle ... 91
17.2 Gewinnung von Wahlhelfern ... 92
17.3 Telearbeit ... 92

18. Datenschutz im kommunalen Bereich ... 93
18.1 Bürgerbüros und informationelle Gewaltenteilung ... 93
18.2 Wahrung des Wahlgeheimnisses bei der Briefwahl ... 94
18.3 Datenschutz und Volksbegehren ... 94
18.4 Ausübung des Vorkaufsrechts ... 95
18.5 Das illegale Wochenendhaus ... 95
18.6 „Den Widerstand aufgeben“; das Datenschutzverständnis eines Kommunalpolitikers ... 96
18.7 Nebentätigkeiten, Wahrnehmung von öffentlichen Ehrenämtern, ehrenamtliche und sonstige Tätigkeiten ... 96
18.8 Verwendung einer Videokamera für Überwachungszwecke ... 97
18.9 Personenstandswesen ... 97
18.9.1 Datenschutz und Familienforschung ... 97
18.9.2 Zwangsvollstreckung gegen Transsexuelle ... 98
18.10 Übersendung von Gräberlisten an die Landeszentrale für politische Bildung ... 98

19. Telekommunikation ... 98
19.1 Schutzgut Fernmeldegeheimnis ... 98
19.1.1 Die gesetzliche Absicherung des Fernmeldegeheimnisses ... 99

Seite

19.1.2 Private Vorsorge zum Schutz des Fernmeldegeheimnisses . . . 99
19.1.3 Gesetzliche Reglementierung des Einsatzes von Verschlüsselungsverfahren? . . . 100
19.2 Entwurf einer neuen Telekommunikations-Datenschutzverordnung . . . 101
19.3 Eckpunktepapier zur Telekommunikations-Überwachungsverordnung . . . 101
19.4 Auswirkungen des Telekommunikationsrechts im Krankenhausbereich . . . 102
19.5 Fehlleitungen bei Telefax . . . 102

20. Medien . . . 103
20.1 Der Datenschutz beim Internet-Zugang in öffentlichen Stellen . . . 103
20.1.1 Vermittlung des Internet-Zugangs an Bedienstete für dienstliche Zwecke . . . 103
20.1.2 Private Nutzung des Internet-Zugangs . . . 103
20.1.3 Elektronische Post . . . 103
20.2 Anwendung des Medienrechts . . . 104
20.3 Vierter Rundfunkänderungsstaatsvertrag . . . 104
20.4 Rundfunkrechtliche Überwachungskompetenz des LfD . . . 105
20.5 Evaluierung des Informations- und Kommunikationsdienste-Gesetzes . . . 105
20.6 Schlussbericht der Enquete-Kommission „Zukunft der Medien in Wirtschaft und Verwaltung“ . . . 106
20.7 Einigung auf EG-Signaturrichtlinie . . . 106

21. Technischer und organisatorischer Datenschutz . . . 107
21.1 Kontroll- und Beratungstätigkeit . . . 107
21.2 Technisch-organisatorische Datenschutzfragen in ausgewählten Verfahren . . . 107
21.2.1 Internet-Firewall LDKN . . . 107
21.2.2 Verschlüsselung auf dem ATM-Backbone des LDKN . . . 108
21.2.3 Zugangskontrolle der Knotenrechner des LDKN . . . 109
21.2.4 X.500-Verzeichnisdienst der Landesverwaltung . . . 110
21.2.5 Elektronische Steuererklärung (ELSTER) . . . 110
21.2.6 Internet-Angebot der Polizei Rheinland-Pfalz . . . 111
21.2.7 Stimmenauszählungsprogramme bei der Kommunalwahl 1999 . . . 112
21.2.8 Overlay-Netz der Verwaltungen des Bundes und der Länder (TESTA) . . . 112
21.2.9 Vorgangsbearbeitungs- und -verwaltungssystem der Polizei (POLADIS-Neu) . . . 113
21.2.9.1 Risikoanalyse und Sicherheitskonzept . . . 113
21.2.9.2 Rollenkonzept und Zugriffskontrolle . . . 114
21.2.9.3 Löschkonzept . . . 114
21.2.9.4 Protokollierungskonzept . . . 114
21.2.10 Elektronische Verarbeitung von Arbeitszeit, Abwesenheit und Mehrarbeit bei der Polizei (EVA) . . . 115
21.2.11 Überwachung der Telekommunikation mit dem System ATIS/MCMR . . . 115
21.2.11.1 Sicherung von Integrität durch kryptografische Maßnahmen . . . 115
21.2.11.2 Aufzeichnung von Verteidigertelefonaten . . . 116
21.2.11.3 Verschlüsselung bei der Bereitstellung über öffentliche Übertragungswege . . . 116
21.2.11.4 Protokollierung der Erstellung von Ausdrucken . . . 116
21.2.12 Einbindung der Gesundheitsämter in die IT-Struktur der Kreisverwaltungen . . . 116
21.2.13 Zugriffsberechtigung im Vertretungsfall im Verfahren Finanzamt 2000 . . . 117
21.2.14 Sicherstellung der Zweckbindung bei der Verarbeitung personenbezogener Daten durch Krankenkassen . . . 117
21.2.14.1 Einsatz freier Abfragesprachen . . . 118
21.2.14.2 Kassenübergreifende Konzentration der DV-Produktion . . . 118
21.2.14.3 Zugriffsbefugnisse auf Versichertendaten . . . 119
21.2.14.4 Archivierung und Löschung von Versichertendaten . . . 119
21.2.14.5 Protokollierung von Abfragen und Auswertungen . . . 120
21.2.15 Verteilung personenbezogener Budgetierungsdaten in den Geschäftsbereichen der Ressorts . . . 120
21.2.16 Dezentrale Datenerfassung bei den Ämtern für Ausbildungsförderung . . . 120
21.2.16.1 Datenerfassung und Übermittlung durch die Ausbildungsförderungsämter auf Kreisebene (Verfahren BAFER) . . . 121
21.2.16.2 Datenerfassung und Übermittlung durch die Ausbildungsförderungsämter der Hochschulen . . . 121
21.2.17 Behandlung defekter Festplatten im Bereich der Polizei . . . 121
21.3 Allgemeine technisch-organisatorische Aspekte . . . 121
21.3.1 Wählleitungsverbindungen bei an das LDKN angeschlossenen Verwaltungen . . . 122
21.3.2 Einsatz von Faxkarten und Faxservern . . . 122
21.3.3 Einrichtung von ISDN-Wählleitungsverbindungen . . . 123
21.3.4 Fernwartung durch nichtöffentliche Stellen . . . 124

Seite

21.3.5 Gestaltung von Internet-Zugängen und-Angeboten . . . 125
21.3.6 Gestaltung von Schulverwaltungsprogrammen . . . 125
21.3.7 Protokollierung der Internet-Nutzung . . . 126
21.3.8 Löschen und Vernichten von Datenträgern . . . 127
21.3.9 Raum- und Gebäudesicherung . . . 127
21.3.9.1 Anforderungen an die Absicherung von Räumen und Gebäuden . . . 127
21.3.9.2 Empfehlungen des Gemeindeversicherungsverbandes zur Schadensminderung bei Einbrüchen . . . 128
21.3.10 Empfehlungen zum Einsatz von Verschlüsselungsverfahren . . . 129
21.3.11 E-Mail in der Verwaltung . . . 129
21.4 Entwicklung des Datenschutzregisters . . . 130

22. Datenverarbeitung bei Sparkassen . . . 130
22.1 SIS West . . . 130
22.2 Datenübermittlung durch eine Sparkasse an das Arbeitsamt . . . 130
22.3 Datenübermittlung durch eine Sparkasse an den Schlichter des Sparkassen- und Giroverbandes . . . 130
22.4 Personalausweiskopie als Voraussetzung einer Vollmachtserteilung . . . 131
22.5 Schufa-Anfragen durch öffentliche Stellen . . . 131

23. Sonstiges . . . 132
23.1 Das nachkartende Katasteramt . . . 132
23.2 Einsichtnahme in Bauakten durch Dritte . . . 132

24. Schlussbemerkung . . . 133
24.1 Zur Situation der Geschäftsstelle . . . 133
24.2 Veröffentlichungen der Dienststelle . . . 133
24.3 Zusammenarbeit mit anderen Datenschutzinstitutionen . . . 134
24.4 Resümee und Ausblick . . . 134

Anlagenübersicht (Anlage 1 bis Anlage 24) . . . 7

Abkürzungen . . . 8
Glossar technischer Begriffe . . . 10

Anlagen

		Seite
1	Entschließung „Novellierung des Bundesdatenschutzgesetzes und Modernisierung des Datenschutzrechts“	136
2	Entschließung „Informationelle Selbstbestimmung und Bild-Ton-Aufzeichnungen bei Vernehmungen im Strafverfahren“	138
3	Entschließung „Erforderlichkeit datenschutzfreundlicher Technologien“	139
4	Entschließung „Datenschutz beim digitalen Fernsehen“	140
5	Entschließung „Datenschutzprobleme der Geldkarte“	141
6	Entschließung „Fehlende bereichsspezifische Regelungen bei der Justiz“	142
7	Entschließung „Dringlichkeit der Datenschutzmodernisierung“	143
8	Entschließung „Entwicklungen im Sicherheitsbereich“	143
9	Entschließung „Weitergabe von Meldedaten an Adressbuchverlage und Parteien“	144
10	Entschließung „Prüfungskompetenz der Datenschutzbeauftragten bei den Gerichten“	144
11	Entschließung „Verweigerung der Auskunft durch das Bundesamt für Finanzen auf Anfragen Betroffener über ihre Freistellungsaufträge“	145
12	Entschließung „Modernisierung des Datenschutzes – umfassende Novellierung des BDSG nicht aufschieben“	145
13	Entschließung „Erweiterte Speicherung von Verbindungsdaten in der Telekommunikation“	146
14	Entschließung „Transparente Hard- und Software“	147
15	Entschließung „Entwurf einer Ratsentschließung zur Überwachung der Telekommunikation (ENFOPOL ’98)“	147
16	Entschließung „Parlamentarische Kontrolle von Lauschangriffen in den Bundesländern“	148
17	Entschließung „Angemessener Datenschutz auch für Untersuchungsgefangene“	149
18	Entschließung „Gesundheitsreform 2000“	150
19	Schreiben der Konferenz der Datenschutzbeauftragten des Bundes und der Länder an den Vorsitzenden der Innenministerkonferenz (Molekulargenetische Untersuchung von Körperzellen)	151
20	Orientierungshilfe „Datenschutz und Telefax“	152
21	Orientierungshilfe „Hinweise zur datenschutzgerechten Gestaltung und Nutzung von E-Mail-Diensten durch öffentliche Stellen“	156
22	Orientierungshilfe „Gestaltung Internet-Angebote“	160
23	Orientierungshilfe der Datenschutzbeauftragten des Bundes und der Länder zum Anschluss öffentlicher Stellen an das Internet	166
24	Entwicklung der Anmeldungen zum Datenschutzregister	166

Abkürzungen

a. a. O.	am angegebenen Ort
ABl.	Amtsblatt
AO	Abgabenordnung
AOK	Allgemeine Ortskrankenkasse
AsylbLG	Asylbewerberleistungsgesetz
AWG	Außenwirtschaftsgesetz
BauGB	Baugesetzbuch
BDSG	Bundesdatenschutzgesetz
BfD	Bundesbeauftragter für den Datenschutz
BFH	Bundesfinanzhof
BGB	Bürgerliches Gesetzbuch
BGBl.	Bundesgesetzblatt
BGH	Bundesgerichtshof
BImSchG	Bundes-Immissionsschutzgesetz
BKA	Bundeskriminalamt
BKAG	Bundeskriminalamtgesetz
BSHG	Bundessozialhilfegesetz
BVerwG	Bundesverwaltungsgericht
BVG	Bundesversorgungsgesetz
BVerfGE	Sammlung der Entscheidungen des Bundesverfassungsgerichts
BZRG	Bundeszentralregistergesetz
DATEV	Datenverarbeitung und Dienstleistung für den steuerberatenden Beruf
DIZ	Daten- und Informationszentrum Rheinland-Pfalz
DNA	Desoxyribonuclein acid (acid = Säure)
DNA-IFG	DNA-Identitätsfeststellungsgesetz
Drs.	Drucksache
DSK	Datenschutzkommission
e. G.	eingetragene Genossenschaft
EG	Europäische Gemeinschaften
EGV	Vertrag über die Europäische Gemeinschaft
EStG	Einkommensteuergesetz
EU	Europäische Union
EuGH	Europäischer Gerichtshof
EUROPOL	Zentrales Europäisches Kriminalpolizeiamt
EWOIS	Einwohnerinformationssystem
FeV	Fahrerlaubnis-Verordnung
ff.	(fort-)folgende
FGG	Gesetz über die Angelegenheiten der freiwilligen Gerichtsbarkeit
FÜV	Fernmeldeüberwachungsverordnung
G 10	Gesetz zu Artikel 10 GG
GemO	Gemeindeordnung
GewO	Gewerbeordnung
GG	Grundgesetz
ggf.	gegebenenfalls
GOLT	Geschäftsordnung des Landtags
GVBl.	Gesetz- und Verordnungsblatt
GwG	Geldwäschegesetz
HeilBG	Heilberufsgesetz
HessVGH	Hessischer Verwaltungsgerichtshof
HGB	Handelsgesetzbuch
HLU	Hilfe zum Lebensunterhalt
IHK	Industrie- und Handelskammer
INPOL	Polizeiliches Informationssystem des Bundes und der Länder beim Bundeskriminalamt
i. S. v.	im Sinne von
IuKDG	Informations- und Kommunikationsdienste-Gesetz
i. V. m.	in Verbindung mit
JVA	Justizvollzugsanstalt
KAG	Kommunalabgabengesetz
KAN	Kriminalaktennachweis
KBA	Kraftfahrtbundesamt
KpS	Kriminalpolizeiliche personenbezogene Sammlungen – Kriminalakten –
KrW-/AbfG	Kreislaufwirtschafts- und Abfallgesetz
KV	Kassenärztliche Vereinigung
KWO	Kommunalwahlordnung
LAbfWAG	Landesabfallwirtschafts- und Altlastengesetz
LAG	Lastenausgleichsgesetz
LBG	Landesbeamtengesetz
LDatG	Landesdatenschutzgesetz vom 21. Dezember 1978
LDKN	Landesdaten- und Kommunikationsnetz Rheinland-Pfalz
LDSG	Landesdatenschutzgesetz
LfD	Landesbeauftragter für den Datenschutz
LHO	Landeshaushaltsordnung
lit.	littera (Buchstabe)
LKA	Landeskriminalamt
LRG	Landesrundfunkgesetz
LSG	Landessozialgericht
LV	Landesverfassung für Rheinland-Pfalz
LVA	Landesversicherungsanstalt
LVO	Landesverordnung
LWO	Landeswahlordnung
MDK	Medizinischer Dienst der Krankenversicherung
MDStV	Mediendienste-Staatsvertrag
MedR	Medizinrecht
MeldDÜVO	Meldedatenübermittlungsverordnung
MG	Meldegesetz
1. MPG-ÄndG	Erstes Gesetz zur Änderung des Medizinproduktegesetzes
MRRG	Melderechtsrahmengesetz
MVO	Meldeverordnung
NJW	Neue Juristische Wochenschrift
OFD	Oberfinanzdirektion
ÖGdG	Gesetz über den öffentlichen Gesundheitsdienst
OLG	Oberlandesgericht
OVG	Oberverwaltungsgericht
PC	Personalcomputer
POG	Polizei- und Ordnungsbehördengesetz

POLIS	Polizeiliches Informationssystem Rheinland-Pfalz
PStG	Personenstandsgesetz
PsychKG	Landesgesetz über psychisch kranke Personen
RdNr.	Randnummer
RDV	Recht der Datenverarbeitung
SchulG	Schulgesetz
SDÜ	Schengener Durchführungsübereinkommen
SGB I	Sozialgesetzbuch – Erstes Buch –
SGB III	Sozialgesetzbuch – Drittes 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
StVollzG	Strafvollzugsgesetz
StVZO	Straßenverkehrs-Zulassungsordnung
Tb.	Tätigkeitsbericht
TDDSG	Teledienstedatenschutzgesetz
TDG	Teledienstegesetz
TDSV	Telekommunikationsdienstunternehmen-Datenschutzverordnung
TKG	Telekommunikationsgesetz
TKÜV	Telekommunikations-Überwachungsverordnung (Entwurf)
TSG	Transsexuellengesetz
TÜ	Telefonüberwachung
Tz.	Textziffer
u. a.	unter anderem
UIG	Umweltinformationsgesetz
u. U.	unter Umständen
VGH	Verwaltungsgerichtshof
VS-nfD	Verschlusssache nur für den Dienstgebrauch
VV	Verwaltungsvorschrift
VwVfG	Verwaltungsverfahrensgesetz
ZEVIS	Zentrales Verkehrsinformations-System
ZBV	Zentrale Besoldungs- und Versorgungsstelle
ZPO	Zivilprozessordnung

Glossar technischer Begriffe

ActiveX	Eine Software-Technologie von Microsoft. ActiveX erlaubt es, so genannte Applets zu erstellen, die vom Server auf den Rechner des Internet-Nutzers übertragen und dort ausgeführt werden. Die Applets können dabei grundsätzlich auf alle Ressourcen des Zielrechners zugreifen, d. h. gegebenenfalls Daten lesen, löschen oder verändern.
Algorithmus	Beschreibung einer Verfahrensweise zur Lösung eines (mathematischen) Problems. Im Zusammenhang mit der *kryptografischen Verschlüsselung* steht der Begriff für die Art und Weise, in der ein Klartext in ein *Chiffrat* umgewandelt wird und umgekehrt. Bekannte Algorithmen sind *DES, RSA* oder *IDEA*.
Asymmetrische Verschlüsselung	Kryptografisches Verfahren, bei dem zwei Schlüssel, ein öffentlicher und ein *geheimer Schlüssel*, verwendet werden. Der öffentliche Schlüssel ist jedem zugänglich, der geheime nur dem jeweiligen Empfänger einer Nachricht. Die Verschlüsselung folgt dabei folgendem Konzept: Wird mit dem *öffentlichen Schlüssel* des Empfängers verschlüsselt, kann die Nachricht nur mit dem geheimen Schlüssel des Empfängers entschlüsselt werden. Mit umgekehrter Verwendung der Schlüssel lässt sich die digitale Signatur realisieren. Wird dabei mit dem geheimen Schlüssel des Absenders signiert, kann die Signatur anhand des öffentlichen Schlüssels des Absenders überprüft werden. Beispiele für asymmetrische Verfahren sind *RSA* und *DSS.*
ATM	Asynchronous Transfer Mode. Ein Kommunikationsprotokoll aus dem Bereich der Netzwerktechnik, d. h. eine Festlegung, in welcher Weise Daten über eine physikalische Leitung übertragen werden.
Attachment	Anhang zu einer *E-Mail*. Ein Attachment kann aus jeglicher Art von Daten bestehen, z. B. Dokumenten, Programmen, Bildern, Grafiken, Video- oder Audiodaten.
Authentisierung	Formeller Nachweis der Berechtigung zur Benutzung eines IT-Systems oder von dessen Ressourcen. Die Authentisierung erfolgt in Verbindung mit der *Identifikation* zumeist im Rahmen der Anmeldung an einem IT-System. Die Eingabe eines gültigen Passwortes ist ein Beispiel für eine Authentisierung.
Authentizität	Verlässliche Zurechenbarkeit einer elektronischen Nachricht zu einem bestimmten Absender.
Backbone	Bezeichnung für den Hauptstrang eines Netzwerks, über den der gesamte Datenverkehr zwischen den zentralen *Knotenrechnern* eines Netzes abgewickelt wird. Der Backbone stellt im Allgemeinen die höchsten Übertragungsraten innerhalb eines Netzes zur Verfügung.
Browser	Programm auf dem Rechner des Benutzers zur Darstellung von Web-Seiten, d. h. von Inhalten im Internet. Gängige Browser sind der Micosoft Internet Explorer und der Netscape Navigator.
Callback	Automatischer Rückruf. Verfahren bei *Wählleitungsverbindungen*, bei welchem ein angewählter Rechner den Verbindungswunsch registriert, die Verbindung abbricht und in umgekehrter Richtung erneut aufbaut. In Verbindung mit Rufnummernlisten kann damit erreicht werden, dass eine Verbindung nur zu einem bestimmten Anschluss hergestellt wird.
CERT-Advisories	Sicherheitshinweise der Computer Emergency Rescue Teams, einer Sicherheitsorganisation für das Internet. Ein deutschsprachiges CERT existiert für das Deutsche Forschungsnetz (DFN) unter der Internet-Adresse www.cert.dfn.de.
CHAP	Challenge Authentication Protocol. Automatisches Verfahren zur *Authentisierung*, bei welchem dem rufenden Anschluss eine binäre Zufallszahl (challenge) zur Verfügung gestellt wird. Diese wird mit einem vorgegebenen *Algorithmus* verarbeitet und das Ergebnis dem gerufenen Anschluss übermittelt. Entspricht das Zurückgelieferte dem erwarteten Ergebnis, wird die Verbindung hergestellt.

Chat	Eigentlich IRC – Internet Relay Chat. Bezeichnung eines Internet-Dienstes, der die Möglichkeit bietet, online zu diskutieren. Die Beiträge werden über die Tastatur eingegeben. Thematisch orientierte Chat-Foren eröffnen die Möglichkeit der Online-Diskussionen mit mehreren Teilnehmern gleichzeitig.
Chiffrat	Ergebnis einer *kryptografischen Verschlüsselung*, d. h. die mittels *Algorithmus* und Schlüssel verschlüsselten Daten.
Client	Begriff aus dem Netzwerkbereich: Ein Client nimmt von einem *Server* angebotene Dienste in Anspruch. Der Client schickt Anfragen an den Server und stellt dessen Antworten in lesbarer Weise auf dem Bildschirm dar. Als Clients werden sowohl Rechner, z. B. PC, als auch Prozesse, z. B. Programmfunktionen, bezeichnet.
Client/Server-Architektur	Modell einer Netzwerkstruktur oder eines Softwarekonzepts, bei der/bei dem eine hierarchische Aufgabenverteilung vorliegt. Der Server ist dabei der Anbieter von Ressourcen, Funktionen oder Daten – die Arbeitsstationen (Clients) nehmen diese in Anspruch.
CLIP	Calling Line Identification Protocol. Anzeige der Nummer des rufenden Anschlusses beim gerufenen Teilnehmer. Die über CLIP bereitgestellte Anschlussnummer kann für die Prüfung der Zugangsberechtigung genutzt werden.
CUG	Closed User Group (Geschlossene Benutzergruppe). Leistungsmerkmal von Kommunikationsdiensten, bei welchem die zugelassenen Anschlüsse in einer Berechtigungstabelle eingetragen werden. Kommunikationsanforderungen von in dieser Tabelle nicht enthaltenen Anschlüssen werden zurückgewiesen.
Denial of Service-Attacke	Angriff, bei welchem durch die Ausnutzung von Schwachstellen in Programmen, Protokollen oder Konfigurationen die Funktionsfähigkeit von Rechnern oder Serverdiensten beeinträchtigt wird. Eine Denial of Service-Attacke kann jedoch auch in der vorsätzlichen Überlastung von Diensten bestehen (vgl. *Spam-Mail*).
DES	Data Encryption Standard. Von IBM in den 70er Jahren entwickeltes symmetrisches Verschlüsselungsverfahren. Bei DES werden Datenblöcke zu je 64 Bits mit einem 56-Bit-Schlüssel codiert. DES ist weit verbreitet und wurde mit der Standardschlüssellänge bereits kompromittiert, d. h. innerhalb überschaubarer Zeit entschlüsselt. Höhere Sicherheit bietet Triple DES (DES 3), bei welchem mehrere Verschlüsselungsrunden aufeinander folgen.
DFÜ	Datenfernübertragung.
Dial-in	Auch Einwahl oder *Inbound* genannt. Vorgang, bei dem ein entfernter Anschluss eine Kommunikationsverbindung zum lokalen IT-System herstellt.
Dial-out	Auch *Outbound* genannt. Vorgang, bei dem eine Kommunikationsverbindung zu einem entfernten IT-System hergestellt wird.
Digitale Signatur	„Elektronische Unterschrift“. Verfahren, bei welchem durch die Verwendung *asymmetrischer Verschlüsselungsverfahren*, meist in Kombination mit *Hash-Verfahren*, die *Integrität* und *Authentizität* einer elektronischen Nachricht sichergestellt werden kann. Eine gesetzliche Sicherheitsvermutung besteht für Signaturverfahren nach dem Signaturgesetz.
D-Kanal-Filter	Programm zur Überwachung der Kommunikation auf dem Steuerungskanal des *ISDN*-Dienstes.
DNS	Domain Name Service. Internet-Dienst, der *IP-Adressen* in leichter zu merkende Rechnernamen umsetzt (z. B. 192.168.100.010 in www.firma.de).
DNS-Server	Rechner bzw. Programme, welche DNS-Dienste bereitstellen.
Download	Herunterladen von Daten aus dem Internet auf das eigene IT-System.

DSS	Digital Signature Standard. Ein kryptografisches Verfahren für die *digitale Signatur*.
E-Mail	Electronic Mail (Elektronische Post). E-Mail ermöglicht das Verschicken elektronischer Nachrichten. Diesen können Dokumente, Programme, Bilder, Grafiken, Video- oder Audiodaten in Form von *Attachments* beigefügt werden.
Ende-zu-Ende-Verschlüsselung	Verschlüsselung des Datenverkehrs zwischen den Kommunikationsteilnehmern. Die Ende-zu-Ende-Verschlüsselung erfolgt im Gegensatz zur *Leitungsverschlüsselung* auf der Anwendungsebene, d. h. bei der Nutzung von Programmen. So muss z. B. eine E-Mail-Nachricht als solche explizit verschlüsselt werden.
Fax-Server	Rechner oder Programme, die Faxdienste (Versand, Empfang) bereitstellen.
Firewall	„Brandmauer". Ein System in Form von Hard- und/oder Software, das den Datenfluss zwischen einem internen und einem externen Netzwerk kontrolliert bzw. ein internes Netz vor Angriffen von außerhalb, z. B. aus dem Internet, schützt.
Freie Abfragesprache	Programmiersprache, mit der beliebige Abfragen an Datenbanksysteme gerichtet werden können. Eine bekannte freie Abfragesprache ist die Standard Query Language.
Gateway	Ein Gateway ist ein Rechner am Übergang zwischen zwei Netzen, der die notwendige Umsetzung bei Verwendung unterschiedlicher *Protokolle* sicherstellt bzw. den Empfang und die Weiterleitung von Daten steuert.
Geheimer Schlüssel	siehe *Private Key.*
Geschlossene Benutzergruppe	siehe *CUG.*
Hash-Verfahren	Mathematisches Verfahren, mit dem ein (langes) elektronisches Dokument auf eine (kurze) Prüfsumme abgebildet wird. Änderungen am Dokument, auch geringste, führen bei erneutem „hashen" zu einer anderen Prüfsumme. Hashverfahren werden im Rahmen der *digitalen Signatur* für den Nachweis der Integrität einer Nachricht benötigt.
Hashwert	Prüfsumme als Ergebnis eines Hash-Vorgangs.
Homepage	Start- und Begrüßungsseite eines Internet-Angebotes. Von der Homepage gelangt man über Verweise (links) zu den weiteren Inhalten des Angebots.
HTML	Hypertext Markup Language. Eine Programmiersprache, in der *Web-Seiten* geschrieben werden. Der *Browser* ermöglicht die grafische Umsetzung der HTML-Befehle. Das Besondere an HTML sind die Einsetzbarkeit auf verschiedenen Systemen (Windows, Unix, Macintosh usw.) und die Verweise (hyperlinks) auf andere *Web-Seiten* auf dem lokalen System oder im Internet.
Hyperlink	siehe *HTML*. Verweis auf andere Web-Seiten auf dem lokalen System/Netzwerk oder andere Rechner im Internet.
IDEA	International Data Encryption Algorithm. Ein *symmetrisches Verschlüsselungsverfahren* mit einer Schlüssellänge von 64 bzw. 128 Bit.
Identifikation	Nachweis über die Identität eines Benutzers eines IT-Systems, z. B. anhand einer Benutzerkennung (User-ID). Die Identifikation erfolgt in Verbindung mit der *Authentisierung* zumeist im Rahmen der Anmeldung an einem IT-System.
Inbound	siehe *Dial-in*.
Integrität	Unversehrtheit und Vollständigkeit der in elektronischer Form gespeicherten oder übermittelten Daten. Der Nachweis der Integrität einer elektronischen Nachricht, z. B. mittels *Hash-Verfahren*, stellt sicher, dass diese während der Übertragung nicht verändert wurde.

Internet-Adresse	Angabe, unter welcher Bezeichnung Informationen oder Dienste im Internet angesprochen werden können. Die Internet-Adresse wird meist als URL (Unique Ressource Locator) angegeben. Eine typische Internet-Adresse ist z. B. http//:www.datenschutz.rlp.de.
IP-Adresse	Internet Protocol-Adresse. Nummerische Angabe für die eindeutige Bezeichnung eines Rechners im Internet (z. B. 192.168.100.010); siehe auch *TCP/IP*.
ISDN	Integrated Services Digital Network. Kommunikationsprotokoll, über das verschiedene Kommunikationsdienste wie Telefonie, Telefax, Datenkommunikation, Bildtelefon usw. in digitaler Form erbracht werden können.
ISDN-Dienstekennung	Bezeichnung des jeweiligen Kommunikationsdienstes innerhalb des ISDN-Protokolls.
ISDN-Karte	PC-seitige Komponente (Steckkarte) zum Anschluss an das ISDN-Netz.
ISDN-Leistungsmerkmal	Einzelne Funktion innerhalb eines ISDN-Dienstes. Beispielsweise die Übermittlung der Rufnummer an den Gesprächspartner beim ISDN-Telefondienst.
ISDN-Router	*Router*, der das ISDN-Protokoll unterstützt.
Java-Script	Eine von den Firmen SUN und Netscape entwickelte Makrosprache. Die damit erstellten Anweisungen (scripts) werden vom Browser des Client-Rechners interpretiert und ausgeführt (siehe auch *ActiveX*).
Knotenrechner	Vermittlungskomponente innerhalb eines Netzwerks (z. B. Router), die die Datenübertragung steuert.
Kryptografische Verschlüsselung	Verfahren, bei welchem mit Hilfe eines kryptografischen *Algorithmus* Klartexte in ein *Chiffrat* umgewandelt, d. h. verschlüsselt werden. Die Wiederherstellung des ursprünglichen Klartextes ist nur mit Kenntnis des jeweiligen Schlüssels möglich.
Leitungsverschlüsselung	Verschlüsselung des Datenverkehrs auf der physikalischen Ebene zwischen den Anschlusskomponenten einer Kommunikationsverbindung (Leitung oder Funkstrecke). Die Leitungsverschlüsselung erfolgt im Gegensatz zur *Ende-zu-Ende-Verschlüsselung* unabhängig von der jeweiligen Anwendung (z. B. E-Mail). Sie wird i. d. R. über technische Komponenten (Verschlüsselungsboxen, Router) realisiert und erfasst alle Datenübertragungen auf der betroffenen Kommunikationsverbindung. Ein Zutun des Benutzers ist anders als bei der Ende-zu-Ende-Verschlüsselung nicht erforderlich.
Mail-Gateway	Vermittlungsrechner, der die Entgegennahme und Weiterleitung von E-Mail-Nachrichten steuert.
Message Authentication Code	Angabe, anhand derer die *Authentizität* einer Nachricht überprüft werden kann.
Network Information Center (NIC)	Kontrollzentrum eines Netzwerkes, in welchem die Administration und Überwachung des Netzes konzentriert sind.
Öffentlicher Schlüssel	siehe *Public Key*.
Outbound	siehe *Dial-out*.
Overlay-Netz	Ein Netz aus Netzen, d. h. ein Netzwerk, dessen Knoten wiederum aus Netzwerken bestehen.
PAP	Password Authentication Protocol. Kommunikationsprotokoll, bei dem die *Authentisierung* über Passworte erfolgt.
Penetrationstest	Der gezielte Test der Möglichkeiten, von außen mit den einem Angreifer verfügbaren Mitteln in ein geschütztes Netz einzudringen.

PGP	Pretty Good Privacy. Ein weitverbreitetes Programm zur Verschlüsselung und digitalen Signatur auf der Basis *asymmetrischer Verschlüsselungsverfahren*. Das Verfahren gilt bei Verwendung ausreichender Schlüssellängen (> 1 024 Bit) derzeit als sicher.
Pretty Good Privacy	siehe *PGP*.
Private Key	Geheimer Schlüssel. Der Teil eines Schlüsselpaares im Rahmen eines *asymmetrischen Verschlüsselungsverfahrens*, der nur dem Empfänger einer verschlüsselten Nachricht bzw. dem digital Signierenden bekannt sein darf. Der geheime Schlüssel dient der Entschlüsselung einer mit dem *öffentlichen Schlüssel* des Empfängers verschlüsselten Nachricht. Eine mit einem geheimen Schlüssel erzeugte Signatur kann nur mit dem öffentlichen Schlüssel des Erzeugers der Signatur verifiziert werden.
Protokoll	Technische Regelung über den Aufbau und die Größe von Datenpaketen und die Art und Weise, wie diese im Rahmen einer Kommunikation übertragen werden.
Public Key	Öffentlicher Schlüssel. Der Teil eines Schlüsselpaares im Rahmen eines *asymmetrischen Verschlüsselungsverfahrens*, der allen Teilnehmern bekannt sein muss. Zum Verschlüsseln wird mit dem öffentlichen Schlüssel des Empfängers verschlüsselt. Die Entschlüsselung erfolgt durch den Empfänger mit dessen *geheimem Schlüssel*. Bei der digitalen Signatur wird durch den Absender mit dessen geheimem Schlüssel signiert und die Signatur beim Empfänger mit dem öffentlichen Schlüssel des Absenders verifiziert.
Query-ID	Bei der Anfrage an einen DNS-Server vergebene Bezeichnung zur Unterscheidung der verschiedenen DNS-Anfragen (queries).
Relationales Datenbanksystem	Datenbanksystem, bei welchem Daten nicht in fest vorgegebenen Strukturen, sondern in Tabellen vorgehalten werden, die über frei definierbare Relationen untereinander verknüpft werden können.
Replay Attack	Angriff, bei welchem ein Datenstrom (z. B. die Passworteingabe an einem IT-System) aufgezeichnet und zu einem späteren Zeitpunkt erneut eingespielt wird. Der Angriff funktioniert bei Kenntnis der Struktur des Datenstroms auch dann, wenn dieser verschlüsselt ist.
Router	Technische Komponente, die die Wegefindung (Routing) und Übermittlung in einem Netzwerk steuert. Mit Routing bezeichnet man den Weg der Datenpakete innerhalb von Netzen. Das Internet kennt keine Direktverbindungen zwischen Rechnern. Stattdessen erfolgt der Versand von Daten in kleinen Paketen und nach Bedarf über verschiedene Zwischensysteme auf dem zum Übermittlungszeitpunkt günstigsten Weg. Diese Form des Datenverkehrs ermöglicht die hohe Flexibilität und Ausfallsicherheit des Internets.
RSA	Aus den Anfangsbuchstaben der Erfinder (Rivest, Shamir und Adleman) zusammengesetzte Bezeichnung für ein *asymmetrisches Verschlüsselungsverfahren*.
Schlüsselpaar	Das Paar aus geheimem und öffentlichem Schlüssel bei *asymmetrischen Verschlüsselungsverfahren*.
Server	Zentraler Rechner in einem Netzwerk, der den Arbeitsstationen/Clients Daten, Dienste usw. zur Verfügung stellt. Auf dem Server ist das Netzwerk-Betriebssystem installiert, und vom Server wird das Netzwerk verwaltet. Als Server werden neben Rechnern auch Softwarekomponenten bezeichnet, die *Client*-Prozessen, z. B. Internet-Bowsern, Informationen und Funktionen zur Verfügung stellen.
Session-Key	Kryptografischer Schlüssel, der nur für eine bestimmte Zeit (Session) verwendet wird und danach seine Gültigkeit verliert.
SMTP	Simple Mail Transfer Protocol. Kommunikationsprotokoll für die elektronische Post im Internet (siehe *E-Mail*).

Spam-Mail	Die Überflutung von (elektronischen) Postfächern mit unerwünschter *E-Mail* mit dem Ziel, die Funktionsfähigkeit des Mail-Servers zu beeinträchtigen (siehe *Denial of Service-Attacke*).
Spoofing	Vorgehensweise, bei der sich jemand als ein anderer Benutzer, Absender oder Rechner ausgibt, um unbefugten Zugriff auf Daten oder IT-Systeme zu erhalten.
SSL	Secure Socket Layer. Ein Sicherheitsprotokoll, das *Client/Server*-Anwendungen eine Kommunikation ermöglicht, die nicht abgehört oder manipuliert werden kann.
Standleitung	Kommunikationsverbindung, die im Gegensatz zu einer *Wählleitungsverbindung* permanent und in der Regel exklusiv für bestimmte Teilnehmer geschaltet ist.
Symmetrische Verschlüsselung	Verschlüsselungsverfahren, bei welchem im Gegensatz zu *asymmetrischen Verfahren* für die Ver- und Entschlüsselung der gleiche Schlüssel verwendet wird. Dieser muss damit dem Empfänger einer Nachricht auf einem zweiten sicheren Kanal zugeleitet werden.
TCP/IP	Transmission Control Protocol/Internet Protocol. Standard-Kommunikations-*Protokoll* im Internet. Das Internet Protocol (IP) dient der Fragmentierung und Adressierung von Daten und übermittelt diese vom Sender zum Empfänger. Das Transmission Control Protocol (TCP) baut darauf auf, sorgt für die Einsortierung der Pakete in der richtigen Reihenfolge beim Empfänger und bietet die Sicherstellung der Kommunikation durch Bestätigung des Paket-Empfangs. Es korrigiert Übertragungsfehler automatisch.
TCP-Sequence Number	Aufsteigende Nummer, die die logische Reihenfolge der Datenpakete einer Datenübertragung festlegt. Die im Internet auf ggf. unterschiedlichen Wegen übertragenen Pakete werden anhand der TCP-Sequence Number beim Empfänger wieder zusammengesetzt.
Telebox 400	E-Mail-Verfahren der Deutschen Telekom AG auf der Basis des *X.400*-Protokolls.
Triple DES	Verfahren, bei welchem der Verschlüsselungsalgorithmus DES in drei aufeinander folgenden Durchgängen durchlaufen wird. Triple *DES* bietet eine höhere Sicherheit gegenüber Entschlüsselungsversuchen als der einfache *DES*.
Trojanisches Pferd	Programm mit Schadensfunktionen, die zeit- oder ereignisgesteuert ohne Wissen des Benutzers im Hintergrund aktiv werden. Häufig wird dem Benutzer vordergründig eine nützliche oder sinnvolle andere Funktion vorgegaukelt.
Trust-Center	Stelle, die im Rahmen des Einsatzes von Verschlüsselungsverfahren zentrale Funktionen wahrnimmt. Beispiele hierfür sind die Erzeugung kryptografischer Schlüssel, die Erteilung und Verwaltung von *Zertifikaten* sowie der Betrieb von *Verzeichnisdiensten*.
Verzeichnisdienst	Serverdienst, in welchem Personen und Ressourcen mitsamt zugehörigen Attributen katalogisiert werden. Verzeichnisdienste werden z. B. als Adressverzeichnisse für die elektronische Post oder im Rahmen des Einsatzes von Signatur und Verschlüsselungsverfahren für die Verwaltung von *Zertifikaten* eingesetzt.
Virtuelles Privates Netz	Logisches Netz auf physikalischen Kommunikationsverbindungen. Die *VPN*-Technologie ermöglicht es, verschiedene, die gleiche Infrastruktur nutzende Netze gegeneinander abzuschotten.
VPN	*Virtuelles Privates Netz*.
Wählleitungsverbindung	Kommunikationsverbindung, die im Gegensatz zu einer *Standleitung* nur bei Bedarf durch Anwahl des gewünschten Anschlusses aufgebaut wird.
Web-Seite	Seite eines Angebots im *Word Wide Web*.

Word Wide Web	Weltweites Netz. Auch als WWW oder W3 bezeichnet. Gemeint ist ein Dienst im Internet, der sich durch hohe Benutzerfreundlichkeit auszeichnet und zur Verbreitung des Internets massiv beigetragen hat. Entwickelt wurde das World Wide Web von Wissenschaftlern, die auf einfache Art Informationen austauschen wollten. Der Zugriff auf die Informationen erfolgt über WWW-*Browser*.
WWW	siehe *Word Wide Web*.
X.400	Ein Übertragungsprotokoll für den Austausch elektronischer Nachrichten (Elektronische Post).
X.500	Protokoll für den Betrieb und die Kommunikation mit *Verzeichnisdiensten*.
Zertifikat	Im Rahmen digitaler Signaturverfahren die Beglaubigung über die Gültigkeit eines öffentlichen Schlüssels und dessen Zuordnung zu einer bestimmten Person oder Stelle.

Tätigkeitsberichte

des Ausschusses für Datenschutz, der Datenschutzkommission und des Landesbeauftragten für den Datenschutz Rheinland-Pfalz

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
16.	Tätigkeitsbericht	Drucksache 13/2427	vom 15. Dezember 1997

1. Vorbemerkung

1.1 Zum Charakter des Tätigkeitsberichtes

Am Charakter des vorliegenden Tätigkeitsberichtes als Spiegel des breiten Spektrums der Tätigkeit der Behörde des LfD hat sich im Vergleich zu den vorangegangenen Berichten nichts Grundsätzliches geändert. Es finden sich Darstellungen von Verstößen gegen datenschutzrechtliche Vorschriften, überwiegend aber werden gutachtliche Stellungnahmen zu datenschutzrechtlichen Zweifelsfragen, die an den LfD herangetragen worden sind, wiedergegeben. Der Charakter eines Handbuches mit Fällen und Lösungen zum Datenschutzrecht ist erhalten geblieben. Auch wenn die Nachteile dieser Darstellungsform (wie gelegentlich schwere Lesbarkeit und teilweise sehr fachspezifische Ausführungen, die sich nur dem Spezialisten erschließen) nicht verkannt werden, dürften sie durch den Nutzen aufgewogen werden, den die rechtlich möglichst präzise Darstellung für die betroffenen Dienststellen und ihre behördlichen Datenschutzbeauftragten hat.

1.2 Fünfundzwanzig Jahre Datenschutz in Rheinland-Pfalz – ein Rückblick

Bereits im Jahr 1971, gegen Ende der 6. Wahlperiode des Landtags, hatte die CDU-Fraktion einen Gesetzentwurf zu einem Landesdatenschutzgesetz eingebracht. Zu Beginn der 7. Wahlperiode, die im April 1971 begann, brachte sie den Entwurf mit einigen kleineren Änderungen erneut ein. Er wurde nach eingehenden Beratungen am 17. Januar 1974 vom Landtag verabschiedet und am 4. Februar 1974 im Gesetz- und Verordnungsblatt verkündet („Gesetz gegen mißbräuchliche Datennutzung, Landesdatenschutzgesetz – LDatG –“, GVBl. S. 31). Damit war Rheinland-Pfalz nach Hessen das zweite Bundesland und nach Schweden weltweit das dritte Land, das ein Datenschutzgesetz erlassen hatte. Ein entsprechendes Bundesgesetz trat erst am 1. Januar 1978 in Kraft. Vorbilder für das Gesetz waren also kaum vorhanden. Umso mehr sind der Mut und die Kreativität des Gesetzgebers zu würdigen, der einen Sprung ins kalte, unbekannte Wasser gewagt hatte. Der Geltungsbereich beschränkte sich allerdings auf Daten, die durch öffentliche Stellen des Landes „elektronisch“ verarbeitet wurden. Seine wichtigsten Bestimmungen betrafen das Auskunftsrecht der Bürger und ihr Recht, den Ausschuss für Datenschutz anzurufen, die Anmeldepflicht für automatisierte Verfahren und die Pflicht, technisch-organisatorische Datenschutzmaßnahmen zu treffen. Bemerkenswert ist auch, dass es mit 16 Paragraphen auf drei Druckseiten des Gesetz- und Verordnungsblattes auskam (das aktuelle LDSG benötigt 39 Paragraphen auf 14 Seiten).

Der Landtag hielt es für erforderlich, zum Schutz vor den durch die Datenverarbeitung dem Einzelnen und dem staatlichen Institutionengefüge drohenden Gefahren eine besondere Kontrollinstanz ins Leben zu rufen. Damit folgte er dem hessischen Beispiel, nicht aber in der Frage der Organisationsform dieser Kontrollinstanz: Er schuf einen besonderen Ausschuss, den „Ausschuß für Datenschutz nach § 9 des Landesgesetzes gegen mißbräuchliche Datennutzung“, dem er diese Aufgabe übertrug. Er hielt die Personalisierung der Aufgabe in einem „Beauftragten“, wie sie in Hessen erfolgt war, für weniger geeignet: Die unterschiedlichen Interessen sollten in einem Kollegialorgan erörtert und zum Ausgleich gebracht werden.

Am 30. April 1974 wurden die vier vom Landtag zu bestimmenden Mitglieder des Ausschusses gewählt: Es waren die Abgeordneten Dr. Walter Schmitt (der vom Ausschuss dann zu seinem Vorsitzenden gewählt wurde), Hermann Belzner und Fritz Schneider sowie der stellvertretende Leiter der Landtagsverwaltung, Ministerialdirigent Walter P. Becker, der mit Mitarbeitern der Landtagsverwaltung die Geschäftsführung des Ausschusses übernahm. Von der Landesregierung wurde Staatssekretär Alois Schreiner als Mitglied bestellt.

Bereits am 17. Oktober 1974 legte der Ausschuss – entsprechend seinem gesetzlichen Auftrag – dem Landtag und der Öffentlichkeit seinen ersten Tätigkeitsbericht vor, in dem er Folgendes feststellte:

> „Die kurze Zeit der Beschäftigung mit der Problematik des Datenschutzes hat dem Ausschuß die Erkenntnis vermittelt, daß im Lande auch schon vor dem Inkrafttreten des Datenschutzgesetzes im Rahmen der Selbstkontrolle sachgerechte Anstrengungen unternommen wurden, um den Mißbrauch gespeicherter Daten zu verhindern. Der Ausschuß hat bisher noch keine Feststellungen treffen können, daß in der Vergangenheit schutzwürdige Belange Einzelner beeinträchtigt worden wären. Insgesamt hat sich aber auch bestätigt, daß es notwendig war, der Entwicklung der Datenverarbeitungstechnik und den sich daraus ergebenden erhöhten Gefahren durch Erlaß eines Gesetzes und die Schaffung einer Kontrollinstanz Rechnung zu tragen.“ (1. Tb., Tz. 5).

In der Folge wurden bis 1981 jährlich und ab diesem Zeitpunkt zweijährig Tätigkeitsberichte vorgelegt.

Das Gesetz wurde in den zurückliegenden 25 Jahren mehrmals und teilweise auch grundlegend geändert:

14. Februar 1975 – „Landesgesetz zur Änderung des Gesetzes gegen mißbräuchliche Datennutzung“ (GVBl. S. 84): Erstreckung des Datenschutzes auf private Krankenhäuser, besondere Regelungen für medizinische Daten.

21. Dezember 1978 – „Landesgesetz zum Schutz des Bürgers bei der Verarbeitung personenbezogener Daten“ (Landesdatenschutzgesetz – LDatG – , GVBl. S. 749): Anpassung an das zum 1. Januar 1978 in Kraft getretene Bundesdatenschutzgesetz, Erweiterung auf herkömmlich gespeicherte Daten, die „zur Übermittlung an Dritte bestimmt sind“, Verankerung des Erforderlichkeitsgrundsatzes als Voraussetzung der Datenverarbeitung, Umbenennung des „Ausschusses für Datenschutz“ in „Datenschutzkommission“.

14. Mai 1982 – „Landesgesetz zur Aufhebung und Änderung von Berichtspflichten gegenüber dem Landtag“ (GVBl. S. 129), Art. 3: Umwandlung der jährlichen in eine zweijährige Berichtspflicht.

27. März 1987 – „Landesstatistikgesetz“ (GVBl S. 57): Streichung der die Statistik betreffenden Regelung im LDatG.

13. Februar 1991 – „Landesgesetz zur Bestellung eines Landesbeauftragten für den Datenschutz“, (GVBl. S. 46): Ersetzung der Datenschutzkommission in Anpassung an die Rechtsentwicklung aller anderen Bundesländer und des Bundes durch einen Landesbeauftragten für den Datenschutz; Schaffung einer aus sechs Mitgliedern (fünf Abgeordneten und einem Vertreter der Landesregierung) bestehenden „Kommission beim Landesbeauftragten für den Datenschutz“.

5. Juli 1994 – „Landesdatenschutzgesetz“ (LDSG, GVBl. S. 293): Anpassung an die Anforderungen des Volkszählungsurteils des Bundesverfassungsgerichts und an das neue Bundesdatenschutzgesetz vom 20. Dezember 1990 (BGBl. I S. 2954). Grundsätzliche Geltung auch für herkömmlich verarbeitete Daten.

18. Juli 1996 – „Landesgesetz zur Änderung von Vorschriften über die Besetzung von Gremien“ (GVBl. S. 270): Erweiterung der Zahl der Mitglieder der Kommission beim Landesbeauftragten für den Datenschutz auf acht.

Absehbar ist eine erneute Novellierung des Gesetzes zur Anpassung an die EG-Datenschutzrichtlinie und zur weiteren Modernisierung der Instrumente des Datenschutzes (vgl. unten Tz. 2 und 3.3).

Mitglieder des Ausschusses für Datenschutz (AfD), der Datenschutzkommission (DSK) und der Kommission beim Landesbeauftragten für den Datenschutz (KbLfD) in alphabetischer Reihenfolge:

Walter P. Becker	Geschäftsführendes Mitglied des AfD von Juni 1974 bis Dezember 1978; Geschäftsführendes Mitglied der DSK von Januar 1979 bis April 1991
Johannes Berg	Mitglied der KbLfD seit Juni 1996
Hermann Belzner	Mitglied des AfD von Juni 1974 bis Mai 1975
Franz Josef Bischel	Mitglied der DSK von Mai 1983 bis April 1991; Vorsitzender der DSK von Mai 1988 bis April 1991; Mitglied der KbLfD seit August 1991; Vorsitzender der KbLfD seit Juni 1996
Jürgen Creutzmann	Mitglied der KbLfD seit April 1999
Dr. Werner Danz	Mitglied der DSK von Januar 1979 bis Mai 1983
Friedel Grützmacher	Mitglied der KbLfD seit August 1996
Hendrik Hering	Mitglied der KbLfD seit April 1999
Herbert Mertin	Mitglied der KbLfD von Juni 1996 bis April 1999
Dieter Muscheid	Mitglied der DSK von Mai 1983 bis April 1991; Vorsitzender der KbLfD von August 1991 bis Mai 1996; Mitglied der KbLfD von Juni 1996 bis April 1999
Carsten Pörksen	Mitglied der KbLfD seit August 1991
Axel Redmer	Mitglied der KbLfD seit August 1996
Prof. Heinrich Reisinger	Mitglied der DSK von Juni 1988 bis April 1991; Mitglied der KbLfD von August 1991 bis Mai 1996
Prof. Dr. Walter Rudolf	Vertreter der Landesregierung in der DSK von April 1987 bis April 1991
Klaus Rüter	Vertreter der Landesregierung in der KbLfD von August bis Dezember 1994
Rudolf Scharping	Mitglied des AfD von Mai 1975 bis Dezember 1978; Mitglied der DSK von Januar 1979 bis Mai 1983
Dr. Walter Schmitt	Vorsitzender des AfD von Juni 1974 bis Dezember 1978; Vorsitzender der DSK von Januar 1979 bis Mai 1983
Fritz Schneider	Mitglied des AfD von Juni 1974 bis Dezember 1974
Leo Schönberg	Vorsitzender der DSK von Mai 1983 bis Mai 1988; Mitglied der KbLfD von August 1991 bis Mai 1996
Alois Schreiner	Vertreter der Landesregierung im AfD von Juni 1974 bis Dezember 1978; in der DSK von Januar 1979 bis Dezember 1979
Dr. Ernst Theilen	Vertreter der Landesregierung in der KbLfD seit Dezember 1994
Dr. Klaus-Dieter Uelhoff	Vertreter der Landesregierung in der DSK von Januar 1980 bis März 1987
Wilhelm Ulmen	Mitglied des AfD von Januar 1975 bis Dezember 1978; Mitglied der DSK von Januar 1979 bis Mai 1979

In das Amt des Landesbeauftragten für den Datenschutz wurde für die Zeit ab April 1991 Universitätsprofessor Dr. Walter Rudolf gewählt; er wurde 1999 für eine weitere Wahlperiode im Amt bestätigt.

Die bisher erschienenen 17 Tätigkeitsberichte mit einem Umfang von insgesamt ca. 3 000 Seiten dokumentieren die Tätigkeit der für die externe unabhängige Datenschutzkontrolle der Verwaltung des Landes Verantwortlichen relativ detailliert. Sie geben zugleich einen Überblick über die technische Entwicklung der Datenverarbeitung in der Verwaltung des Landes.

Zusammenfassend kann festgestellt werden, dass die Entwicklung des Datenschutzes, wie sie in Rheinland-Pfalz früh begonnen hat, wie sie sich aber auch andernorts und inzwischen europaweit vollzogen hat und noch vollzieht, notwendig war und unumkehrbar ist. Datenschutz ist als zu beachtender Gesichtspunkt bei der Fortentwicklung der Datenverarbeitung und der Kommunikationstechnik eine Selbstverständlichkeit geworden. Dies begründet die Erwartung, dass auch künftig die Entwicklung sich nicht unter Missachtung der Rechte der betroffenen Bürger, sondern unter Beachtung der von der Allgemeinheit für notwendig gehaltenen, vom Gesetzgeber normierten Regeln vollziehen wird. Einen Beitrag dazu wird die unabhängige externe Datenschutzkontrolle auch weiterhin leisten.

1.3 Zur aktuellen Situation des Datenschutzes und des Datenschutzrechts in Rheinland-Pfalz

Die Situation für den Datenschutz hat sich in den letzten beiden Jahren nicht grundlegend gewandelt; die im 16. Tb. hierzu enthaltenen allgemeinen Ausführungen sind nach wie vor zutreffend. Einige Aspekte sollen dennoch hervorgehoben werden:

Die Internet-Nutzung durch private und öffentliche Stellen gewinnt ständig an Bedeutung: Derzeit sollen ca. 11,8 Mio. Deutsche das Netz nutzen, die Zahl der Homepages ist international kaum übersehbar. Die damit einhergehenden Anforderungen an den Datenschutz sind vielfältig: Internationale Regelungen sind zu schaffen, vor Ort muss eine kompetente Beratung der öffentlichen Stellen erfolgen, die diese Technik ebenfalls zunehmend nutzen.

In den letzten Jahren hat sich verstärkt die Erkenntnis durchgesetzt, dass keinesfalls nur oder in erster Linie der Staat als Inhaber von Datenmacht das Persönlichkeitsrecht der Bürger gefährden kann. Die extensive Nutzung der automatisierten Datenverarbeitung durch private Datenverarbeiter in allen Bereichen, angefangen bei Versicherungen über Krankenkassen zu Versandhäusern und Anbietern von Internetangeboten, gekennzeichnet durch Stichworte wie „Data-Mining“ und „Data-Warehouses“, verdeutlicht, dass dem Datenschutz gerade auch in diesem Bereich besondere Bedeutung zukommt.

Das für den Zuständigkeitsbereich des LfD ständig an Bedeutung gewinnende Thema „Outsourcing“ – die Auslagerung von Aufgaben öffentlicher Stellen an Privatunternehmen – wird unter Tz. 14.6 behandelt. Dort sind die Ergebnisse einer unter Federführung des LfD von der Konferenz der Datenschutzbeauftragten des Bundes und der Länder eingesetzten Arbeitsgruppe ausführlich dargestellt.

Immer mehr öffentliche Stellen nutzen das Instrument der „Telearbeit“, wodurch ebenfalls neue Fragen entstehen (s. u. Tz. 17.3).

Auch der zunehmende Einsatz der Videoüberwachungstechnik ist zu erwähnen. Datenschutz darf sich aber auch in dieser Situation nicht als Verhinderungsinstrument für die Fortentwicklung der Kommunikationsaktivitäten in der Gesellschaft verstehen. Ein wesentlicher Teil unserer Volkswirtschaft und unseres Bruttosozialproduktes beruht auf unserer gut funktionierenden kommunikationstechnischen Infrastruktur und den technisch fortgeschrittenen Möglichkeiten der globalen Kommunikation. Das erklärte Ziel der Landesregierung, durch die Propagierung neuer Medien und neuer Technologien die Wettbewerbsfähigkeit des Landes zu stärken, ist auch aus datenschutzrechtlicher Sicht keinesfalls abzulehnen. Zudem darf nicht vergessen werden, dass der Mensch als soziales Wesen auf Kommunikation angelegt ist. Nicht der Einsiedler in seiner unzugänglichen Höhle, sondern der dem Gemeinwesen gegenüber aufgeschlossene und sich ihm verpflichtet fühlende Bürger entspricht dem Menschenbild des Grundgesetzes. Dazu gehört allerdings die Selbstbestimmungsfähigkeit und das entsprechende Recht, sich Kommunikationspartner auszusuchen und sich unerwünschten Kontaktaufnahmen oder allwissenden Kontaktsuchenden entziehen zu können.

Die klassischen datenschutzrechtlichen Instrumente verlieren angesichts der angedeuteten technischen Entwicklung an Wirksamkeit. Sie sind zu ergänzen. In der aktuellen Diskussion werden dabei insbesondere die Stichworte „Datenschutz durch Technik“, „Grundsatz der Datenvermeidung und Datensparsamkeit“ sowie „Einführung eines Datenschutz-Audits“ hervorgehoben. Diese Gesichtspunkte zielen darauf ab, durch Technikgestaltung bereits im Vorfeld der Entwicklung eines automatisierten Datenverarbeitungsverfahrens datenschutzfreundliche Technologien zu berücksichtigen.

Der LfD geht nicht so weit, in diesen Neuerungen einen Paradigmenwandel zu sehen oder sie als „neuen Datenschutz“ zu bezeichnen. Es handelt sich um die Fortentwicklung von rechtlichen Gesichtspunkten und technisch-organisatorischen Instrumenten, die bereits in der Vergangenheit Bedeutung hatten, wenn sie auch nicht mit dieser Betonung und mit dieser Benennung zu den grundlegenden Datenschutzinstrumenten gezählt worden sind.

Zur Beschränkung des Einsatzes optischer Erfassungen und Speicherungen der Bürger (Stichwort: Verbreitung der Videoüberwachung) müssen noch angemessene Regelungen entwickelt werden; die Datenschutzbeauftragten bemühen sich derzeit um die Erarbeitung von gemeinsamen Vorschlägen.

Was die Datenschutzgesetzgebung angeht, ist der im 16. Tb. bereits genannte Gesichtspunkt erneut hervorzuheben, dass die Zunahme detaillierter bereichsspezifischer Datenschutzregelungen keineswegs zwangsläufig zu einer Verbesserung des Datenschutzes führt. In letzter Zeit hat der frühere Bundesbeauftragte für den Datenschutz, Universitätsprofessor Dr. Bull, diesen Gesichtspunkt systematisiert und konkrete Folgerungen daraus gezogen (vgl. Bull, Bemerkungen über Stil und Technik der Datenschutzgesetzgebung, RDV 1999, S. 148 f.). Die dort deutlich werdenden Bestrebungen, das allgemeine Datenschutzrecht einerseits zu vereinfachen, es andererseits aber auch in seiner Bedeutung für die Praxis dadurch zu stärken, dass datenschutzrechtlich inhaltsarme bereichsspezifische Regelungen entfallen, werden durch den LfD nachdrücklich unterstützt.

2. Zur Novellierung des Bundesdatenschutzgesetzes

Es zeichnet sich ab, dass der Bundesgesetzgeber das Bundesdatenschutzgesetz an die EG-Datenschutzrichtlinie anpassen wird. Der derzeit vorliegende Entwurf des Bundesinnenministeriums enthält darüber hinaus auch eine Reihe von Regelungen, die der Modernisierung des Datenschutzrechts dienen sollen. So sollen der Grundsatz der Datensparsamkeit bzw. Datenvermeidung sowie eines „Datenschutz-Audits“ im Gesetz geregelt werden. Auch der Chipkarteneinsatz findet Erwähnung. Der LfD hat allerdings in diesem Zusammenhang noch verschiedene Anliegen formuliert. Das Bundesdatenschutzgesetz wird in seiner neuen Fassung selbstverständlich Auswirkungen auf die – aus Gründen der Anpassung an die EG-Datenschutzrichtlinie und seiner allgemeinen Modernisierung – anstehende Novellierung des Landesdatenschutzgesetzes haben. Vorschriften des Bundesgesetzes, die in vergleichbarer Weise also auch für öffentliche Stellen des Landes bedeutsam werden könnten und deren Leitbildfunktion insoweit nahe liegt, haben deshalb bei der Beurteilung der BDSG-Novellierung durch den LfD besondere Bedeutung.

a) Der LfD hält eine gesetzliche Klarstellung, dass das Beobachten und Speichern mit optisch-elektronischen Einrichtungen (also mit Hilfe von Videokameras) vom Begriff der Datenverarbeitung umfasst wird, für zumindest nützlich.

b) Das BDSG hält im derzeit vorliegenden Entwurf an der Dreiteilung der Definition des Umgangs mit Daten im Erheben, Verarbeiten und Nutzen von Daten fest. Die EG-Datenschutzrichtlinie sieht – ebenso wie das rheinland-pfälzische Landesdatenschutzgesetz – demgegenüber einen einheitlichen Verarbeitungsbegriff vor. Der Verarbeitungsbegriff sollte insgesamt in diesem Sinne vereinheitlicht werden. Selbst wenn sich hieraus nur geringe praktische Konsequenzen ergeben, liegt dies im Interesse einer möglichst einheitlichen europaweiten Terminologie.

c) Die Definition des „Pseudonymisierens“ in § 3 Abs. 6 a und § 3 a des Entwurfs sollte noch weiter verbessert werden; durch die derzeitige Fassung wird der Unterschied zwischen „Pseudonymisieren“ und „Anonymisieren“ nicht genügend deutlich. Außerdem sollte nicht auf den beabsichtigten Zweck, sondern auf den Erfolg der Maßnahme abgestellt werden: Untaugliche Pseudonymisierungsversuche dürften nicht als „Pseudonymisierungen“ i. S. d. Gesetzes zu betrachten sein. Schließlich ist eindeutig zu bestimmen, für wen es nach erfolgter Pseudonymisierung wesentlich erschwert sein muss, einen Personenbezug herzustellen: jedermann, der Daten verarbeitenden Stelle oder nur bestimmten Dritten? Insoweit schlägt der LfD in Anlehnung an einen Formulierungsvorschlag des hamburgischen Landesdatenschutzbeauftragten folgende Definition vor: „Pseudonymisieren ist das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche und sachliche Verhältnisse ohne Nutzung der Zuordnungsregel durch die Daten verarbeitende Stelle oder Dritte nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.“

   Schließlich sollten auch die Rechtsfolgen einer erfolgten Pseudonymisierung im Gesetz ausreichend deutlich werden; dies ist nach dem vorliegenden Entwurf nicht der Fall.

d) Bei der Regelung der Einwilligung des Betroffenen als Rechtsgrundlage für den Umgang mit Daten (§ 4 a des Entwurfs) sollte – wie in § 5 Abs. 3 Satz 2 LDSG – eine Bestimmung aufgenommen werden, dass der Betroffene die Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen kann. Außerdem sollte, um die absehbare technische Entwicklung in diesem Zusammenhang zu berücksichtigen, eine Regelung zur elektronisch erteilten Einwilligung aufgenommen werden.

e) Das BDSG sollte – wie künftig auch das Landesrecht – Beamte und Arbeitnehmer im öffentlichen Dienst unter datenschutzrechtlichen Gesichtspunkten gleichstellen. Gründe für eine Differenzierung sind hier nicht ersichtlich. Insoweit wäre § 12 Abs. 4 des Entwurfs zu ändern.

f) Das Recht der behördlichen Datenschutzbeauftragten, sich an die jeweils zuständige Datenschutzaufsichtsbehörde (also hier den BfD) zu wenden, wird im vorliegenden Entwurf dadurch eingeschränkt, dass dies nur im Benehmen mit dem Leiter der verantwortlichen Stelle zulässig sein soll (§ 4 g Abs. 1 Satz 2 BDSG-Entwurf). Art. 20 Abs. 2 2. Alternative der EG-Datenschutzrichtlinie enthält diese Einschränkung nicht, sondern spricht nur davon, dass der (interne) Datenschutzbeauftragte im Zweifelsfall die Kontrollstelle (also den Bundes- bzw. Landesbeauftragten für den Datenschutz) konsultieren muss. Auch die Vereinfachung des Anmeldeverfahrens gem. Art. 18 der Richtlinie setzt die unabhängige Überwachung des Datenschutzes durch interne Datenschutzbeauftragte voraus. In Erwägungsgrund 49 (letzter Satz) wird diese Stellung mit folgender Formulierung unterstrichen: „Ein solcher Beauftragter, ob Angestellter der für die Verarbeitung Verantwortlichen oder externer Beauftragter, muss seine Aufgaben in vollständiger Unabhängigkeit ausüben können.“ Die im Entwurf vorgesehene Einschränkung sollte also entfallen.

g) Zu begrüßen ist, dass im vorliegenden Entwurf eine Regelung über den Einsatz von Chipkarten enthalten ist (§ 6 c des Entwurfs). Es sollte erwogen werden, ergänzend auch materielle Voraussetzungen für den Einsatz solcher mobiler personenbezogener Speicher- und Verarbeitungsmedien zu regeln.

h) Zu den technischen und organisatorischen Maßnahmen des Datenschutzes, die in § 9 sowie der Anlage zum Gesetzentwurf genannt sind, sollten ergänzend zu der konkreten Aufzählung bestimmter Kontrollmaßnahmen, die der LfD nach wie vor für wichtig und unverzichtbar hält (und die sich an den Katalogen der novellierten Datenschutzgesetze Hessens und Brandenburgs orientieren sollten), weitere technikunabhängige allgemeine Ziele dieser technischen und organisatorischen Datenschutzmaßnahmen (Sicherheitsziele: Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität, Revisionsfähigkeit und Transparenz) definiert werden.

i) Das Widerspruchsrecht Betroffener gegen die datenschutzrechtliche Kontrolle von Sicherheitsüberprüfungsakten (§ 24 Abs. 2 Satz 4 des Entwurfs) sollte gestrichen werden. Dieses Widerspruchsrecht kann im Hinblick auf das umfassende Kontrollrecht gem. Art. 28 Abs. 3 der EG-Datenschutzrichtlinie nicht aufrechterhalten bleiben.

   Dies gilt auch bezüglich der Einschränkungen der Kontrollbefugnisse des BfD in § 24 Abs. 4 Satz 4 des Entwurfs.

j) Die Strafvorschrift des § 43 Abs. 1 und Abs. 2 Nr. 1 des Entwurfs hat – wie die entsprechende Vorschrift des geltenden BDSG – die Straflosigkeit des rechtswidrigen Umgangs mit „offenkundigen“ Daten zur Folge. Die Rechtsprechung hat den Begriff der „offenkundigen“ Daten allerdings so weit ausgedehnt, dass dadurch eine bedenkliche Strafbarkeitslücke entstanden ist, die aus der Sicht des LfD nicht hingenommen werden kann. Daher sollte der Halbsatz „die nicht offenkundig sind“ durch die Formulierung „die nicht jeder Person ohne rechtlich geregelte Voraussetzung frei zugänglich sind“ ersetzt werden.

3. Datenschutz in Europa

3.1 Nachholbedarf bei der Umsetzung der EG-Datenschutzrichtlinie

Die EG-Datenschutzrichtlinie hätte bis zum 24. Oktober 1998 in Bundes- und Landesrecht umgesetzt werden müssen. Dies ist – mit Ausnahme des entsprechend novellierten hessischen Landesdatenschutzgesetzes – weder für die allgemeinen noch für die bereichsspezifischen datenschutzrechtlichen Vorschriften fristgerecht erfolgt.

Fragen der Umsetzung der EG-Datenschutzrichtlinie haben den LfD in der Vergangenheit wiederholt beschäftigt. So wurde das Thema bereits in den zurückliegenden Tätigkeitsberichten angesprochen und ausführlich dargestellt (vgl. 14. Tb.,Tz. 3; 15. Tb., Tz. 3.1.2; 16. Tb., Tz. 3.2). Zur Konzeption der Umsetzung hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder im Berichtszeitraum mit einer Entschließung Position bezogen (vgl. Anlage 1). Die Umsetzung betrifft vor allem den Datenschutz im privaten Sektor, für den der Bund die Gesetzgebungsbefugnis besitzt. So hat die Richtlinie im Hinblick auf das BDSG erheblichen Novellierungsbedarf ausgelöst.

Auf einen Gesichtspunkt hat der LfD in diesem Zusammenhang stets aufmerksam gemacht: Es ist außerordentlich wichtig, eine einheitliche Nomenklatur zu erreichen, um der sich abzeichnenden terminologischen Sprachverwirrung zu begegnen. Insbesondere sollten die Regelungen hinsichtlich der Datenübermittlung in Staaten außerhalb der Europäischen Union in Deutschland einheitlich sein. Auch im Bereich technisch-organisatorischer Regelungen ist eine Verzahnung mit der Terminologie des BDSG anzustreben.

Sobald der Entwurf der Bundesregierung zur Novellierung des BDSG vorliegt, ist davon auszugehen, dass zeitnah auch der Entwurf eines Gesetzes zur Novellierung des LDSG vorgelegt werden wird.

3.2 Die unmittelbare Wirkung der EG-Datenschutzrichtlinie vom 24. Oktober 1995

Zunächst ist darauf hinzuweisen, dass die EG-Datenschutzrichtlinie sich nur auf Tätigkeiten bezieht, die in den Anwendungsbereich des Gemeinschaftsrechts fallen. Soweit Landesrecht nicht in den Kompetenzbereich der EG fällt, können von der EG-Datenschutzrichtlinie abweichende Regelungen getroffen oder beibehalten werden (z. B. im Polizei- und Ordnungsbehördengesetz, Landesverfassungsschutzgesetz, Meldegesetz).

Nachdem die dreijährige Umsetzungsfrist verstrichen ist, sind die vom EuGH entwickelten Grundsätze zur unmittelbaren Anwendung nicht rechtzeitig umgesetzter Richtlinien zu beachten. Voraussetzung für eine Direktwirkung ist, dass die Richtlinie Einzelnen ein hinreichend bestimmtes unbedingtes subjektives Recht gegenüber dem Staat einräumt. Ein Problem in diesem Zusammenhang liegt darin, dass zahlreiche Regelungen der Richtlinie inhaltlich nicht so genau gefasst sind, dass sie für eine unmittelbare Anwendung in Frage kommen. So gewährt eine ganze Reihe von Vorgaben den Mitgliedstaaten bei der Ausgestaltung des nationalen Datenschutzrechts einen erheblichen Spielraum. Insoweit könnte es an der von der EuGH-Rechtsprechung geforderten hinreichenden Bestimmtheit und Unbedingtheit fehlen. Einige Regelungen erfüllen jedoch die Voraussetzungen direkter Wirkung. In diesem Bereich ist dann zu beachten, dass die Direktwirkung nur zu Gunsten und nicht zu Lasten von Privatpersonen gilt. Sie wird auch nur dort relevant, wo BDSG, LDSG oder bereichsspezifische Vorschriften nicht bereits die Anforderungen der Richtlinie erfüllen. Unter diesen Voraussetzungen sind insbesondere die nachfolgend genannten Vorschriften der EG-Datenschutzrichtlinie zu beachten:

– Nach Art. 8 (Verarbeitung besonderer Kategorien personenbezogener Daten) ist die Verarbeitung von Daten über die rassische und ethnische Herkunft, politische Meinungen, religiöse und weltanschauliche Überzeugungen, die Gewerkschaftszugehörigkeit, die Gesundheit oder das Sexualleben grundsätzlich nur dann zulässig, wenn sie durch Spezialvorschrift erlaubt ist oder eine ausdrückliche Einwilligung der Betroffenen vorliegt.

– Die Artikel 10 und 11 regeln die Information der von der Verarbeitung personenbezogener Daten Betroffenen. Die Richtlinie sieht hier eine weiter gehende Informationspflicht der Daten verarbeitenden Stelle als das bisher geltende Datenschutzrecht vor. Dem Wortlaut nach ist hierzu kein Antrag der Betroffenen erforderlich, vielmehr haben die Daten verarbeitenden Stellen die Betroffenen schriftlich zu benachrichtigen und dabei unter anderem zu informieren über die Rechtsgrundlage und den Zweck der Datenverarbeitung, die Art der Daten, mögliche Empfänger, das Bestehen von Auskunfts- und Berichtigungsrechten sowie über mögliche Folgen einer unterlassenen Beantwortung. Die Benachrichtigung hat mit der Speicherung bzw. bei einer Übermittlung mit deren Durchführung zu erfolgen. Keine weiter gehende Pflicht zur Information Betroffener besteht dann, wenn die Daten beim Betroffenen selbst erhoben werden, die Verarbeitung ausdrücklich durch ein Gesetz vorgesehen ist, Betroffene anderweitig Kenntnis von der Verarbeitung ihrer personenbezogenen Daten erhalten haben, die Benachrichtigung der Betroffenen unmöglich ist oder einen unverhältnismäßig großen Aufwand erfordert.

– Art. 12 garantiert Betroffenen ein weit gehendes Auskunftsrecht. Einschränkungen sind unter den in Art. 13 Abs. 1 a bis g genannten Voraussetzungen zulässig. Sie betreffen u. a. Datenverarbeitungen im Zusammenhang mit der Sicherheit des Landes, der Landesverteidigung, der öffentlichen Sicherheit, der Gefahrenabwehr oder der Strafverfolgung.

– Art. 14 räumt Betroffenen auch bei einer rechtmäßigen Verarbeitung personenbezogener Daten ein Widerspruchsrecht ein. Die Verarbeitung ist in den dort genannten Fällen nur dann zulässig, wenn die Daten verarbeitende Stelle nach pflichtgemäßem Ermessen entscheidet, dass das persönliche Interesse konkret Betroffener hinter dem öffentlichen Interesse an der Verarbeitung personenbezogener Daten zurückzustehen hat. Das Widerspruchsrecht entfällt allerdings dann, wenn ein Gesetz die Datenverarbeitung ausdrücklich vorsieht. In diesem Fall wird davon ausgegangen, dass der Gesetzgeber bei Schaffung der jeweiligen Rechtsvorschrift die notwendige Güterabwägung bereits vorgenommen hat. Die Betroffenen sind über das Ergebnis der Prüfung ihres Widerspruchs zu unterrichten.

3.3 Novellierungsbedarf des LDSG auf Grund der Vorgaben der EG-Datenschutzrichtlinie

Der LfD hat – was die richtlinienkonforme Umsetzung des LDSG anbelangt – insbesondere hinsichtlich struktureller und terminologischer Fragen im Zusammenhang mit der Anpassung des BDSG (vgl. oben Tz. 3.1) angeraten, Zurückhaltung zu üben, um die künftige – einheitliche – Rechtsanwendung nicht zu erschweren.

Bei der Novellierung des LDSG können u. a. folgende Regelungen der EG-Datenschutzrichtlinie eine Rolle spielen:

– Die Regelungsgegenstände der Artikel 8 und 10 bis 14 wurden bereits in Bezug auf die Direktwirkung unter Tz. 3.2 erläutert.

– In Art. 15 ist ein generelles Verbot automatisierter Einzelentscheidungen vorgesehen (Ausnahmen sind zulässig).

– Art. 23 erweitert die Haftung und macht sie bei rechtswidriger Datenverarbeitung weder von der Anwendung eines automatisierten Verfahrens noch von dem nach § 823 BGB erforderlichen Vorliegen eines Verschuldens abhängig.

– Die EG-Datenschutzrichtlinie macht eine Neuregelung der Datenübermittlung ins Ausland notwendig. Die Anforderungen aus Art. 25 und 26 sind umzusetzen, soweit sie auf öffentliche Stellen anwendbar sind. Grundsätzlich gilt Folgendes:

  a) Für die Übermittlung von personenbezogenen Daten an ausländische Personen und Stellen im Hoheitsgebiet der Mitgliedstaaten der Europäischen Union sowie für die Verarbeitung personenbezogener Daten im Auftrag durch solche Personen und Stellen gelten die Vorschriften für die Übermittlung an deutsche Stellen entsprechend.

  b) Die Übermittlung personenbezogener Daten an andere ausländische Personen und Stellen sowie an sonstige über- und zwischenstaatliche Stellen ist zulässig, soweit dies in einem Gesetz, einem Rechtsakt der Europäischen Gemeinschaft oder einem internationalen Vertrag geregelt ist.

  c) Eine Übermittlung darf auch erfolgen, wenn die Voraussetzungen der nationalen Übermittlung erfüllt sind und im Empfängerland gleichwertige Datenschutzregelungen gelten.

  d) Die Gleichwertigkeit von Datenschutzregelungen in einem Staat außerhalb der Europäischen Union (Drittland) wird unter Berücksichtigung aller Umstände festgestellt, die bei der Datenübermittlung eine Rolle spielen (z. B. Sicherheitsmaßnahmen im Drittland, Art der Daten, Zweckbestimmung).

  e) Eine Übermittlung personenbezogener Daten an Personen und Stellen in einem Drittland ist auch zulässig, wenn dies zur Erfüllung eines Vertrages zwischen der verarbeitenden Stelle und dem Betroffenen erforderlich ist oder wenn dies unzweifelhaft zur Wahrnehmung eines überwiegenden öffentlichen Interesses oder zur Wahrung lebenswichtiger und vergleichbarer Interessen der Betroffenen erforderlich ist.

Im Hinblick auf den konkreten Handlungsbedarf steht der LfD im Gespräch mit der Landesregierung.

3.4 Vereinbarung zum Datenschutz zwischen der Europäischen Union und den Vereinigten Staaten in Sicht

Der Dialog über den Datenschutz zwischen der Europäischen Union und den USA schreitet weiter voran. Bei einer Zusammenkunft im Juni 1999 wurde ein gemeinsamer Bericht der Kommissionsdienststellen und des amerikanischen Handelsministeriums vorgestellt. In diesem Bericht wird darauf hingewiesen, dass beide Parteien demnächst eine Einigung über die so genannten „Grundsätze des sicheren Hafens“ (safe harbour principles) erzielen möchten. Dieser neue Ansatz würde es ermöglichen, eine Brücke zwischen der Europäischen Gesetzgebung (EG-Datenschutzrichtlinie) und der US-Gesetzgebung zu schlagen. Dabei würde bei der Übermittlung personenbezogener Daten ein effektiver Schutz der Privatsphäre gewährleistet.

3.5 Datenschutz innerhalb der Gemeinschaftsorgane und -einrichtungen

Die Europäische Kommission und die anderen Einrichtungen der Gemeinschaft haben täglich mit einer Vielzahl personenbezogener Daten umzugehen. Ein Austausch dieser Daten erfolgt beispielsweise auch zwischen der Gemeinschaft und den Mitgliedstaaten. Der Vertrag von Amsterdam enthält Regelungen über den Datenschutz bei den Organen und Einrichtungen der Gemeinschaft sowie für die Errichtung einer unabhängigen Datenschutzkontrollinstanz. Die Bestimmung des Art. 286 EGV lautet:

„(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 diesen Vertrag oder auf der Grundlage dieses Vertrags errichteten Organe und Einrichtungen der Gemeinschaft Anwendung.

(2) Vor dem in Absatz 1 genannten Zeitpunkt beschließt der Rat gemäß dem Verfahren des Artikels 251 die Errichtung einer unabhängigen Kontrollinstanz, die für die Überwachung der Anwendung solcher Rechtsakte der Gemeinschaft auf die Organe und Einrichtungen der Gemeinschaft verantwortlich ist, und erlässt erforderlichenfalls andere einschlägige Bestimmungen.“

Die Gemeinschaftsorgane sind danach verpflichtet, Vorkehrungen zum Datenschutz zu treffen. Die Europäische Kommission hat nunmehr einen Vorschlag für eine Verordnung zum Schutz von Daten innerhalb der Gemeinschaftsorgane und -einrichtungen vorgelegt. Der Verordnungsvorschlag muss vom EU-Ministerrat und dem Europäischen Parlament im Mitentscheidungsverfahren angenommen werden.

Die datenschutzrechtlichen Regelungen des Verordnungsvorschlags gründen sich auf bestehende gemeinschaftsrechtliche Regelungen zum Datenschutz, die für die Mitgliedstaaten Geltung haben, insbesondere auf die EG-Datenschutzrichtlinie. Diese stellt jedoch lediglich einen rechtlichen Rahmen dar. Die konkreten Vorschriften für Organe und Einrichtungen der Gemeinschaft müssen daher in einer Verordnung mit direkter Geltungskraft festgelegt werden. Der Verordnungsvorschlag sieht vor, dass personenbezogene Daten

- den Zwecken entsprechen, für die sie erhoben oder weiterverarbeitet werden, dafür erheblich sind und nicht darüber hinausgehen;
- nach Treu und Glauben und auf rechtmäßige Weise verarbeitet werden;
- sachlich richtig und, wenn erforderlich, auf den neuesten Stand gebracht sind;
- für genau bestimmte, eindeutige und rechtmäßige Zwecke erhoben und nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden;
- nicht länger, als es für die Erhebungs- oder Weiterverarbeitungszwecke erforderlich ist, in einer Form aufbewahrt werden, die die Identifizierung der betroffenen Personen ermöglicht.

Nach dem Verordnungsvorschlag hätten die Bürgerinnen und Bürger durchsetzbare Rechte, wie das Recht auf Zugang, Berichtigung, Sperrung und Löschung sie betreffender personenbezogener Daten, die bei den einzelnen Organen und Einrichtungen der Gemeinschaft vorhanden sind.

Von besonderer Bedeutung ist die vorgesehene Einsetzung eines Europäischen Datenschutzbeauftragten. Aufgabe dieser neuen unabhängigen Gemeinschaftseinrichtung wäre es zu überwachen, ob die Organe und Einrichtungen der Gemeinschaft die datenschutzrechtlichen Vorschriften korrekt anwenden. Diese Einrichtung wäre vergleichbar mit den Kontrollstellen, die gemäß der Datenschutzrichtlinie in den Mitgliedstaaten bestehen. Die Bürgerinnen und Bürger könnten Beschwerden direkt an den Europäischen Datenschutzbeauftragten richten, wenn sie der Meinung sind, dass sie in ihren Rechten verletzt worden sind, die ihnen durch die Verordnung gewährt werden.

3.6 Zugang der Öffentlichkeit zu staatlichen Informationen

Was die Frage der Transparenz im Rahmen der Europäischen Union anbelangt, treffen auf der Ebene der Mitgliedstaaten zwei unterschiedliche Kulturen aufeinander. Dies kommt prägnant in einer Äußerung des ehemaligen Kommissionsmitglieds Joao de Deus Pinheira zum Ausdruck: „Es gibt in Europa zwei Tendenzen. Eine, die ich als napoleonisch bezeichnen würde, behandelt

alles als geheim, abgesehen von dem, was öffentlich ist. Für die andere dagegen ist alles öffentlich, bis auf einen sehr begrenzten Teil, der aus unterschiedlichen Gründen geheim gehalten werden muss." Dänemark, die Niederlande, Finnland und – seit über zwei Jahrhunderten – Schweden repräsentieren eine offene Verwaltungspraxis, während Belgien, Deutschland, Frankreich, Luxemburg und das Vereinigte Königreich den Kern einer geschlosseneren Verwaltungstradition bilden.

Die durch den Vertrag von Maastricht an den EGV angehängte Erklärung Nr. 17 zum Recht auf Zugang zu Informationen hatte keine Rechtswirkung. Dem unter Berufung auf diese Erklärung zwischen Rat und Kommission vereinbarten Verhaltenscodex wurde vom EuGH im Urteil Niederlande/Rat keine Rechtswirkung zugebilligt (EuGH vom 30. April 1996, Rs C-58/94, Slg. S. I 2169).

Die Rechtslage hat sich mit dem Amsterdamer Vertrag und dem In-Kraft-Treten des Artikels 255 EGV geändert. Dieser Artikel räumt jeder natürlichen oder juristischen Person mit Wohnsitz oder Sitz in einem Mitgliedstaat das Recht auf Zugang zu Dokumenten des Europäischen Parlaments, des Rates und der Kommission ein und erteilt dem Rat und dem Europäischen Parlament das Mandat, binnen zwei Jahren nach In-Kraft-Treten des Vertrages die allgemeinen Grundsätze für die Ausübung dieses Rechts auf Zugang sowie die Einschränkungen dieses Rechts aus Gründen des öffentlichen oder privaten Interesses festzulegen.

In diesem Zusammenhang hat die Europäische Kommission im Januar 1999 das Grünbuch „Informationen des öffentlichen Sektors – eine Schlüsselressource für Europa" verabschiedet. Der Wettbewerbsvorteil der USA gegenüber Europa bei den neuen Informations- und Kommunikationstechnologien ist nach Auffassung der Kommission auch deswegen entstanden, weil in den USA bereits 1966 im „Freedom of Information Act" der kostenlose (bzw. sehr preisgünstige) Zugang zu hoch entwickelten und leistungsfähigen Informationssystemen der öffentlichen Stellen garantiert wurde. Im Gegensatz zur Rechtslage in den meisten EU-Mitgliedstaaten können nach US-Recht grundsätzlich alle staatlichen Informationen und Akteninhalte von privaten Stellen abgefragt werden (eine Ausnahme bildet u. a. die nationale Sicherheit).

Die Europäische Kommission schlägt nicht vor, mehr Informationen zu sammeln, sondern die vorhandenen nicht vertraulichen Datenbestände zugänglicher, übersichtlicher und für potentielle Nutzer transparenter zu machen. Das Grünbuch ist über das Internet unter „http://www2.echo.lu/info2000/de/publicsector/gp-index.html" erhältlich. Darin kommt zum Ausdruck, dass der Zugang zu Informationen des öffentlichen Sektors mit einer ganzen Reihe von Fragen verknüpft ist, die sorgfältig geprüft werden müssen. Sie reichen von der Definition des Begriffs „Informationen des öffentlichen Sektors" bis hin zu Datenschutzfragen. So wird der öffentliche Sektor von Mitgliedstaat zu Mitgliedstaat unterschiedlich definiert. Die gesetzlichen Rahmenbestimmungen auf nationaler Ebene sehen Ausnahmen vom Zugangsrecht vor. Hier können vier Kategorien unterschieden werden:

- Ausnahmen im staatlichen Interesse (nationale Sicherheit, öffentliche Ordnung). Es handelt sich also um Fragen, die meist in die ausschließliche Zuständigkeit der Mitgliedstaaten fallen.
- Ausnahmen im Interesse Dritter (Schutz der Privatsphäre, Geschäftsgeheimnisse, Gerichtsverfahren usw.).
- Ausnahmen zum Schutz von Entscheidungsverfahren (vorläufige oder nur für den Dienstgebrauch bestimmte Informationen).
- Ausnahmen zur Vermeidung von unvertretbaren Kosten oder unvertretbarem Verwaltungsaufwand bei der betroffenen Dienststelle.

Die Realisierung des Rechts auf Informationen durch den Staat erfordert sicherlich eine neue Interpretation der „allgemein zugänglichen Quellen" in Art. 5 Abs. 1 Satz 2 des Grundgesetzes.

Zum Datenschutz wird in Kapitel III.7 Folgendes ausgeführt:

> „Bei einem Teil der Informationen des öffentlichen Sektors handelt es sich um personenbezogene Daten, d. h. um Angaben über eine bestimmte oder bestimmbare Person. Das gilt z. B. für Bevölkerungs-, Handels-, Kraftfahrzeug- oder Kreditregister sowie für medizinische, Beschäftigungs- und Sozialschutzdaten. Informationen dieser Art können für das Marketing, die Forschung oder sonstige Aktivitäten der Privatwirtschaft von Nutzen sein. In diesem Fall müssen das Informationsrecht der Bürger und der Unternehmen und das Recht des Einzelnen auf Schutz seiner Privatsphäre gegeneinander abgewogen werden. In allen einzelstaatlichen Zugangsregelungen hat man dem Rechnung getragen. (...) Die EG-Datenschutz-Richtlinie enthält verbindliche Regeln für den öffentlichen und den privaten Sektor und bringt den Grundsatz des freien Zugangs zu Informationen des öffentlichen Sektors mit dem Datenschutz in Einklang. Sie ist uneingeschränkt auf personenbezogene Daten, die von öffentlichen Stellen vorgehalten werden, anwendbar. Es ist Sache der jeweils für die Daten verantwortlichen öffentlichen Stellen, unter Berücksichtigung der in der EG-Datenschutz-Richtlinie niedergelegten Prinzipien, insbesondere des Prinzips der Zweckgebundenheit, die vereinbarte Abwägung vorzunehmen zwischen dem Grundsatz des offenen Zugangs für wirtschaftliche und sonstige Zwecke einerseits und dem Schutz der Privatsphäre andererseits. Ein Sonderfall sind statistische Daten. Auf diesem Gebiet verstärkt der allgemein anerkannte Grundsatz der statistischen Geheimhaltung den Schutz personenbezogener Daten. Das Statistikgeheimnis verhindert nicht nur den Zugriff privater Nutzer auf die Daten Dritter, sondern auch die Weitergabe vertraulicher Daten an Behörden, soweit es sich nicht um statistische Ämter handelt."

Der Schutz personenbezogener Daten wird in dem Dokument also nicht außer Acht gelassen, auch wenn diese Frage nicht im Mittelpunkt der Betrachtung steht. Jedenfalls wird deutlich, dass der Wandel zur Informationsgesellschaft auch in diesem Bereich neue Bedrohungen der Privatsphäre mit sich bringt, wenn eine Vielzahl amtlicher Register elektronisch (vor allem online und im Internet) zur Verfügung gestellt werden soll.

3.7 Entwurf einer Ratsentschließung zur Überwachung der Telekommunikation (ENFOPOL) vorerst gestoppt

Die Pläne des Rates der Europäischen Union sahen vor, dass die ermächtigten Behörden Teilnehmer von Fernmeldeverkehr und Internetkommunikation überwachen dürfen und die Diensteanbieter aufgrund abzuschließender Rechtshilfeabkommen zwecks EU-weitem Zugriff den Behörden die Daten inklusive Inhalt der Kommunikation, Dauer, Zeit und Partner entschlüsselt bereitstellen sollten.

Innerhalb der „dritten Säule“ des Maastrichter Vertrags wird die Zusammenarbeit der Justiz- und Innenminister geregelt. Hier beraten sich die Minister der Mitgliedstaaten im Rat und können einstimmig gemeinsame Maßnahmen verabschieden oder Abkommen zur Ratifizierung durch die Mitgliedstaaten empfehlen. Der Rat kann selbst keine rechtlich verbindlichen Beschlüsse abgeben, sondern nur Empfehlungen aussprechen.

Da die Innen- und Justizpolitik die Souveränität der Mitgliedstaaten berührt, werden alle relevanten Entscheidungen von den Staaten selbst getroffen. Dies hindert sie jedoch nicht daran, innerhalb der dritten Säule Entscheidungen vorzubereiten und im Rahmen multilateraler Verträge zu kooperieren.

Arbeitsgruppen dienen der Vorbereitung politischer Entscheidungen in den einzelnen Mitgliedstaaten. Von der Arbeitsgruppe K 4 „Polizeiliche Zusammenarbeit“ wurden Abhörpläne für den Bereich der EU erarbeitet. In Englisch trägt die Gruppe die Bezeichnung „Enforcement Police“. Alle Dokumente dieser Gruppe tragen daher das Registerzeichen ENFOPOL. Die Gruppe beschäftigt sich nicht nur mit dem Abhören von Telekommunikation, sondern beispielsweise auch mit Rowdytum bei Großveranstaltungen oder technischen Standards für Polizeitechnik.

In diese Arbeitsgruppe gehen Papiere aus anderen informellen Arbeitsgruppen wie dem International Law Enforcement Telecommunications (ILETS) Seminar ein. Bedienstete der nationalen Polizeien, nicht nur von EU-Mitgliedstaaten, sondern auch der USA und Kanadas erarbeiten im ILETS gemeinsame Vorschläge und technische Richtlinien oder legen Standards fest. ILETS erarbeitete u. a. die International User Requirements (IUR) zum Abhören von Telekommunikation.

Die Ergebnisse der Arbeitsgruppen werden in so genannte Lenkungsgruppen eingebracht. Es gibt drei Lenkungsgruppen für die Bereiche Asyl, Polizei und Justiz. Diese Gruppen bereiten die Papiere für den „K-4-Ausschuss“ vor, der nach dem Artikel 4 des Maastrichter Vertrags benannt ist. Er koordiniert auf Staatssekretärsebene die Zusammenarbeit der nationalen Innen- und Justizressorts und fungiert als Vorstufe für die Beschlüsse der Minister. Die flexible Strukturierung der EU-Arbeitsgruppen innerhalb der dritten Säule ermöglicht eine effektive Zusammenarbeit innerhalb eines Fachgebiets. Ratsempfehlungen haben daher, auch wenn sie rechtlich nicht bindend sind, Signalwirkung und werden als europäische Legitimation nationaler Gesetzesanpassungen benutzt. So ist die allmähliche Vereinheitlichung der Gesetzgebung in den einzelnen Mitgliedstaaten und das politische Zusammenwachsen der Europäischen Union auch Ziel des Amsterdamer Vertrages.

Der Ratsbeschluss zur Überwachung der Telekommunikation sollte bis zum 27. Mai 1999 gefasst werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in ihrer Entschließung vom 26. März 1999 kritisiert, dass der Entwurf geheim gehalten und ohne Einbeziehung der Datenschutzbeauftragten beraten wurde. Sie hat die Bundesregierung aufgefordert, der Schaffung gemeinsamer Standards zur grenzüberschreitenden Überwachung der Telekommunikation nur insoweit zuzustimmen, als damit nicht zusätzliche Eingriffe in das Recht auf unbeobachtete Kommunikation und das Fernmeldegeheimnis verbunden sind und die Nutzung datenschutzfreundlicher Technologien nicht konterkariert wird (vgl. Anlage 15). Aufgrund der vielfältigen Proteste (u. a. auch von Provider-Verbänden) wurde die EU-Gesetzesinitiative nunmehr auf Eis gelegt.

4. Meldewesen

4.1 EWOISneu

Die Bemühungen, für das rheinland-pfälzische Einwohnermeldeverfahren eine neue technische Grundlage zu schaffen, sind im Berichtszeitraum einen entscheidenden Schritt vorangekommen. Das neue Verfahren stützt sich nicht mehr ausschließlich auf eine zentrale Verarbeitung der Meldedaten durch das DIZ, sondern berücksichtigt in einem dezentralen Teil die funktionalen Anforderungen nach dem Meldegesetz, indem es die Städte und Verbandsgemeinden in die Lage versetzt, ihre Einwohnerdaten selbst zu verarbeiten. Es existiert freilich auch weiterhin ein zentrales Register mit den Meldedaten aller Einwohner des Landes. Dieses zentrale Register bildet die Datenbasis für regionale und überregionale Melderegisterzugriffe anderer Behörden. Zugleich unterstützt dieser zentrale Teil die Arbeit der Meldebehörden, indem er Meldedaten in solchen Fällen bereitstellt, in denen Einwohnerdaten aus dem Zuständigkeitsbereich einer anderen Meldebehörde übernommen werden können (z. B. bei Umzug). Die Aktualisierung des zentralen Teils erfolgt in der Weise, dass dezentral verarbeitete Änderungen des Melderegisters im automatisierten Verfahren übergeben werden.

EWOIS existiert seit fast dreißig Jahren. Es beruht auf einem Programmsystem, das in seinen Grundzügen vor dem Jahr 1971 entwickelt und in der Folgezeit mit erheblichem Aufwand ergänzt und – soweit dies möglich war – den veränderten Anforderungen angepasst wurde. Es ist freilich nie vollständig gelungen, EWOIS inhaltlich und formal so zu organisieren, dass den Datenschutz-

anforderungen des Meldegesetzes in vollem Umfange entsprochen wird. Die Datenschutzkommission und der LfD haben hierauf in früheren Tätigkeitsberichten immer wieder hingewiesen (z. B. 12. Tb. Tz., 4.1, 13. Tb., Tz. 4.1). Es fehlte beispielsweise auch an normenklaren gesetzlichen Grundlagen für den automatisierten Abruf von Meldedaten aus dem zentralen Landesbestand (vgl. unten Tz. 4.1.1).

Vom Ministerium des Innern und für Sport wurde zutreffend immer wieder darauf hingewiesen, dass das existierende landeseinheitliche Verfahren für den Datenschutz auch Vorteile hat. Hierzu gehören die strenge Standardisierung und Typisierung der Verarbeitung, die es nicht zulassen, dass einzelne Meldebehörden abweichende, vom Meldegesetz nicht gedeckte Verarbeitungsformen oder Übermittlungsverfahren anwenden. Das landeseinheitliche Verfahren EWOIS ermöglichte es, auch Datenschutzprobleme landeseinheitlich zu lösen. In einer Gesamtbeurteilung von EWOIS dürfen auch solche Gesichtspunkte nicht unbeachtet bleiben.

Die Konzeption von EWOISneu, die auf zentralen und dezentralen Verfahrensteilen beruht, birgt die Gefahr, dass die aus der Sicht des Datenschutzes nachteiligen Effekte einer dezentralen Verarbeitung eintreten, zugleich aber auch die schon in der Vergangenheit beklagten Mängel des landeseinheitlichen Verfahrens erhalten bleiben. Erfreulicherweise ist der LfD in die Verfahrensentwicklung eingebunden. Er wird alles daransetzen, eine Verschlechterung des Datenschutzes im Bereich des Meldewesens zu verhindern.

4.1.1 Gesetzliche Grundlagen von EWOIS und Folgerungen für EWOISneu

EWOIS ermöglicht es, dass staatliche Stellen, z. B. die Polizei, auf den gesamten Meldedatenbestand des Landes in Online-Verfahren direkt zugreifen können. Diese Zugriffsmöglichkeit besteht inhaltlich differenziert auch für alle Meldebehörden und eine Vielzahl anderer Behörden des Landes.

In der Vergangenheit wurden solche Zugriffe, soweit sie durch Dritte erfolgten, als automatisierte Datenübermittlungen qualifiziert. Es war freilich bekannt, dass Regelungsdefizite bestehen, und zwar sowohl in Bezug auf Meldebehörden, denn § 38 MG betrifft nur Fälle der gleichzeitigen Zuständigkeit (insbesondere Nebenwohnungen), als auch auf andere Behörden, denen die Zugriffsmöglichkeit auf Meldedaten außerhalb ihres Zuständigkeitsbereichs eröffnet ist.

Das Kernproblem besteht darin, dass ein automatisiertes Datenübermittlungsverfahren die Datenweitergabe zwischen zwei „bestimmten“ Stellen betrifft. Es ist für solche Verfahren charakteristisch, dass die Datenübermittlung ohne Mitwirkung der übermittelnden Stelle erfolgt; vorausgesetzt ist aber, dass die übermittelnde Stelle bekannt ist. Der Fall, dass Daten vieler Stellen in einem gemeinsamen Datenbestand zusammengefasst und im Rahmen einer Recherche genutzt werden, ist von den gesetzlichen Regelungen der automatisierten Datenübermittlung nicht umfasst. Beim Zugriff auf einen gemeinsamen Datenbestand weiß die empfangende Stelle oft erst nach Abschluss des Übermittlungsvorganges, wer speichernde Stelle ist. Die Verhältnismäßigkeitsprüfung vor der Einrichtung eines automatisierten Übermittlungsverfahrens setzt aber grundsätzlich voraus, dass die Interaktionspartner bekannt sind.

Gegen diese Beurteilung kann eingewandt werden, dass die Eröffnung des Zugriffs auf einen gemeinsamen Datenbestand datenschutzrechtlich als eine Vielzahl automatisierter Übermittlungsverfahren anzusehen ist. Auch bei dieser Sichtweise kann aber nicht bestritten werden, dass der Abruf aus einem gemeinsamen Datenbestand unter Datenschutzgesichtspunkten eine andere Qualität hat, weil er dem Übermittlungsempfänger die aufwendige Einzelrecherche in den Datenbeständen der speichernden Stellen – im Meldebereich des Landes sind dies mehr als 200 – erspart. Die Vereinfachung des Datenzugriffs durch die Datenverarbeitungstechnik bewirkt eine höhere Gefährdung der Datenschutzrechte.

Es ist auch zu berücksichtigen, dass spezielle Datenschutzprobleme, wie sie zum Beispiel bei der Übermittlung von Auskunftssperren oder der melderechtlichen Behandlung von Adoptionen aufgetreten sind, eng mit diesen Besonderheiten des rheinland-pfälzischen Verfahrens zusammenhängen.

Bei einer Gesamtbetrachtung der Verhältnismäßigkeit des Verfahrens ist zu berücksichtigen, dass Datenabrufe – und damit auch der Missbrauch personenbezogener Daten – erleichtert werden. Wie auch in anderen Fällen der Risikoerhöhung durch die Anwendung neuer Datenverarbeitungstechniken – beispielsweise maschinenlesbarer Personalausweis – ist deshalb zu fordern, dass die Frage nach der Verhältnismäßigkeit des Verfahrens durch den Gesetzgeber beantwortet wird. Aber auch die Anforderungen an die Normenklarheit gesetzlicher Eingriffsgrundlagen i. V. m. der Tatsache, dass in dem Zugriff auf einen gemeinsamen Datenbestand, wie oben dargelegt, ein Aliud zur automatisierten Datenübermittlung zu sehen ist, gebieten es, eine Entscheidung des Gesetzgebers herbeizuführen.

Im Ergebnis verschließt sich der LfD nicht der Realisierung einer verteilten Datenverarbeitung in der beschriebenen Weise, er hält es aber für geboten, dass die Gesetzeslage sowie die gegenwärtige und die künftige Praxis der Meldedatenverarbeitung zur Übereinstimmung gebracht werden. §§ 37 und 38 MG sind diesbezüglich weder normenklar, noch inhaltlich ausreichend.

4.1.2 Löschung und Aufbewahrung von Daten

§ 11 MG regelt detailliert die Löschung und Aufbewahrung von Daten. Die Praxis der Meldedatenverarbeitung in EWOIS stimmt mit diesen gesetzlichen Vorgaben nicht überein. Die Datenschutzkommission hat hierauf bereits in ihrem 9. und 11. Tb. – Drs. 10/270, 11/710 – hingewiesen. Es gehört selbstverständlich zu den Grundanforderungen an EWOISneu, dass solche Abweichungen vermieden werden.

Die nach Melderecht gebotenen Löschungen/Sperrungen und Archivierungen sollten, soweit sie an bestimmte Fristen (z. B. § 11 Abs. 3 MG) oder Ereignisse (Wegzug, Tod) gebunden sind, automatisiert erfolgen. Über das „Mitteilungssystem“ sind im Rahmen der Konsolidierung entsprechende Informationen in etwaige weitere, dezentral gespeicherte Datensätze zu übernehmen.

4.1.3 Meldedatensatz

§ 3 Abs. 2 Nr. 9 MG lässt zu, dass für die Mitwirkung bei der Erhebung von Abfallbeseitigungsgebühren die Tatsache der Zugehörigkeit zu einem bestimmten Haushalt im Sinne des Abfallbeseitigungsrechts gespeichert wird. Diese Daten dürfen nach § 4 MeldDÜVO an die zuständige Kreisverwaltung übermittelt werden. Tatsächlich ist der Meldebehörde die Zugehörigkeit zu einem Haushalt im Sinne des Abfallbeseitigungsrechts nicht bekannt. Gespeichert und übermittelt wird die Zugehörigkeit zu einem Familienverband, dem andere Kriterien zugrunde liegen. Der LfD empfiehlt, das Meldegesetz in diesem Punkt zu ändern und an die bestehende Praxis anzupassen.

4.1.4 Auskunftssperren

EWOIS lässt gegenwärtig nicht zu, dass alle nach dem MG möglichen Auskunftssperren einzeln im Meldedatensatz gespeichert werden. Die Praxis behilft sich mit Gruppenbildungen; die Darstellung beliebiger Kombinationen von Auskunftssperren im Meldedatensatz ist nicht möglich. Dieses Problem müsste in EWOISneu gelöst werden.

4.2 Erklärung über steuerliches Getrenntleben

Nach § 3 Abs. 2 Nr. 2 MG erheben Meldebehörden für die Mitwirkung bei der Ausstellung von Lohnsteuerkarten Daten über das dauernde Getrenntleben von Ehegatten.

Nach der Rechtsprechung des BFH leben Ehegatten dauernd getrennt i. S. v. § 26 Abs. 1 EStG, wenn die zum Wesen der Ehe gehörende Lebens- und Wirtschaftsgemeinschaft nach dem Gesamtbild der Verhältnisse nicht mehr besteht. Demzufolge wäre es unbedenklich, wenn in den Vordrucken der Meldebehörden nach dem Bestehen einer Lebens- und Wirtschaftsgemeinschaft gefragt würde. Unbedenklich wäre es auch, wenn diese Begriffe verdeutlicht würden, sofern diese Verdeutlichung an Lebenssachverhalte anknüpft, die Außenbezug haben.

Feststellungen in mehreren Fällen ergaben, dass die Meldebehörden für die Datenerhebung Vordrucke verwenden, in denen von den Betroffenen u. a. zu bestätigen ist, dass sich die Trennung „auf das eheliche Leben, den Haushalt und die Wirtschaftsführung“ erstreckt. Aus der Aufzählung wird deutlich, dass mit dem ehelichen Leben weder die Haushaltsführung noch die Wirtschaftsführung gemeint sein können. Der Begriff ist auch nicht synonym zur Lebensgemeinschaft, denn in einer Lebensgemeinschaft können auch solche Personen zusammenleben, die nicht verheiratet sind. Zu den vom BFH genannten Kriterien (Bestehen einer Ehe – als Rechtsform –, Lebens- und Wirtschaftsgemeinschaft) bildet das „eheliche Leben“ ein Aliud.

Der Begriff des ehelichen Lebens bezieht sich auf den unantastbaren Bereich privater Lebensgestaltung, der von Natur aus Geheimnischarakter hat und in den der Staat nicht eindringen darf (BVerfGE 27, 1,7).

Das Ministerium des Innern und für Sport und das Ministerium der Finanzen haben diese Rechtsauffassung anerkannt. Die Meldebehörden wurden aufgefordert, die Frage nach dem „ehelichen Leben“ künftig zu unterlassen.

4.3 Vorsicht bei Müllgebühren

Gelegentlich können Datenschutzprobleme für Bürger recht kostspielig sein. Die Wahrscheinlichkeit, dass zu viel Müllgebühren gezahlt werden, ist groß, wenn Personen in einem Haushalt zusammenleben und nicht verheiratet oder in einem Eltern-Kind-Verhältnis miteinander verbunden sind.

Einwohnerbezogene Müllabfuhrgebühren sind üblicherweise nach der Haushaltsgröße gestaffelt. Leben mehrere Personen in einem Haushalt zusammen, so ist die Gebühr zwar höher als die eines Einpersonenhaushalts. Wird jede der zu dem Haushalt gehörenden Personen aber einzeln veranlagt, so ist das für die Betroffenen in der Summe viel teurer als die Veranlagung in einem Mehrpersonenhaushalt.

Die Festsetzung der Müllabfuhrgebühren obliegt den Landkreisen und kreisfreien Städten. Diese können von den Meldeämtern nur dann erfahren, dass mehrere Personen in einem Haushalt zusammenleben, wenn es sich um Eheleute handelt oder wenn Kinder bei den Eltern oder einem Elternteil leben. Personen, die in einer anderen Wohngemeinschaft zusammenleben, werden als mehrere Einpersonenhaushalte gemeldet und, sofern den für die Festsetzung der Müllabfuhrgebühren zuständigen Behörden nichts anderes bekannt wird, als Einpersonenhaushalte veranlagt. Ursache hierfür ist, dass der Haushaltsbegriff des Melderechts nicht mit dem Haushaltsbegriff im abfallrechtlichen Sinne übereinstimmt. § 3 Abs. 2 Nr. 9 MG bestimmt zwar, dass für die Mitwirkung bei der Erhebung von Abfallbeseitigungsgebühren die Tatsache der Zugehörigkeit zu einem bestimmten Haushalt im Sinne des Abfallbeseitigungsrechts gespeichert werden darf; tatsächlich verfügen Meldebehörden aber nicht über solche Angaben und können sie deshalb auch nicht an die Abfallbehörden übermitteln, was zur Folge hat, dass Veranlagungsfehler vorkommen.

Betroffene Mieter bemerken diese Fehler häufig nicht, weil der Müllabfuhrgebührenbescheid dem Hauseigentümer zugestellt wird. Dieser berücksichtigt die Müllabfuhrgebühren zwar in seiner Nebenkostenabrechnung. Nur in den seltensten Fällen dürfte diese Abrechnung indessen ausweisen, dass Gebühren für mehrere Haushalte berechnet wurden, obwohl Personen in einer Haushaltsgemeinschaft zusammenleben. Für die Mieter ist der Veranlagungsfehler nur dann erkennbar, wenn sie die Nebenkostenabrechnung überprüfen und sich den Gebührenbescheid vorlegen lassen.

Die Abfallbeseitigungsbehörden können gebührenmindernde Umstände – wie das Zusammenleben in einer Wohngemeinschaft – nur dann bei der Gebührenveranlagung berücksichtigen, wenn sie ihnen von den Betroffenen mitgeteilt werden. Alle Bürgerinnen und Bürger haben nach den Bestimmungen des Landesdatenschutzgesetzes das Recht, bei den zuständigen Behörden (Landkreise, kreisfreie Städte) zu erfragen, ob sie als Einpersonenhaushalt oder Mehrpersonenhaushalt veranlagt werden, und können erforderlichenfalls eine Berichtigung verlangen. Die Wahrnehmung dieser Datenschutzrechte kann zu erheblichen Gebühreneinsparungen führen.

Der LfD hat sich im Berichtszeitraum durch Einschaltung des Ministeriums des Innern und für Sport sowie des Landkreis- und des Städtetages Rheinland-Pfalz bemüht, eine Lösung des Problems herbeizuführen, die es nicht ausschließlich der Initiative der Mieter überantwortet, dass richtig veranlagt wird. Eine solche Lösung konnte nicht gefunden werden. Das Verfahren EWOIS lässt es technisch gar nicht zu, dass der Familienverband im abfallrechtlichen Sinne gespeichert wird. Außerdem ist dies kein Merkmal, das nach der Meldeverordnung erhoben wird. Folglich werden in einer Vielzahl von Fällen Daten übermittelt, die zu einer unrichtigen Veranlagung führen. Die Städte und Landkreise erfahren dies nur dann, wenn sie vom Vermieter als Abgabenschuldner oder von den Mietern informiert werden.

Die Abfallbeseitigungsbehörden sollten regelmäßig und in geeigneter Form auf die Möglichkeit zur Kosteneinsparung durch Berichtigung der Veranlagungsgrundlage hinweisen.

4.4 Meldescheine von Beherbergungsstätten

Wer als Gast in einer Beherbergungsstätte für nicht länger als zwei Monate aufgenommen wird, unterliegt nach § 26 MG zwar nicht der Meldepflicht; er muss am Tage der Ankunft aber einen besonderen Meldeschein ausfüllen und unterschreiben. Nach § 27 MG muss der Meldeschein für die Polizeidienststellen zur Einsichtnahme oder Abholung bereitgehalten oder, auf Verlangen, an diese übermittelt werden.

§ 3 MVO schreibt vor, dass als Meldeschein ein ganz bestimmter Vordruck (Muster Anlage 6 MVO) verwendet wird. Das Ministerium des Innern und für Sport kann andere Vordrucke mit anderem Format und anderer Anordnung der Angaben zulassen, soweit diese inhaltlich dem Muster der Anlage 6 entsprechen. Die Meldescheine sind in einfacher Ausfertigung auszufüllen; in Gemeinden, in denen ein Kurbeitrag nach § 12 Abs. 2 KAG erhoben wird, kann eine weitere Ausfertigung verlangt werden.

Den Interessen von Kurgemeinden ist mit diesen Regelungen nicht entsprochen. Sie wollen die Kurkarte so in den Meldeschein integrieren, dass sie vom Gast oder Gastgeber in einem Arbeitsgang ausgefüllt, der Gemeinde vorgelegt, abgetrennt und an den Berechtigten zurückgegeben werden kann. Außerdem benötigen die Kurgemeinden aufgrund ihrer Satzung über die Erhebung des Kurbeitrags nicht selten ergänzende Angaben (z. B. Geburtsjahr der mitangemeldeten Kinder), die sie unter Verwendung des Meldescheins erheben wollen. Für ihre Statistik (Erfolgskontrolle) wünschen Kurgemeinden und Fremdenverkehrsgemeinden freiwillige Angaben über die Wirksamkeit von Werbemitteln, über die für die Anreise genutzten Verkehrsmittel und über den Reisezweck (Kur, Geschäftsreise usw.). Weil dies alles nach den gesetzlichen Vorschriften nicht zulässig ist, fordern die betroffenen Städte und Gemeinden mit Nachdruck, die Meldeverordnung so zu ändern, dass die Meldescheine für die genannten Zwecke und in der beschriebenen Weise genutzt werden können.

Datenschutzgründe stehen einer solchen Änderung nicht entgegen. Dies gilt bei Beachtung des Landesstatistikgesetzes auch für die Erhebung von Statistikangaben auf freiwilliger Grundlage.

4.5 Übermittlung von Meldedaten an politische Parteien

Nach § 35 Abs. 1 MG darf die Meldebehörde (Stadt- und Verbandsgemeindeverwaltung) Parteien, Wählergruppen und anderen Trägern von Wahlvorschlägen im Zusammenhang mit Parlaments-, Kommunal- und Ausländerbeiratswahlen in den sechs der Wahl vorangehenden Monaten eine einfache Melderegisterauskunft (Vor- und Familiennamen, Doktorgrad, Anschriften) über Gruppen von Wahlberechtigten erteilen, soweit für deren Zusammensetzung das Lebensalter bestimmend ist. Eine weitere Voraussetzung für die Datenübermittlung ist, dass die Betroffenen nicht widersprochen haben.

4.5.1 Nutzung des Melderegisters für Zwecke der persönlichen Ansprache von EU-Ausländerinnen und -Ausländern

Nach dieser Vorschrift ist eine andere Gruppenbildung – etwa unter Verwendung des Merkmals „EU-Ausländer“ – unzulässig. Nur bei Ausländerbeiratswahlen ergibt sich eine Besonderheit insoweit, als nur Ausländer wahlberechtigt sind. Die Gruppe der Wahlberechtigten umfasst hier also nur Ausländer. Eine Eingrenzung auf „EU-Ausländer“ wäre aber auch hier unzulässig.

Das Ministerium des Innern und für Sport hat diese Rechtsauffassung in seinem Rundschreiben vom 17. März 1999 –Az.: 31519 535-1 – bestätigt. In diesem Rundschreiben wird auf das Urteil des Verwaltungsgerichts Darmstadt vom 30. November 1998 verwiesen, das wegen einer vergleichbaren Rechtslage nach dem Hessischen Meldegesetz durchaus als Auslegungshilfe herangezogen werden kann. Das Gericht hält eine Auswertung der Melderegister unter Berücksichtigung des Merkmals „Staatsangehörigkeit" für unzulässig. Eine derartige Nutzung würde gerade den Zielen der Neuregelung des Kommunalwahlrechts, nämlich der Gleichstellung der EU-Bürger mit Bundesbürgern in den Kommunen, widersprechen. Der Grundsatz der freien und gleichen Wahl bedeute insoweit auch, die Wahlberechtigten einer gleichen Behandlung zuzuführen bzw. deren Daten gleich zu behandeln.

Im Ergebnis, so das Ministerium, ist danach weder die Erteilung von Auskünften über wahlberechtigte EU-Ausländerinnen und -Ausländer an Parteien oder sonstige Träger von Wahlvorschlägen noch die Auswertung der Melderegister zum Zwecke der persönlichen Ansprache mit Wahlwerbebriefen einzelner Träger von Wahlvorschlägen zulässig.

4.5.2 Beschränkung der Auskunft auf bestimmte Altersgruppen

§ 35 Abs. 1 MG erlaubt eine Datenübermittlung an politische Parteien nur unter der Voraussetzung, dass die Anfrage von vornherein auf einzelne Altersgruppen beschränkt ist. Eine Partei versuchte dies dadurch zu umgehen, dass sie von einer Verbandsgemeinde eine Liste aller Erstwähler, aller Senioren ab 60 Jahre sowie aller sonstigen Wähler anforderte. Im Ergebnis würden damit die Anschriften aller Wahlberechtigten übermittelt. Der Gesetzgeber wollte politischen Parteien, Wählergruppen und anderen Trägern von Wahlvorschlägen jedoch lediglich das gezielte Ansprechen bestimmter Altergruppen ermöglichen, ansonsten hätte es der Einschränkung auf dieses Auswahlkriterium nicht bedurft. Die Auskunft konnte daher nur in entsprechend reduzierter Form erteilt werden.

4.5.3 Widerspruchs- oder Einwilligungslösung?

Die Weitergabe von Meldedaten an politische Parteien hängt ebenso wie die Weitergabe an Adressbuchverlage davon ab, dass der Betroffene nicht widersprochen hat. Die Meldebehörde hat auf diese Widerspruchsmöglichkeit bei der Anmeldung sowie mindestens einmal jährlich durch öffentliche Bekanntmachung hinzuweisen. Wie die sich insbesondere vor Wahlen häufende Zahl der Beschwerden von Bürgern über persönlich an sie adressierte Wahlwerbung zeigt, ist dieses Recht dennoch weitgehend unbekannt. Datenschutzfreundlicher ist indessen eine Einwilligungslösung, bei der eine Übermittlung nur bei vorherigem Einverständnis des Betroffenen zulässig ist. Für die Datenweitergabe an Adressbuchverlage ist diese „Einwilligungslösung" zwischenzeitlich in den Meldegesetzen des Saarlandes und Nordrhein-Westfalens eingeführt worden. Die 56. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 5./6. Oktober 1998 (vgl. Anlage 9) hat den gesetzgebenden Körperschaften in einer Entschließung empfohlen, bei der Weitergabe von Meldedaten an Adressbuchverlage und an politische Parteien künftig die Einwilligungslösung vorzusehen. Der LfD wird sich bei der nächsten Novellierung des Meldegesetzes hierfür einsetzen.

4.6 Erteilung von Melderegisterauskünften durch die Wegzugsbehörde

Unter Tz. 4.4 des 16. Tb. berichtete der LfD über Gefährdungen des Datenschutzes, die bei der Erteilung von Melderegisterauskünften durch die Wegzugsbehörde entstehen können. Da nicht in allen Ländern die gesetzliche Verpflichtung besteht, Auskunftssperren – insbesondere bei einer Gefahr für Leben, Gesundheit, persönliche Freiheit oder ähnliche schutzwürdige Belange (§ 21 Abs. 5 MRRG) – im Rahmen der Rückmeldung (§ 17 MRRG) mitzuteilen, ist nicht auszuschließen, dass die Wegzugsbehörde in Unkenntnis Auskunft über eine außerordentlich schutzbedürftige aktuelle Anschrift erteilt. Im Übrigen ist keineswegs sichergestellt, dass eine Auskunftssperre wegen einer Gefahr für Leben, Gesundheit usw. auch dann noch der Wegzugsbehörde mitgeteilt und von dieser berücksichtigt wird, wenn seit dem Umzug längere Zeit vergangen ist.

Die Melderechtsreferenten der Länder erzielten im Unterausschuss „Melde-, Pass- und Personalausweiswesen" Einvernehmen darüber, dass es den Betroffenen zuzumuten sei, sich selbst beim Vorliegen der Voraussetzungen für eine Auskunftssperre um einen umfassenden Schutz zu kümmern, indem sie die Auskunftssperre auch bei früher zuständigen Meldebehörden beantragen.

Der LfD trat dieser Argumentation entgegen. Er verwies auf die staatliche Verpflichtung, ein für den Bürger weitgehend undurchsichtiges und unverständliches staatliches Verwaltungsverfahren so zu organisieren, dass schwer wiegende Beeinträchtigungen schutzwürdiger Belange zuverlässig ausgeschlossen sind. In der rechtlichen Beurteilung des vorgeschlagenen Verfahrens ist zu berücksichtigen, dass die Wegzugsbehörde nicht mehr die zuständige Meldebehörde ist. Sie soll aber über einen Antrag des Betroffenen entscheiden und es ist keineswegs sichergestellt, dass sie in der Würdigung der Antragsbegründung der örtlich zuständigen Meldebehörde folgt. M. a. W.: Sie kann einen Antrag ablehnen und ohne Rücksicht auf eine am Zuzugsort eingetragene Auskunftssperre Melderegisterauskünfte erteilen. In einem dem LfD bekannt gewordenen Falle ist dies auch geschehen, weil die früher zuständige rheinland-pfälzische Meldebehörde meinte, die Antragsgründe hinsichtlich ihres Wahrheitsgehalts besser beurteilen zu können als die Zuzugsbehörde. Es stellt sich die Frage, welche Rechtsschutzmöglichkeiten ein Betroffener hat, wenn die früher zuständige Meldebehörde eine Auskunft in Unkenntnis der Sperrungsvoraussetzungen erteilt oder wenn sie einen Antrag auf Sperrung ablehnt. Wird die Entscheidung über einen Antrag als Verwaltungsakt qualifiziert, stellt sich auch die Frage, ob ein solcher von der Wegzugsbehörde überhaupt erlassen werden darf.

Eine unter Datenschutzgesichtspunkten zufrieden stellende Lösung setzt Gesetzesänderungen in den Ländern voraus, deren Meldegesetze keine Verpflichtung zur Mitteilung von Auskunftssperren enthalten (Baden-Württemberg, Berlin und Sachsen). Die rheinland-pfälzischen Meldebehörden wurden vom Ministerium des Innern und für Sport im Vorgriff auf die Gefährdungs-

möglichkeiten hingewiesen und gebeten, die für die vorherige Wohnung und den für weitere Wohnungen zuständigen Meldebehörden über Auskunftssperren wegen einer Gefahr für Leben, Gesundheit, persönliche Freiheit oder ähnliche schutzwürdige Belange auch dann zu unterrichten, wenn die Eintragung der Auskunftssperre nicht bei der Anmeldung erfolgt (Rundschreiben vom 3. Juli 1998; Az.: 315/19 534-11). Auskunftsersuchen über Personen, die nach Baden-Württemberg, Berlin oder Sachsen verzogen sind, sollen an die für die aktuelle Wohnung zuständige Meldebehörde weitergeleitet werden. Dies gilt auch für Auskunftsersuchen über Personen, die vor mehr als drei Jahren weggezogen sind.

4.7 Meldedaten von Transsexuellen

Durch Eingaben erhielt der LfD Kenntnis von der unzureichenden Sicherung der Daten von Transsexuellen im Melderegister. Weil die Einwohnerdaten mit dem Hinweis „Auskunftssperre“ und der Ergänzung „ts“ für Transsexuelle auf den Bildschirmen angezeigt wurden, erhielten alle Meldebehörden, Polizeibehörden, Bußgeldstellen, Kreisverwaltung (Abfallbeseitigung) und Kfz-Zulassungsstellen im Rahmen des Online-Zugriffs Kenntnis von diesem durch § 5 TSG besonders geschützten Merkmal (16. Tb., Tz. 4.5).

Da sich eine den gesetzlichen Anforderungen entsprechende Verfahrensänderung immer wieder verzögerte – Ursache waren technische Probleme bei der notwendigen Änderung von Suchtabellen – wies der LfD mit allem Nachdruck darauf hin, dass der mit einer technischen Umstellung verbundene Aufwand die Beibehaltung des gesetzwidrigen Zugriffsverfahrens nicht rechtfertigen könne.

Auf Verlangen des LfD wurde das Verfahren geändert (Rundschreiben des Ministeriums des Innern und für Sport vom 16. Februar 1999, Az.: 315/19 537-5). Die Übermittlungsempfänger erhalten nur noch Meldedaten, die das Merkmal „transsexuell“ nicht mehr enthalten.

4.8 Auskunftssperre nur für Volljährige?

Eine Verbandsgemeinde lehnte die Eintragung einer Auskunftssperre für Adressbuchverlage eines Minderjährigen mit dem Verweis auf § 35 Abs. 4 MG ab. Diese Norm besagt jedoch lediglich, dass an Adressbuchverlage eine einfache Melderegisterauskunft über sämtliche Einwohner, die das 18. Lebensjahr vollendet haben, erteilt werden darf, sofern die Betroffenen nicht widersprochen haben. Die vorherige Ausübung des Grundrechts ist nach Auffassung des LfD hierdurch nicht ausgeschlossen. Die Verbandsgemeinde schloss sich dem an; sie wird künftig auch Widersprüche beachten, die von Jugendlichen im Hinblick auf die Vollendung ihres 18. Geburtstages eingelegt werden.

4.9 Alters- und Ehejubiläen

Nach § 35 Abs. 3 MG können Einwohner der Auskunftserteilung aus dem Melderegister über Alters- oder Ehejubiläen von Einwohnern widersprechen. Die Daten dürfen dann weder im Rahmen von Einzelauskünften noch listenmäßig an Privatpersonen, an die Presse, an Mandatsträger oder andere private Interessenten übermittelt werden.

Aus unterschiedlichen Gründen werden an Stellen innerhalb des öffentlichen Bereichs listenmäßig oder in einer anderen Form zusammengefasste Einwohnerdaten übermittelt, die, weil sie beispielsweise das Geburtsdatum umfassen, gleichfalls Fälle von Altersjubiläen erkennen lassen. Eine Rechtsgrundlage hierfür ist § 8 MeldDÜVO, der die Datenweitergabe an die Kreisverwaltung und an die Ortsgemeinden regelt. Die Ausübung des Widerspruchsrechts nach § 35 Abs. 3 MG hindert in diesen Fällen nicht die Datenübermittlung, die Übermittlungsempfänger werden aber darauf hingewiesen, dass im Melderegister ein Widerspruch eingetragen ist. Sie können dann selbst Glückwünsche aussprechen oder an die Jubilare übermitteln, dürfen aber selbstverständlich ihrerseits nicht das tun, was der Meldebehörde verwehrt ist, nämlich die Presse über das Jubiläum informieren oder Jubiläumsdaten an Dritte weitergeben. Offensichtlich bereiten Glückwünsche des Bürgermeisters, des Landrats oder des Ortsvorstehers in Fällen, in denen das Widerspruchsrecht ausgeübt wurde, nicht immer nur Freude, denn gelegentlich beschweren sich die Betroffenen oder fragen beim LfD an, ob sie sich „dieses Eindringen in ihre Privatsphäre“ gefallen lassen müssen.

Anders lag der Fall eines Altersjubilars, dem, weil er sein Widerspruchsrecht nach § 35 Abs. 3 MG ausgeübt hatte, zwar nicht in der Tageszeitung gratuliert wurde – das Meldeamt hatte keine Daten an die Presse übermittelt – , der aber einen Hinweis auf seinen Geburtstag im Gemeindeblatt fand. Die Veröffentlichung war von einem Ortsvorsteher, der den Hinweis auf den ausgeübten Widerspruch übersehen hatte, veranlasst worden. Die Veröffentlichung war ärgerlich für den Betroffen und – vermutlich – für den Ortsvorsteher, denn der LfD beanstandete diesen Verstoß gegen datenschutzrechtliche Vorschriften.

4.10 Namensverwechslungen

Mit – unschöner – Regelmäßigkeit enthalten die Tätigkeitsberichte des LfD Beiträge über Namensverwechslungen (vgl. 11. Tb. Tz. 6.1.2, 13. Tb. Tz. 4.6, 15. Tb. Tz. 4.7), die für die Betroffenen günstigstenfalls „nur“ ärgerlich, gelegentlich aber auch geschäftsschädigend oder mit noch weiter gehenden Beeinträchtigungen ihrer schutzwürdigen Belange verbunden sind. Die Beschwerden beim LfD richten sich meist gegen den Rechtsanwalt, den Gerichtsvollzieher, ein Inkassounternehmen oder eine andere Stelle, die tätig geworden ist; eine genauere Nachprüfung führt aber meistens zu dem Ergebnis, dass die Verwechslung von der Meldebehörde zu verantworten ist.

So war es auch im Falle einer Ärztin, die wiederholt recht unerfreuliche Post von einem Rechtsanwalt – der ihr nicht glauben wollte, dass die Adresse unrichtig ist – und schließlich den Besuch eines Gerichtsvollziehers erhielt.

Eine genauere Prüfung ergab, dass die zuständige Meldebehörde auf Anfrage die Anschrift der Ärztin weitergegeben hatte, obwohl sich die Anfrage des Rechtsanwalts an die Meldebehörde auf eine Person mit anderer Schreibweise des Vornamens bezog, eine andere Wohnanschrift genannt war und das Geburtsdatum als ergänzendes Identifizierungsmerkmal nicht zur Verfügung stand.

Nach Nr. 16.1 der VV zum Meldegesetz dürfen Meldebehörden bei Zweifeln, ob der Einwohner, über den eine Auskunft eingeholt werden soll, genau bezeichnet ist, eine Melderegisterauskunft nicht erteilen. Abweichende Schreibweisen des Namens können solche Zweifel begründen. Wird ein Einwohner aber trotz einer geringfügigen Abweichung des Namens – beispielsweise Meier statt Maier – über ergänzende vom Anfrager genannte Merkmale – z. B. frühere Anschrift und Geburtsdatum – identifiziert, so kann es auch angemessen sein, die Auskunft unter Vorbehalt zu erteilen. Die Mitarbeiter des Meldeamtes haben insoweit einen Beurteilungsspielraum.

5. Polizei

5.1 Allgemeine Tendenzen im Sicherheitsbereich

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in ihrer 56. Sitzung am 5./6. Oktober 1998 mit Zustimmung des LfD festgestellt, dass die Sicherheitsbehörden in den vergangenen Jahren umfangreiche zusätzliche Eingriffsbefugnisse erhalten haben. Demgegenüber würden aber in weiten Teilen Erkenntnisse über die Wirksamkeit und Grundrechtsverträglichkeit der Anwendung dieser Instrumente fehlen, wie z. B. bei der Schleppnetzfahndung und der Ausweitung der Telefonüberwachung.

Die Datenschutzbeauftragten des Bundes und der Länder haben ihrer Erwartung Ausdruck gegeben, dass der Bundesgesetzgeber und die Bundesregierung die Erforderlichkeit und die Wirksamkeit aller Eingriffsbefugnisse anhand objektiver Kriterien überprüfen (Evaluierung; die Entschließung ist als Anlage 8 abgedruckt), um ggf. die Eingriffsbefugnisse auch wieder zurückzunehmen.

5.2 Überprüfungen bei der Polizei

Im Berichtszeitraum wurden örtliche Feststellungen bei 24 Polizeidienststellen durchgeführt. Beim Landeskriminalamt erfolgten zahlreiche Informationsbesuche.

In keinem Fall musste eine Beanstandung ausgesprochen werden; in verschiedenen Prüfbereichen wurden Empfehlungen durch den LfD gegeben.

- In mehreren Fällen wurden in Dienststellen selbst erstellte Dateien betrieben, die nicht beim LfD angemeldet waren. Zum Betrieb dieser Dateien waren auch keine innerdienstlichen Regelungen getroffen worden, so dass der Zugriff teilweise ungesichert und die Speicherungsdauer nicht durch deutliche Vorgaben begrenzt war.
- Die erforderlichen Aufzeichnungen über Einsichtnahmen in die Lichtbildkartei des Pass- oder Ausweisregisters zum Zweck der Verfolgung von Verkehrsordnungswidrigkeiten waren nicht auf allen Dienststellen erfolgt.
- Vernehmungsaufzeichnungen waren in POLADIS, dem polizeilichen EDV-System zur Vorgangsbearbeitung, teilweise nicht mit einer Sperre gegen Veränderung versehen.
- Zweitschriften von strafrechtlichen Ermittlungsverfahren wurden ohne Erfordernis über mehrere Jahre aufbewahrt.
- Wie schon in früheren Jahren wurden wieder Unterlassungen bei der Pflicht zur Zusatzprotokollierung bei Abfragen für andere im polizeilichen Informationssystem POLIS festgestellt. Allerdings war in diesem Bereich eine erfreuliche Zunahme der Protokollierungen festzustellen.
- Umfassende polizeiliche Tätigkeitsberichte wurden – mit Personalien versehen – mehreren polizeilichen Stellen routinemäßig zugesandt. Hierzu wurde von Seiten des LfD eine Einschränkung des Umfanges der zu übermittelnden Informationen angeregt.
- Der Umfang der kriminalpolizeilichen Sammlungen entsprach nicht immer den datenschutzrechtlichen Anforderungen. Ohne Erfordernis und ohne eine Begründung in der Akte anzuführen, wurden teilweise vollständige Ermittlungsvorgänge in die KpS integriert.
- Anhand der KpS wurden die Einstellungen in den KAN-Bund, den bundesweiten Nachweis polizeilicher Erkenntnisse im Informationssystem INPOL, überprüft. Hierbei wurde festgestellt, dass in der Deliktsgruppe „Besitz von Betäubungsmitteln“, auch wenn es sich hierbei um jugendliche Ersttäter handelte, eine ausnahmslose Erfassung erfolgte. Diese Verfahrensweise wird derzeit mit dem zuständigen Ministerium erörtert.

Bei qualifizierten Observationen werden Observationsberichte sowohl von den Fahndungsdienststellen als auch von den sachbearbeitenden Dienststellen verwahrt. Bei örtlichen Feststellungen stellte sich die Frage nach der Zulässigkeit der Aufbewahrung und der Aufbewahrungsdauer dieser Berichte. Nach weiteren Informationen bei zwei Dienststellen hält der LfD die Aufbewahrung für grundsätzlich zulässig und gab Empfehlungen für die Dauer der Aufbewahrung.

5.3 Datenschutzrechtliche Schwerpunkte bei der automatisierten polizeilichen Datenverarbeitung

Der Siegeszug der PC macht auch vor den Polizeibehörden nicht halt. Der Schwerpunkt der polizeilichen automatisierten Datenverarbeitung liegt allerdings nach wie vor bei den zentralen Dateien POLIS und INPOL. Es handelt sich um komplexe Dateien, die im Wesentlichen dem überregionalen Nachweis von Unterlagen über Verdächtige und Straftäter dienen, die polizeibekannt geworden sind. Die Verfahren sind alt und datenschutzrechtlich unter den verschiedensten Gesichtspunkten überprüft.

Sie sollen allerdings durch neue Verfahren abgelöst werden, die zunächst die gleichen Funktionen wie die alten Verfahren erfüllen, die darüber hinaus aber eine sehr viel komfortablere Einbindung in die tägliche Arbeit, insbesondere auch in die Verwaltungsarbeit der Polizei, ermöglichen. Näheres wird dazu unten unter „POLADIS-neu“ sowie „INPOL-neu“ (Tz. 21.2.9) ausgeführt.

Daneben existieren dezentrale, grundsätzlich nicht vernetzte automatisierte Systeme, im Wesentlichen PC. Diese dienen der Unterstützung der Tätigkeit der einzelnen Sachbearbeiter und umfassen vorrangig Verfahren zur Textverarbeitung. Die modernen Textverarbeitungsprogramme decken jedoch auch Funktionen der klassischen Dateiverarbeitung mit ab. Bei den verschiedenen örtlichen Feststellungen in den Polizeidienststellen des Landes hat sich ergeben, dass die Datenverarbeitung auf PC durchaus nicht nur der Textverarbeitung im engeren Sinne dient. Die einzelnen Sachbearbeiter erhalten vielmehr durch die Speicherung ihrer Texte in automatisierter Form eine Dokumentation ihrer Tätigkeit, die auch über einen gewissen unterschiedlich langen Zeitraum nach dem Ausdruck der Dokumente abrufbar und nutzbar ist. Dies ist aus datenschutzrechtlicher Sicht grundsätzlich zulässig. Allerdings sind in diesem Zusammenhang technische und organisatorische Datenschutzanforderungen zu erfüllen; sie sind durch entsprechende Vorgaben auf der Ebene von Verwaltungsanordnungen bzw. Dienstanweisungen oder Errichtungsanordnungen gem. § 25 g POG verbindlich zu regeln.

Hier waren gewisse Defizite festzustellen, die aber im Zusammenwirken mit den Polizeidienststellen behoben werden.

Generell war bei den datenschutzrechtlichen Überprüfungen festzustellen, dass auf der polizeilichen Führungsebene eine große Bereitschaft besteht, den Anforderungen des Datenschutzes zu entsprechen.

Bei den Bediensteten vor Ort war gelegentlich allerdings wegen der damit verbundenen Erschwernisse sowie wegen der vermeintlichen Diskrepanz zwischen den stringenten Datenschutzanforderungen im öffentlichen Bereich (insbesondere bei der Polizei) und den wesentlich dahinter zurückbleibenden Anforderungen bei privaten Stellen (insbesondere bei Versicherungen, der Werbewirtschaft und sonstigen privaten Datenverarbeitern) ein gewisses Unverständnis festzustellen.

Es bleibt also auch eine wesentliche Aufgabe des Datenschutzes im Bereich der Polizei, bei den Bediensteten vor Ort das Verständnis für die datenschutzrechtlichen Anliegen zu fördern. Dazu gehört auch unnötige, bürokratische mit Datenschutz begründete, ihm aber nicht dienende Anforderungen abzubauen.

5.4 Überprüfungen von POLIS/INPOL-Speicherungen

Im Rahmen von örtlichen Feststellungen bei einzelnen Polizeibehörden wurden die Speicherungen von Daten über Kinder überprüft, die wegen des Verdachts der Begehung von Straftaten erfolgt sind.

Es hat sich ergeben, dass die hier bestehenden gesetzlichen und untergesetzlichen Vorgaben beachtet worden sind: Bei den überprüften Datensätzen hat es sich ausnahmslos um Fälle gehandelt, in denen Kinder erhebliche Straftaten (insbesondere gewerbsmäßigen Einbruchsdiebstahl) begangen haben und teilweise auch als Werkzeug von erwachsenen Tätern benutzt worden sind.

Die entsprechenden Prüffristen, nach deren Ablauf die Polizei in jedem einzelnen Fall gesondert zu prüfen hat, ob eine weitere Speicherung notwendig ist, waren jeweils angemessen.

Stichprobenweise wurde auch ein anderer Bereich von INPOL/POLIS-Speicherungen geprüft, nämlich die Erfassung jugendlicher Verdächtiger, die erstmals im Zusammenhang mit dem Verdacht der Begehung eines Betäubungsmitteldeliktes gespeichert worden sind. Dabei hat sich ergeben, dass landesweit der Verdacht der Begehung eines entsprechenden Deliktes auch bei erstmaliger Kontaktnahme mit der Polizei in Bagatellfällen zu einer überregionalen Erfassung in INPOL-Bund geführt hat. Dies ist aus datenschutzrechtlicher Sicht problematisch: Nach § 2 BKAG dürfen in die Verbunddatei beim BKA nur Daten über Verdächtige eingespeichert werden, deren angebliche Tat überregionale Bedeutung besitzt. Dies ist bei dem Verdacht auf bloßen Konsum von Rauschmitteln, der erstmals der Polizei bekannt wurde, aus der Sicht des LfD nicht der Fall. Die Erörterungen zu dieser Frage mit dem Ministerium des Innern und für Sport dauern gegenwärtig noch an.

5.5 Internet-Fahndung durch die Polizei des Landes

In Rheinland-Pfalz wurde ein landesweites Internet-Angebot der Polizei – unter datenschutzrechtlichen Gesichtspunkten in Abstimmung mit dem LfD – zentral entwickelt und allen Internet-Nutzern unter der Adresse „http://www.polizei.rlp.de“ zur Verfügung gestellt

Aus datenschutzrechtlicher Sicht sind folgende Punkte dabei besonders hervorzuheben:

Die neue Qualität der Internet-Fahndung im Vergleich zu bisherigen Formen der Öffentlichkeitsfahndung (unter den Gesichtspunkten Intensität des Eingriffs wegen internationaler Abrufbarkeit der Information, Manipulationsgefährdung und unkontrollierbare Fertigung von Kopien durch Dritte) lässt es dringend wünschenswert erscheinen, dass der Gesetzgeber die Voraussetzungen und Modalitäten der Internet-Fahndung regelt.

Allerdings erscheint es nicht vertretbar, die Nutzung des Internets zur Information der Bürger und auch zur Straftatenverfolgung unter diesen Gesichtspunkten derzeit auszuschließen, wenn folgende Anforderungen beachtet werden:

Soweit Fahndungsmaßnahmen mit Hilfe des Internets durchgeführt werden sollen, sind zusätzlich zu den allgemein vor Einleitung der Öffentlichkeitsfahndung zu beachtenden Schranken besondere Verhältnismäßigkeitsprüfungen durchzuführen. In der entsprechenden Verwaltungsvorschrift heißt es hierzu:

„Es ist stets zu prüfen, ob dem Täter oder anderen Betroffenen drohende Nachteile dadurch vermindert werden können, dass nur Publikationsorgane von geringerer Breitenwirkung in Anspruch genommen werden oder dass die Fahndungshilfe örtlich oder in anderer Weise, etwa durch Verzicht auf die Verbreitung des Bildes eines Gesuchten, beschränkt wird.“

Dies hat zur Folge, dass eine Fahndung im Internet nur bei schweren Straftaten von besonderer Bedeutung sowie dann genutzt werden darf, wenn ein dringender Tatverdacht vorliegt. Grundsätzlich muss auch ein Haft- oder Unterbringungsbefehl vorhanden sein. Die Fahndung nach Zeugen unterbleibt im Internet grundsätzlich. Für die Löschung ist festgelegt, dass in kurzen Zeitabständen die Erforderlichkeit der weiteren Fahndung unter Zugrundelegung der obigen Kriterien geprüft wird (zu den technisch-organisatorischen Anforderungen siehe Tz. 21.2.6).

Die Aufnahme von Personaldaten betroffener Bediensteter ist grundsätzlich von ihrer Zustimmung abhängig.

Unter diesen Voraussetzungen, deren Beachtung das Ministerium des Innern und für Sport durch den Erlass entsprechender Regelungen veranlasst hat, hält es der LfD für zulässig, das Internet zu Fahndungsmaßnahmen zu nutzen, auch wenn aus technisch-organisatorischer Sicht keine vollständige Sicherheit der Speicherungen vor Fälschung und dauerhafter Speicherung bei Dritten gegeben ist. Eine Abwägung der hierin liegenden Risiken mit dem Gebot der effektiven Straftatenverfolgung unter Nutzung geeigneter technischer Mittel führt aus der Sicht des LfD dazu, dass die datenschutzrechtlichen Bedenken zurücktreten müssen.

5.6 Presse- und Öffentlichkeitsarbeit bei der Polizei

Auch vor dem Hintergrund des landesweiten Internet-Angebotes von Presseveröffentlichungen durch die Polizei hat es der LfD für erforderlich gehalten, dass die Presse- und Öffentlichkeitsarbeit durch eine allgemeine Richtlinie geregelt wird. Im Bereich der Justiz ist dies bereits seit längerem der Fall. Für die Polizei sollten ähnliche Grundsätze gelten. Grundsätzlich besteht hierüber Übereinstimmung mit dem Ministerium des Innern und für Sport. Die praktische Umsetzung ist bisher noch nicht erfolgt.

5.7 Ergänzung des Polizei- und Ordnungsbehördengesetzes; verdachtsunabhängige Personenkontrolle

In den vergangenen Tätigkeitsberichten wurde wiederholt darauf hingewiesen, dass aus datenschutzrechtlicher Sicht eine Reihe von Fragen im Polizei- und Ordnungsbehördengesetz geregelt werden sollten (vgl. 14. Tb., Tz. 5.13; 15. Tb., Tz. 5.4; 16. Tb., Tz. 5.3). Es bestehen insbesondere folgende Regelungsdefizite:

- bei der Datenverarbeitung zur Vorbereitung von Hilfeleistungen und Handeln in Gefahrenfällen;
- beim Abgleich von Daten, die die Polizei bei ihrer Aufgabenerfüllung erlangt hat, insbesondere mit dem Fahndungsbestand;
- bei der Übermittlung von Daten an die allgemeinen Ordnungsbehörden zur konkreten Gefahrenabwehr (in der Regel zum Zweck von Zuverlässigkeitsprüfungen).
- In diesem Zusammenhang ist auch zu erwähnen, dass die Prüffrist von drei Monaten in § 25 e Abs. 1 Satz 3 POG sich als wenig praktikabel und für den Schutz der Betroffenen wenig effektiv erwiesen hat. Hier könnten aus datenschutzrechtlicher Sicht auch längere Fristen Eingang finden.

Bereits im 16. Tb. hat der LfD darauf hingewiesen, dass aus seiner Sicht keine grundsätzliche Änderung der Regelungssystematik des Polizei- und Ordnungsbehördengesetzes erforderlich ist, dass die Regelung dieser Fragen vielmehr durch wenige konkrete Änderungen der Vorschriften der §§ 25 a bis 25 g POG erfolgen könnte.

Es ist zu hoffen, dass die entsprechenden Vorbereitungsarbeiten im Ministerium des Innern und für Sport voranschreiten. Dem LfD ist bislang noch kein Entwurf zur Verfügung gestellt worden.

Auf politischer Ebene sind vorrangig andere Gesichtspunkte im Zusammenhang mit der Novellierung des Polizei- und Ordnungsbehördengesetzes diskutiert worden:

So stand im Vordergrund einer kontrovers geführten Diskussion die Frage, ob eine verdachtsunabhängige Personenkontrolle eingeführt werden sollte und ob diese datenschutzverträglich sei. Zwischenzeitlich hat eine Reihe von Bundesländern ihr Polizeigesetz entsprechend erweitert. Aus datenschutzrechtlicher Sicht bleibt festzuhalten, dass eine solche gesetzliche Regelung für die Polizei mit dem Ziel, die Identität einzelner Personen festzustellen, nicht grundsätzlich als unzulässig (verfassungswidrig) bezeichnet werden kann. Unter den derzeit bestehenden Bedingungen allerdings hält der LfD die Einführung einer solchen Regelung in Rheinland-Pfalz für unverhältnismäßig. Die Möglichkeiten des Bundesgrenzschutzes, in einem 20 km breiten Streifen an der Grenze entsprechende Feststellungen zu treffen, sind ausreichend. Für die praktische Polizeiarbeit im Land reichen schließlich die Möglichkeiten aus, die nach § 10 POG gegeben sind. Danach kann die Identität einer Person festgestellt werden, wenn dies zur Abwehr einer Gefahr erforderlich ist. Darüber hinaus kann die Polizei die Identität einer Person feststellen, wenn sie sich an einem Ort aufhält, von dem aufgrund tatsächlicher Anhaltspunkte erfahrungsgemäß anzunehmen ist, dass dort Personen Straftaten verabreden, vorbereiten oder verüben, sich Personen treffen, die gegen aufenthaltsrechtliche Vorschriften verstoßen, oder sich Straftäter verbergen oder an dem Personen der Prostitution nachgehen. Die Nähe zu einem Objekt, das gefährdet ist, reicht ebenfalls aus, um eine Identitätsfeststellung durchzuführen. Schließlich kann auch an einer Kontrollstelle, die von der Polizei eingerichtet worden ist, um bestimmte Straftaten zu verhindern, jedermann nach seinem Ausweis gefragt werden. Die Schaffung einer darüber hinausgehenden gesetzlichen Grundlage wäre das Schaffen einer Eingriffsermächtigung auf Vorrat für möglicherweise eintretende Gefährdungslagen, die konkret nicht absehbar sind. Davon rät der LfD dringend ab; mit dieser Beurteilung befindet er sich in Übereinstimmung mit dem Ministerium des Innern und für Sport.

5.8 Polizeiliche Datenverarbeitung auf europäischer Ebene; Europol

Die Europol-Konvention über die Errichtung und die Arbeit eines europäischen Polizeiamtes wird seit dem 1. Juli 1999 in die Praxis umgesetzt. Bis dahin war die Europäische Drogenstelle (EDS) als Vorläuferorganisation von Europol tätig. Dies erfolgte ohne eigenständige Verarbeitung personenbezogener Daten auf der Grundlage, dass die nach Den Haag zu EDS entsandten Verbindungsbeamten in dem Umfang, in dem die nationalen Rechtsgrundlagen dies zulassen, Daten aus den nationalen Datenbeständen an ihre europäischen Kollegen in der Europäischen Drogenstelle weitergeben. Das europäische Polizeiamt Europol konnte seine Arbeit deshalb erst Mitte 1999 aufnehmen, weil zwar die Konvention selbst zum 1. Oktober 1998 in Kraft getreten war, die erforderlichen Durchführungsbestimmungen aber noch nicht erlassen waren. Insbesondere fehlte die Geschäftsordnung für die gemeinsame Kontrollinstanz. Zu Einzelheiten in diesem Zusammenhang wird auf Tz. 11.3 des 17. Tb. des BfD, S. 265 verwiesen.

Der LfD hielt es in Übereinstimmung mit den Datenschutzbeauftragten des Bundes und der anderen Länder für geboten, dass der Beschwerdeausschuss nach Artikel 24 Abs. 7 der Europol-Konvention so ausgestaltet wird, dass er eine effektive, gerichtsähnliche Kontrolle einzelner Datenverarbeitungsvorgänge bei Europol vornehmen kann. Die Mitglieder des Beschwerdeausschusses müssen also die Befähigung zum Richteramt haben; außerdem muss ihre Unabhängigkeit von Einflussnahmen der sie entsendenden Regierungen gewährleistet sein. Nur dann kann hingenommen werden, dass Eingriffe in das informationelle Selbstbestimmungsrecht von deutschen Bürgern durch eine europäische Institution vorgenommen werden dürfen.

Die nun erlassenen Regelungen entsprechen diesen Anforderungen im Wesentlichen. Der Schwerpunkt der weiteren datenschutzrechtlichen Begleitung der Tätigkeit von Europol wird die Überprüfung von Übermittlungen an diese Dienststelle sowie der dort erfolgenden Verarbeitung der Informationen sein. Für die letztgenannte Frage besteht allerdings keine Zuständigkeit des LfD.

5.9 Einsichtnahme in das Pass- und Personalausweisregister

Mehrere Eingaben betrafen das Verhalten der Polizei bei der Aufklärung von Verkehrsordnungswidrigkeiten im Zusammenhang mit Geschwindigkeitsüberschreitungen. Die Verkehrsverstöße waren durch Fahrzeugführer begangen worden, die nicht Halter der Fahrzeuge waren. Die Fahrzeughalter hatten zunächst auf den Anhörformularen der Straßenverkehrsbehörde angegeben, dass ihnen nicht bekannt sei, wer das jeweilige Fahrzeug zu der betreffenden Zeit gefahren habe. Die daraufhin der Polizei zur Verfügung gestellten Beweisfotos begründeten einen Verdacht gegen bestimmte Angehörige der Kfz-Halter. Von diesen Verdächtigen besorgten sich die Beamten dann Lichtbilder aus den Registern der jeweiligen Pass- und Personalausweisbehörden. Diese Bilder und die Beweisfotos legten sie zu Identifizierungszwecken, ohne weiteren Kontakt mit den Kfz-Haltern oder den Verdächtigen aufgenommen zu haben, Nachbarn der Betroffenen vor.

In den hier vorliegenden Fällen waren die Geschwindigkeitsüberschreitungen so erheblich, dass sie einen Eintrag in das Verkehrszentralregister zur Folge gehabt hätten. Aus diesem Grund sind nach den Richtlinien eine Einsichtnahme der Polizei in das Pass- und Personalausweisregister und Ermittlungen bei Dritten grundsätzlich zulässig. Ermittlungen bei Dritten dürfen jedoch erst erfolgen, wenn weniger einschneidende Maßnahmen erfolglos oder unmöglich sind.

In den zu beurteilenden Fällen wäre eine Befragung der Verdächtigen ein geeignetes Mittel zur Identitätsfeststellung gewesen und hätte deren Persönlichkeitsrechte weit weniger beeinträchtigt als die Befragung der Nachbarn.

Gegenüber dem Ministerium des Innern und für Sport hat der LfD die Unzulässigkeit dieser Ermittlungshandlungen festgestellt. Von dort wurden die betroffenen Behörden und Beamten darauf hingewiesen.

5.10 Wie privat ist ein „Privates Fach“?

Zur Unterstützung polizeilicher Bürotätigkeit wird auf zahlreichen Polizeidienststellen das EDV-System CEO eingesetzt. In diesem System gliedert sich die Ablage u. a. in öffentliche und private Fächer. Die privaten Fächer sind jedem einzelnen Beamten zugewiesen und mit einem persönlichen Passwort gesichert. Eine Regelung über die Nutzung privater Fächer und über mögliche Zugriffsrechte bestand zunächst nicht.

Auf einer Dienststelle wurde das private Fach eines Beamten während dessen mehrtägiger Abwesenheit durch den Systemverwalter auf Anordnung des Dienststellenleiters geöffnet und das Protokoll einer Dienstbesprechung, das er mit der elektronischen Post erhalten hatte, geändert. Hierbei wurde systembedingt das persönliche Passwort außer Kraft gesetzt und das private Fach war bis zur Rückkehr des Beamten auch für andere Bedienstete unter Anwendung eines Standardpasswortes zugänglich.

Aus der Stellungnahme des LfD geht hervor, dass der Eingriff in das passwortgeschützte Ablagefach während der Abwesenheit des Beamten weder sachlich noch zeitlich erforderlich und damit unzulässig war. Das Innenministerium wurde gebeten, die Nutzungsbedingungen und Zugriffsberechtigungen in Bezug auf die privaten Fächer landeseinheitlich zu regeln. Dies ist zwischenzeitlich in einer Ergänzung der Dienstanweisung über den Datenschutz und die Datensicherheit erfolgt.

5.11 Zusammenarbeit zwischen Bundeswehr, Polizei und anderen Behörden der Gefahrenabwehr

Vom Bundesministerium des Innern wurde der Entwurf der vollständig überarbeiteten „Richtlinie für die Zusammenarbeit zwischen Bundeswehr, Polizei und anderen Behörden der Gefahrenabwehr“ den Innenministerien und -senatsverwaltungen der Länder zur Stellungnahme zugeleitet.

In Abschnitt A dieser Richtlinie ist unter Ziffer 1 Absatz 1 geregelt, dass Bundeswehr einerseits und Polizei und andere Verwaltungen andererseits sich gegenseitig um Amtshilfe ersuchen können.

Der LfD hat im Rahmen seiner Beteiligung angeregt, diese Bestimmung dahin gehend zu ergänzen, dass Datenübermittlungen im Rahmen der Amtshilfe nur stattfinden dürfen, wenn sie aufgrund von Rechtsvorschriften (z. B. Polizeigesetze, Datenschutzgesetze) zulässig sind. Durch diese Ergänzung soll dem Missverständnis vorgebeugt werden, dass aus der Pflicht zur Amtshilfe eine Befugnis zur Übermittlung personenbezogener Daten resultiert.

Das Innenministerium des Landes hat die Anregung des LfD in seine Stellungnahme an das Bundesinnenministerium aufgenommen.

5.12 Zentrale Datei zur Erfassung von Verdachtsanzeigen nach dem Geldwäschegesetz

Über das Ministerium des Innern und für Sport erhielt der LfD davon Kenntnis, dass der Bundesminister des Innern die Errichtung einer Zentraldatei zur Erfassung aller Geldwäscheverdachtsanzeigen beim BKA vorgeschlagen hat. Zur näheren Begründung verwies der Bundesinnenminister auf den Schlussbericht der Projektgruppe „Länderauswertung Verdachtsanzeigen“. Hieraus war zu entnehmen, dass seitens der Praxis eine solche Datei für sinnvoll gehalten werde; nähere Aussagen über ihre Struktur, ihren Inhalt und die Speichervoraussetzungen waren nicht enthalten. Vor diesem Hintergrund wurden vom LfD nur folgende allgemeine Hinweise gegeben:

Bei der Speicherung von Daten der Polizei des Landes Rheinland-Pfalz in einer Zentraldatei des BKA sind – jedenfalls solange in der Strafprozessordnung keine vorrangigen Regelungen enthalten sind – sowohl die Regelungen des Polizei- und Ordnungsbehördengesetzes von Rheinland-Pfalz (insbesondere §§ 25 a, 25 c und 25 e) wie die des BKAGes (hier insbesondere § 8) zu beachten. Daraus ergibt sich, dass keineswegs undifferenziert alle Personen in einer Zentraldatei des BKA gespeichert werden dürfen, deren Verhalten zum Erstellen einer Verdachtsanzeige gemäß § 11 GwG geführt hat.

Bezüglich der Beschuldigten dürfen gem. § 8 Abs. 1 BKAG ohne weitere Voraussetzungen die Personendaten sowie andere zur Identifizierung geeignete und erforderliche Merkmale, die kriminalaktenführende Polizeidienststelle, die Kriminalaktennummer, die Tatzeiten und Tatorte und die Tatvorwürfe durch Angabe der gesetzlichen Vorschriften und der näheren Bezeichnung der Straftaten übermittelt werden.

Weitere Beschuldigtendaten sowie Daten von Personen, die einer bestimmten Straftat verdächtigt werden, können gespeichert werden, wenn zu Beginn der Speicherung feststeht, dass sie erforderlich ist, weil wegen der Art oder Ausführung der Tat, der Persönlichkeit des Betroffenen oder sonstiger Erkenntnisse Grund zu der Annahme besteht, dass (weitere) Strafverfahren gegen

den Beschuldigten oder Tatverdächtigen zu führen sind (§ 8 Absatz 2 BKAG). Mit anderen Worten: Eine Einspeicherung kommt frühestens dann in Betracht, wenn durch die zuständigen Ermittlungsbehörden des Landes aufgrund einer eigenen Beurteilung das Vorliegen dieser Voraussetzungen festgestellt worden ist.

Auch sonstige Personen könnten in die Zentraldatei eingespeichert werden, wenn und soweit dies erforderlich ist, weil bestimmte Tatsachen die Annahme rechtfertigen, dass die Betroffenen Straftaten von erheblicher Bedeutung begehen werden (§ 8 Absatz 5 BKAG). Auch diese Voraussetzung muss aufgrund eigener Erkenntnisse der Ermittlungsbehörden des Landes in jedem Einzelfall festgestellt werden.

Allerdings war auch auf die Löschungsverpflichtung des § 25 e POG hinzuweisen: Wenn sich im Verlauf der Ermittlungen herausgestellt hat, dass der Verdacht der Geldwäsche gegenstandslos war, ist unverzüglich eine Löschung auch in der Zentraldatei zu veranlassen (§ 25 e Abs. 2 Nr. 2 POG).

Abschließend ist festzustellen, dass bei Einhaltung der o. g. Voraussetzungen aus datenschutzrechtlicher Sicht keine grundsätzlichen Bedenken gegen die Einrichtung einer Zentraldatei Geldwäsche bestehen.

5.13 Zusammenarbeit von Staatsanwaltschaft und Polizei bei der Bekämpfung der Geldwäsche

Zur Bearbeitung von Verdachtsanzeigen nach § 11 GwG wurde bei der Zentralstelle „Finanzermittlungen“ des Landeskriminalamtes in Mainz die „Gemeinsame Clearingstelle Polizei/Zoll“ gegründet. Obwohl die Zuständigkeit des Zolls in diesem Deliktsbereich auf die international organisierte Geldwäsche begrenzt ist, erhält er auf diesem Wege Kenntnis von allen Sachverhalten der Geldwäsche; er soll Gelegenheit erhalten zu prüfen, ob nach den ihm zur Verfügung stehenden ergänzenden Informationen ein internationaler Bezug besteht. Eine ausdrückliche Rechtsgrundlage für diese Einbeziehung einer zunächst unzuständigen Stelle besteht nicht. In einem Gemeinsamen Rundschreiben des Ministeriums des Innern und für Sport und des Ministeriums der Justiz wurde eine Regelung getroffen, wonach die gemeinsame Bearbeitung aller Verdachtsanzeigen durch Polizei und Zoll in Ausübung ihrer Sachleitungsbefugnis generell von der Staatsanwaltschaft angeordnet wird. Dies ist nach Auffassung des LfD zulässig.

Ein weiterer Stein des Anstoßes war für den LfD die vorgesehene Regelung, dass alle Verdachtsanzeigen mit Personenangaben, unabhängig davon, ob die Voraussetzungen eines Anfangsverdachts nach § 152 Abs. 2 StPO erfüllt sind, in das so genannte „Js-Register“ bei den Staatsanwaltschaften eingetragen werden sollen. Hierdurch war zu befürchten, dass dieser Eintrag eine generelle Speicherung im bundesweiten staatsanwaltschaftlichen Verfahrensregister (ZStV) nach sich ziehen werde. Die Bedenken des LfD wurden zumindest teilweise durch eine Zusicherung des Justizministeriums ausgeräumt, dass nur in den Fällen, in denen durch eine Prüfung des zuständigen Dezernenten ein Anfangsverdacht festgestellt werde, ein Eintrag in das ZStV vorgenommen werde.

5.14 Datei „Ringalarmfahndung“

Bereits in seinem 16. Tb. hatte der LfD darauf hingewiesen, dass in einem bestimmten Fall die durch eine Ringalarmfahndung erlangten Daten über mehrere Jahre hinweg gespeichert worden waren (vgl. 16. Tb., Tz. 5.19). In diesem Zusammenhang wurde auch angeregt, eine generelle Regelung für die Speicherung dieser Daten zu schaffen. Vom Innenministerium wurde nun die Verfahrensbeschreibung einer landeseinheitlich zu nutzenden Datei „Ringalarmfahndung“ als Entwurf vorgelegt.

Nach dieser Verfahrensbeschreibung soll die Speicherung von Haltern und Insassen von Fahrzeugen erfolgen, deren amtliche Kennzeichen in Durchfahrtkontrollen erfasst wurden. Außerdem sollen diejenigen Personen in der Datei gespeichert werden, die außerhalb eingerichteter Kontrollstellen aufgrund konkreter Verdachtsmomente einer Überprüfung unterzogen wurden.

Die Speicherung dieser Daten soll so lange möglich sein, bis entweder das der Ringalarmfahndung zu Grunde liegende Delikt geklärt oder – bei ungeklärten Fällen – die Strafverfolgungsverjährung eingetreten ist.

Keine Bedenken hat der LfD in Bezug auf die Erhebung und Speicherung der Daten von Verdächtigen, also von denjenigen Personen, die aufgrund konkreter Verdachtsmomente überprüft wurden. Kritischer war jedoch die Erhebung und Speicherung der bei Durchfahrtkontrollen erlangten Daten zu bewerten, da hierdurch eine große Anzahl unverdächtiger Personen betroffen wird.

Der Gesetzgeber hat es für erforderlich gehalten, die Datenerhebung an Kontrollstellen in § 111 StPO und die automatisierte Speicherung und Nutzung der dabei erhobenen Daten in § 163 d StPO spezialgesetzlich und abschließend zu regeln.
Die gesetzliche Regelung enthält folgende Sicherungsmaßnahmen:

– Beschränkung auf einen Straftatenkatalog,

– Begrenzung der Speicherungsdauer auf höchstens neun Monate,

– grundsätzlicher Richtervorbehalt bei der Anordnung.

Diese einengenden Voraussetzungen sind zwingend zu beachten. Aus der Sicht des LfD gelten diese gesetzlichen Regelungen auch für Kennzeichendaten bei Durchfahrtkontrollen, die in der geplanten Datei erfasst werden sollen.

Die Landesregierung teilt die Ansicht des LfD; der Aufbau entsprechender Datenbanken wird deshalb nur unter den genannten Voraussetzungen erfolgen. Ob solche Dateien unter Einhaltung dieser Bedingungen tatsächlich eingerichtet werden, ist derzeit noch nicht abschließend geklärt.

5.15 Vorsätzliche Verstöße gegen Datenschutzvorschriften durch Polizeibedienstete

Die Zahl der Polizeivollzugsbediensteten in Rheinland-Pfalz beträgt ca. 10 000. Damit sind sie nach den Lehrern die zahlenmäßig stärkste Berufsgruppe unter den öffentlich Bediensteten im Land. Der größte Teil dieser Bediensteten hat die Möglichkeit, auf Daten aus den polizeilich zugänglichen Dateien zuzugreifen: auf INPOL/POLIS-Daten, auf Daten aus dem Melderegister, auf solche des Kraftfahrt-Bundesamtes (ZEVIS) oder aus dem polizeilichen Vorgangsverwaltungssystem „Poladis“. So ist es nicht verwunderlich, dass unter dieser großen Zahl auch das eine oder andere „schwarze Schaf“ die sensiblen Polizeidaten zu privaten Zwecken missbraucht. Folgende Fälle sind dem LfD im Berichtszeitraum bekannt geworden:

Im Zusammenhang mit polizeilichen bzw. staatsanwaltschaftlichen Ermittlungen im Trierer Rotlichtmilieu erfolgte vom Landtag Rheinland-Pfalz die Einsetzung eines Untersuchungsausschusses zur Aufklärung von Verdächtigungen gegen öffentlich Bedienstete und Personen des öffentlichen Lebens. In einem Zwischenbericht dieses Untersuchungsausschusses wurde auf mehrere Strafverfahren gegen öffentlich Bedienstete hingewiesen, in denen teilweise Urteile ergangen waren. Eine Einsichtnahme in diese Urteile ergab Folgendes:

In einem Fall wurde einem Polizeibeamten unter anderem vorgeworfen, sieben Personenüberprüfungen ohne dienstlichen Anlass im polizeilichen Informationssystem INPOL durchgeführt und die Ergebnisse den Betroffenen übermittelt zu haben. Der Beamte wurde zwar vom Vorwurf der Bestechlichkeit freigesprochen; das Gericht war aber zweifelsfrei davon überzeugt, dass der Vorwurf des unzulässigen Datenabrufs berechtigt war. Der LfD hat sich an das zuständige Ministerium mit der Frage gewandt, ob und in welcher Weise das dienstliche Fehlverhalten dienstaufsichtliche Folgen hatte. Er geht nämlich davon aus, dass bei aufgeklärten Fällen dieser Art nur durch abschreckende Sanktionen vermieden werden kann, dass solche Handlungen als tolerable und lässliche Sünden erscheinen. Trotz der Vertraulichkeit von Dienstordnungsverfahren sprechen sich Sanktionen, die teilweise ohnehin auch Sozialbezug haben, im Kollegenkreis schnell herum. Es ergab sich, dass gegenüber dem Beamten zunächst das Verbot der Amtsführung ausgesprochen wurde, dass er über ein Jahr vorläufig vom Dienst enthoben war und dass er schließlich – wenn auch außerhalb eines förmlichen Disziplinarverfahrens – eine dienstaufsichtliche Rüge für sein Verhalten erhalten hat.

In einem anderen Fall hatte ein Bediensteter der Polizei, dessen Freundin als Prostituierte tätig war, sich die Kfz-Kennzeichen von Freiern notiert. Da er selbst keinen Zugang zu polizeilichen Informationssystemen hatte, veranlasste er drei Kollegen, ihm die Halterauskünfte zu beschaffen. Die Strafverfahren in diesem Zusammenhang sind noch nicht sämtlich rechtskräftig abgeschlossen.

Schließlich steht der Vorwurf eines Leitenden Oberstaatsanwaltes unwidersprochen im Raum, dass die Polizei in einem Fall ohne die vorgesehene staatsanwaltschaftliche Genehmigung einen V-Mann (Vertrauensperson) eingesetzt habe. Damit hätte die Polizei unzulässig in verdeckter Form Daten erhoben.

In einem ganz anderen Zusammenhang hatte sich der bereits im 15. Tb., Tz. 5.7 geschilderte Fall ereignet, dass sich ein Polizeibeamter über einen unzulässigen Einblick in das „EWOIS“ (das zentrale Melderegister des Landes) die Privatadresse einer Ministerin verschaffte und anschließend versuchte, diese zu einem bestimmten Verhalten (im Zusammenhang mit der Anlage einer Sondermülldeponie) zu nötigen. Dieser Beamte wurde wegen versuchter Nötigung und wegen Verstoßes gegen § 27 LDatG zu einer Freiheitsstrafe von elf Monaten, die zur Bewährung ausgesetzt wurde, verurteilt. Schließlich wurde er degradiert und eine Beförderungssperre verhängt.

Vor diesem Hintergrund hat der LfD auch einen anonymen Hinweis ernst genommen, wonach Polizeibeamte zu privaten Zwecken unzulässig Halterdaten abrufen würden. In Zusammenarbeit mit dem LfD wurden von der Polizei Ermittlungen geführt, die allerdings nicht zur Bestätigung der Vorwürfe führten.

Diese Vorgänge zeigen, wie ernst auch in Bezug auf Datenschutz die Dienstaufsicht zu nehmen ist und dass die Anstrengungen des LfD, möglichst wirksame technisch-organisatorische Vorkehrungen unter Einschluss detaillierter Protokollierungen durchzusetzen, nicht überflüssig sind. Sie sind auch deshalb wichtig, um ggf. bestimmte Vorwürfe des unzulässigen Datenabrufs (z. B. mithilfe einer lückenlosen, aussagekräftigen Protokollierung) widerlegen zu können. Die vorstehend beschriebenen Einzelfälle dürfen auch aus der Sicht des LfD angesichts der eingangs genannten Zahlen nicht überbewertet werden und nicht zu einem generell negativen Urteil über die Integrität der Polizei führen. Gerade die Aufklärung und Publizierung solcher Fälle beweist, dass die bestehenden Kontrollmechanismen im Prinzip funktionsfähig und effektiv sind und dass Polizei und Aufsichtsbehörden ein starkes eigenes Interesse daran haben, solche Vorgänge zu verhindern.

6. Verfassungsschutz

6.1 Novellierung des Landesverfassungsschutzgesetzes

Im Berichtszeitraum wurde das Landesverfassungsschutzgesetz grundlegend überarbeitet und neu verkündet (LVerfSchG vom 6. Juli 1998, GVBl. S. 184, BS 12-2). In Anlehnung an das Bundesverfassungsschutzgesetz wurden insbesondere die Vorschriften zur Datenverarbeitung (4. Teil, §§ 11 bis 19) neu geschaffen, durch die das Gesetz an den zwischenzeitlich erreichten Stand der Diskussion auch unter Datenschutzgesichtspunkten angepasst werden sollte.

Der LfD wurde von Beginn an in vorbildlicher Weise in die Diskussion um diese Regelungen einbezogen. Unter inhaltlichen Gesichtspunkten ist das Ergebnis aus datenschutzrechtlicher Sicht seiner Auffassung nach als datenschutzverträglich zu bezeichnen.

Durch die extensiv genutzte Verweisungstechnik ist allerdings gerade der vierte Teil des Gesetzes, der sich mit der Datenverarbeitung befasst, nicht leicht verständlich. Auch die zwangsläufig in großem Umfang verwendeten unbestimmten Rechtsbegriffe entsprechen sicher nicht dem Ideal einer normenklaren Regelung. Andererseits sind diese Begriffe, die bereits seit Jahrzehnten in den Verfassungsschutzgesetzen des Bundes und der Länder Verwendung gefunden haben, zwischenzeitlich durch die Praxis und auch durch die Rechtsprechung so konkretisiert worden, dass sie als ausreichend klar angesehen werden können. Dies betrifft beispielsweise den als Anknüpfungspunkt für Aufgaben und Befugnisse des Verfassungsschutzes grundlegend bedeutsamen Begriff der „tatsächlichen Anhaltspunkte für den Verdacht von Bestrebungen oder Tätigkeiten, die gegen die freiheitliche demokratische Grundordnung, den Bestand oder die Sicherheit des Bundes oder eines Landes gerichtet sind“ (vgl. § 11 Abs. 1 Nr. 1).

Besonders hervorzuheben ist, dass die nachrichtendienstlichen Mittel, die zur Beschaffung von Informationen eingesetzt werden dürfen, jedenfalls beispielhaft (durch eine mit „insbesondere“ eingeleitete Aufzählung) beschrieben sind. Sie sind abschließend in einer Dienstvorschrift zu benennen, die auch die Zuständigkeit für die Anordnung von Informationsbeschaffungen unter Einsatz solcher Mittel regelt. Die Dienstvorschrift ist der Parlamentarischen Kontrollkommission vorzulegen (§ 10 Abs. 1).

Die Regelungen über Eingriffe in das Fernmeldegeheimnis sind ebenfalls sehr detailliert und entsprechen den verfassungsrechtlichen und datenschutzrechtlichen Anforderungen (§ 10 Abs. 2). Gleiches gilt für die Regelung des Abhörens in Wohnungen (§ 10 Abs. 5). In diesem Zusammenhang spielt die Pflicht zur Benachrichtigung der Betroffenen nach Abschluss der Maßnahme (§ 10 Abs. 8) aus datenschutzrechtlicher Sicht eine besondere Rolle.

Die intensiven Diskussionen der datenschutzrechtlichen Fragen haben dazu geführt, dass noch während der parlamentarischen Beratung in den zuständigen Ausschüssen Änderungen im Interesse des Datenschutzes durchgesetzt werden konnten. Der LfD hat zwar nicht in allen Punkten seine Vorstellungen umsetzen können; das Parlament hat aber ebenso wie die Landesregierung dadurch bestätigt, welchen Stellenwert sie dem Datenschutz einräumen und dass bei den notwendigen Abwägungen die Individualinteressen eine herausragende Bedeutung haben.

An diesem Gesamturteil ändert auch die Tatsache nichts, dass der Wunsch des LfD, seine Prüfkompetenz gesetzlich ohne Ausnahme umfassend festzulegen, nicht erfüllt wurde. Aus seiner Sicht ist die vorhandene Ausnahmemöglichkeit, wonach der Innenminister im Einzelfall im Interesse der Sicherheit des Landes einen Einblick in Daten gegenüber dem LfD untersagen kann, zumindest entbehrlich. Eine Beschränkung auf eine Einsichtsbefugnis durch den Landesbeauftragten persönlich (wie dies in anderen Ländern erfolgt ist) hätte aus seiner Sicht gereicht, um den Sicherheitsinteressen des Landes zu genügen.

6.2 Befugnisse des LfD im Bereich von Abhörmaßnahmen nach dem G-10-Gesetz

Im Bereich der Abhörmaßnahmen des Landesverfassungsschutzes nach dem G-10-Gesetz hat der LfD keine Kontrollkompetenz. Dies ergibt sich aus § 5 des Landesgesetzes zur Ausführung des Gesetzes zu Artikel 10 GG (AG G 10 vom 24. September 1979, GVBl. S. 296, BS 12-1). Danach fällt die Verarbeitung von Daten, die der Kontrolle durch die parlamentarische G-10-Kommission unterliegen, nicht in die Kontrollkompetenz des LfD, es sei denn, die Kommission ersucht diesen, die Einhaltung der Vorschriften über den Datenschutz bei bestimmten Vorgängen oder in bestimmten Bereichen zu kontrollieren und ausschließlich ihr darüber zu berichten.

Fraglich ist, in welchem Umfang die parlamentarische Kommission zu Artikel 10 GG Befugnisse zur Kontrolle besitzt. Der LfD geht davon aus, dass dieser Kommission gesetzlich umfassende Befugnisse zugewiesen sind. Eine andere Frage ist, in welchem Umfang die Kommission ihre Befugnisse auch tatsächlich ausschöpft. Jedenfalls kann der LfD in diesem Bereich nur tätig werden, wenn die Kommission ihm hierzu einen ausdrücklichen Auftrag erteilt. Dies ist bislang nicht geschehen.

Die Rechtslage wird von einigen Landesbeauftragten für den Datenschutz mit ähnlichen landesgesetzlichen Regelungen zum Teil anders beurteilt. Diese vertreten die Auffassung, die Parlamentarische Kontrollkommission habe keine umfassenden Befugnisse in diesem Zusammenhang. Sie erhoffen sich insoweit eine klarstellende Entscheidung des Bundesverfassungsgerichts. Derzeit ist das Ergebnis nicht abzusehen.

6.3 Landessicherheitsüberprüfungsgesetz

Das Landessicherheitsüberprüfungsgesetz ist im Berichtszeitraum bis zur Kabinettsreife gediehen. Es soll in Kürze in die parlamentarischen Beratungen eingebracht werden. Damit sollen der Zweck, die Voraussetzungen und die weiteren Einzelheiten des Verfahrens bei der Durchführung von Sicherheitsüberprüfungen gesetzlich geregelt werden.

Der vorliegende Entwurf, der sich in vielen Punkten sinnvollerweise an das Sicherheitsüberprüfungsgesetz des Bundes anlehnt, ist weitgehend mit dem LfD einvernehmlich erörtert worden. Die datenschutzrechtlichen Anliegen haben im Wesentlichen in den Gesetzentwurf bereits Eingang gefunden. Dazu gehören insbesondere folgende Punkte:

– Beschränkung der Sicherheitsüberprüfung auf sicherheitsrelevante Tätigkeitsbereiche von öffentlich Bediensteten, keine Ausweitung auf sonstige Felder wie etwa Korruptionsbekämpfung;

– deutliche Regelung der Zweckbindung der zu Sicherheitsüberprüfungszwecken erhobenen und gespeicherten Daten;

– angemessene Ausgestaltung des Auskunftsrechts der Betroffenen über gespeicherte Informationen.

Der LfD hätte darüber hinaus – wie im Bereich des Landesverfassungsschutzgesetzes – begrüßt, wenn seine Prüfkompetenz gesetzlich ohne Ausnahme anerkannt worden wäre. Aus seiner Sicht ist die auch hier vorgesehene Ausnahmemöglichkeit, wonach der Innenminister im Einzelfall im Interesse der Sicherheit des Landes einen Einblick in Sicherheitsüberprüfungsvorgänge gegenüber dem LfD untersagen kann, zumindest entbehrlich. Eine Beschränkung auf eine Einsichtsbefugnis durch den Landesbeauftragten persönlich hätte aus seiner Sicht gereicht, um den Sicherheitsinteressen des Landes zu genügen.

Eine Unterwerfung der Person des LfD unter die Pflicht zur Durchführung einer Sicherheitsüberprüfung hält er aus grundsätzlichen Erwägungen und auch aus rechtssystematischen Gründen für nicht angemessen: Der Leiter einer obersten Landesbehörde kann sich letztlich nicht selbst überprüfen. Eine entsprechende Klarstellung sollte in das Gesetz aufgenommen werden. Insgesamt ändern diese Punkte aber nichts am grundsätzlich positiven Gesamturteil über den vorliegenden Entwurf eines Landessicherheitsüberprüfungsgesetzes aus datenschutzrechtlicher Sicht.

6.4 Scientology und Verfassungsschutz

Grundsätzliches zur Datenerhebungsbefugnis des Verfassungsschutzes in Bezug auf Scientology hat der LfD im 16. Tb., Tz. 6.3, ausgeführt.

Im Berichtszeitraum war zu klären, ob Sektenbeauftragte im öffentlichen Dienst verpflichtet sind, dem Verfassungsschutz auf dessen Aufforderung hin Informationen über Einzelfälle zu übermitteln.

Der LfD hat – letztlich nicht im Gegensatz zur Verfassungsschutzbehörde des Landes – die Bedeutung der Vertraulichkeit solcher Beratungen hervorgehoben und auch die verfassungsrechtliche Qualität des Schutzes der Vertraulichkeit in diesem Zusammenhang betont. Dies bedeutet, dass aus seiner Sicht personenbezogene Informationen nur mit Zustimmung der Beratenen an den Verfassungsschutz übermittelt werden dürfen.

Er hat allerdings auch erklärt, dass wegen der Mitwirkungspflicht öffentlicher Stellen gegenüber dem Verfassungsschutz die befragten Stellen dazu verpflichtet sind, die beratenen Personen – allerdings unter Hinweis auf die Freiwilligkeit – um ihre Einwilligung zu ersuchen. Auch wenn dies gelegentlich arbeitsaufwendig ist, so lässt die Rechtslage aus der Sicht des LfD keine andere Verfahrensweise zu.

6.5 Erfassung einfacher Mitglieder von extremistischen Personenzusammenschlüssen durch die Verfassungsschutzbehörden

Der Berliner Datenschutzbeauftragte wandte sich Mitte 1998 an die Datenschutzbeauftragten des Bundes und der Länder und wies auf die Problematik der Erfassung einfacher Mitglieder von extremistischen Personenzusammenschlüssen durch die Verfassungsschutzbehörden hin. Der LfD hat gegenüber dem Berliner Datenschutzbeauftragten folgende Auslegung der maßgeblichen Regelungen des Landesverfassungsschutzgesetzes vertreten:

Das am 17. Juni 1998 verabschiedete Landesverfassungsschutzgesetz unterscheidet in § 4 Abs. 1 Satz 1 Ziff. 3 i. V. m. Satz 2 nur zwischen Verhaltensweisen „in einem“ oder „für einen“ Personenzusammenschluss und knüpft hieran unterschiedliche Voraussetzungsmerkmale. „In einem“ Personenzusammenschluss reicht eine bestimmte ziel- und zweckgerichtete Verhaltensweise. Wer „für einen“ Personenzusammenschluss – also außerhalb – handelt, kommt für Maßnahmen wie die sog. „Verkartung“ nur dann in Frage, wenn er „ihn in seinen Bestrebungen nachhaltig unterstützt“. In einem Personenzusammenschluss stellt die bloße Mitgliedschaft dann eine Bestrebung dar, wenn sie als politisch bestimmte, ziel- und zweckgerichtete Verhaltensweise anzusehen ist. Dies kann nicht von jeder Mitgliedschaft in jeder Organisation, insbesondere bei sog. „Karteileichen“, behauptet werden. Die Begründung zu § 4 spricht von den in einer Organisation tätigen Personen. Bloß nominelle Mitglieder sind in einer Organisation nicht tätig, sondern untätig. Es müssen – jedenfalls bei Organisationen, die an die Mitgliedschaft keine besonderen Anforderungen stellen – weitere Indizien für ein unterstützendes Verhalten hinzukommen; bei sog. „Kaderparteien“, die eine Mitgliedschaft vom aktivem Einsatz abhängig machen, ist allerdings die Mitgliedschaft allein ausreichender Ausdruck eines zielgerichteten Verhaltens.

Eine Speicherung von Daten der Mitglieder, die danach ziel- und zweckgerichtet unterstützend handeln, kommt nach § 11 Abs. 1 Nrn. 1 und 2 LVerfSchG in Betracht, wenn dies für die Erforschung und Bewertung von Bestrebungen erforderlich ist.

Nunmehr hat der Berliner Datenschutzbeauftragte mitgeteilt, dass das Innenministerium Rheinland-Pfalz in einer dem LfD im Wortlaut nicht vorliegenden Stellungnahme im Gegensatz dazu Folgendes erklärt habe:

Die Beobachtung von Bestrebungen im Sinne des § 4 Landesverfassungsschutzgesetz erstrecke sich nicht nur auf die betreffenden Personenzusammenschlüsse als solche, sondern erfasse unter der Voraussetzung einer gewissen Handlungsintensität auch die Verhaltensweisen der in oder für einen solchen Zusammenschluss handelnden einzelnen Personen. Als tatsächlicher Anhaltspunkt dafür werde bei mitgliedschaftlich verfassten Zusammenschlüssen auch die formelle Mitgliedschaft als beiderseitiger Ausdruck einer festen Zugehörigkeit mit nicht nur vorübergehendem Bindungswillen angesehen. So könne eine möglichst zutreffende Einschätzung der beobachteten Bestrebung vorgenommen werden. Dementsprechend sehe die „Arbeitsanleitung für die Behandlung personenbezogener Daten im Bereich der Auswertung (Verkartungsplan)“ eine Zeitspeicherung der Mitgliedschaft sowohl in der amtsinternen Personenarbeitsdatei als auch in der Verbunddatei NADIS vor. Nicht in jedem Fall sei dabei die Feststellung über den Besitz eines Mitgliedsausweises erforderlich. Werde eine mindestens dreimalige Teilnahme an internen Zusammenkünften des beobachteten Personenzusammenschlusses bekannt, so werde nach Entscheidung des zuständigen Referenten des höheren Dienstes unter Würdigung der Gesamtumstände eine Mitgliedschaft vermutet. Erhalte die Landesverfassungsschutzbehörde von bestimmten Tatsachen Kenntnis, wonach eine Person nicht mehr Mitglied eines beobachteten Personenzusammenschlusses sei oder keinerlei Unterstützungshandlungen wie Beitragszahlungen mehr leiste, würden ihre Daten im Rahmen der gesetzlichen Prüfungsfristen wieder gelöscht.

Im Übrigen habe man sich im Ministerium des Innern und für Sport Rheinland-Pfalz über die vom Berliner Datenschutzbeauftragten übermittelte Rechtsauffassung des LfD Rheinland-Pfalz verwundert gezeigt. Denn diese Ansicht, die das Innenministerium für eine Überinterpretierung der Gesetzesbegründung halte, habe der rheinland-pfälzische Datenschutzbeauftragte weder im Gesetzgebungsverfahren noch anlässlich von Prüfbesuchen geäußert. Das Ministerium des Innern und für Sport Rheinland-Pfalz habe klargestellt, dass eine nachdrückliche Unterstützung auch durch eine bloße Mitgliedschaft erfolgen könne und sich gegen ein Erfordernis weiterer Indizien ausgesprochen, da dies nicht aus dem Gesetz ableitbar sei.

Nach der Einschätzung des LfD dürften die Unterschiede in der Sache allerdings geringer sein, als die im letzten Absatz wiedergegebene angebliche Äußerung des Innenministeriums des Landes Rheinland-Pfalz vermuten lassen könnte:

Übereinstimmung besteht sicherlich darin, dass die Unterstützung einer verfassungsfeindlichen Organisation nicht allein durch das formale Kriterium der Mitgliedschaft bestimmbar ist. So gibt es einerseits die Möglichkeit, eine solche Organisation intensiv zu unterstützen, ohne Mitglied zu sein. Andererseits allerdings dürfte auch außer Streit stehen, dass es Formen der Mitgliedschaft gibt, etwa diejenige, die mit dem Begriff „Karteileiche“ bezeichnet wird, die keine aktive Unterstützung einer verfassungsfeindlichen Organisation im Sinne des Landesverfassungsschutzgesetzes begründen. Darauf deutet auch das vom Ministerium des Innern und für Sport genannte Kriterium hin, wonach dann, wenn eine Person keinerlei Unterstützungshandlungen wie Beitragszahlungen mehr leiste, ihre Daten im Rahmen der gesetzlichen Prüfungsfristen wieder gelöscht werden würden.

Die Erörterungen zu diesem Thema sind derzeit noch nicht abgeschlossen.

6.6 Örtliche Feststellungen im Bereich des Verfassungsschutzes

Im Berichtszeitraum fanden erneut örtliche Feststellungen beim Verfassungsschutz statt. Gegenstand der Prüfungen waren automatisiert geführte Dateien sowie personenbezogene Vorgänge und Sachakten. Hervorzuheben ist die bereitwillige Mitwirkung der geprüften Stelle.

Im technischen Bereich wurden Empfehlungen zur Verbesserung des Datenschutzes ausgesprochen, denen weitgehend gefolgt worden ist. Ein Verstoß gegen datenschutzrechtliche Bestimmungen war nicht zu rügen.

7. Justiz

7.1 Grundsätzliches zum Verhältnis Datenschutz und Justiz

Nach wie vor ist die Grundsatzfrage zwischen dem Ministerium der Justiz und dem LfD umstritten, wie weit der Begriff der „Justizverwaltung“ zu interpretieren ist und dementsprechend, in welchem Umfang dem LfD Kontrollbefugnisse zustehen und Beratungspflichten obliegen. Die Kontroverse wurde im Einzelnen im 16. Tb., Tz. 7, dargestellt. Nunmehr hat auch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hierzu eine einheitliche Auffassung formuliert, die mit der des LfD übereinstimmt (s. Anlage 10).

Aus der Sicht des LfD sollte die anstehende Novellierung des Landesdatenschutzgesetzes (s. o. Tz. 3.3) dazu genutzt werden, Klarstellungen im Sinne des Grundrechts auf informationelle Selbstbestimmung und im Sinne der Bürger in das Gesetz aufzunehmen.

Unabhängig von dieser rechtlichen Kontroverse ist es dem LfD allerdings ein Anliegen zu betonen, dass die Justizbehörden im Berichtszeitraum, insbesondere auch das Ministerium der Justiz, den Informationsbedürfnissen des LfD bereitwillig nachgekom-

men sind. Seine inhaltlichen Anregungen sind – wenn ihnen auch nicht in jedem Fall gefolgt wurde – doch sachlich gewürdigt worden. Damit hat sich das Verhältnis zur Justiz insgesamt entkrampft. Dies ist sicherlich auch ein entscheidendes Verdienst des aus dem Amt geschiedenen Ministers der Justiz, dessen Rückzug aus dem Amt aus gesundheitlichen Gründen der LfD außerordentlich bedauert.

7.2 Gesetzgebung im Justizbereich

Der Bundesgesetzgeber hat zwar nunmehr eine Reihe von seit Jahren von den Datenschutzbeauftragten angemahnten Gesetzgebungsvorhaben (wie Novellierung des Strafvollzugsgesetzes, Justizmitteilungsgesetz) abgeschlossen. Das Untersuchungshaftvollzugsgesetz, das ebenfalls datenschutzrechtliche Bedeutung besitzt, liegt mit einem Referentenentwurf vor. Dazu hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder einige Anforderungen aus ihrer Sicht formuliert (s. den Text des Beschlusses in der Anlage 17). Auch zur Frage von Bild-Ton-Aufzeichnungen bei Vernehmungen im Strafverfahren, die zwischenzeitlich (aus datenschutzrechtlicher Sicht aber nicht völlig ausreichend) in der Strafprozessordnung geregelt sind (§§ 168 e, 247 a, 255 a StPO), hat sich die Konferenz geäußert (vgl. Anlage 2).

Wichtige Gesetzgebungsvorhaben stehen noch aus (s. den Konferenzbeschluss in Anlage 6); insbesondere ist zu beklagen, dass die Ergänzung der Strafprozessordnung um datenschutzrechtliche Grundnormen zur automatisierten Datenspeicherung bei den Ermittlungsbehörden, den Rechten der Betroffenen in diesem Zusammenhang und auch den Regelungen zur Datennutzung für die wissenschaftliche (kriminologische) Forschung nicht vorangebracht worden ist.

7.3 Telefonüberwachungsmaßnahmen – neue Techniken, alte Probleme

Das Ministerium der Justiz hat eine Verwaltungsvorschrift zur Durchführung der Telefonüberwachung im Einvernehmen mit dem Ministerium des Innern und für Sport erlassen, durch die einige Fragen im Zusammenhang mit dem technisch-organisatorischen Datenschutz bei der Durchführung solcher Maßnahmen zufrieden stellend gelöst worden sind. Zu den hier bestehenden datenschutzrechtlichen Anliegen s. 15. Tb., Tz. 7.5.3 und 16. Tb., Tz. 7.1.4. So sind die Fragen der Protokollierung, der Vernichtung von Unterlagen aus Telekommunikationsüberwachungen und der Verantwortlichkeit bei der Löschung von Speichermedien nunmehr klarer geregelt worden.

Insbesondere folgende Probleme bestehen allerdings weiterhin:

– Es fehlt an einer zureichenden Datengrundlage, um flächendeckend die Wirksamkeit und Angemessenheit von Telekommunikationsüberwachungen im Verhältnis zu den damit einhergehenden Beeinträchtigungen auch von unbeteiligten Dritten beurteilen zu können. Es bestehen unzureichende Evaluationsmöglichkeiten aufgrund unzureichender Statistiken. So ist unklar, in welchem Umfang bundesweit tatsächlich – wie der Presse zu entnehmen war – in den letzten beiden Jahren die Zahl der Abhörmaßnahmen gestiegen ist. In den Statistiken der Netzbetreiber wird die Zahl der abgehörten Anschlüsse (wobei mehrere Anschlüsse einem Inhaber zugeordnet sein können), in den Justizstatistiken die Zahl der betroffenen Verfahren bzw. der betroffenen Anschlussinhaber erfasst. Vergleichbar sind jeweils nur identische Datenkategorien. Transparenz in diesem Bereich ist sicher für alle Beteiligten eminent bedeutsam. Die Zahlen der Justizbehörden ergeben für Rheinland-Pfalz keinen Anstieg der Abhörmaßnahmen, im Gegenteil: 1997 waren es in 125 Strafverfahren 202 Anschlussinhaber, 1998 in 118 Strafverfahren 195 Anschlussinhaber.

– Aus seiner Kontrollpraxis bei Staatsanwaltschaften und Polizeidienststellen heraus kann der LfD zu Telefonabhörmaßnahmen auf der Basis von Stichproben ergänzend Folgendes anmerken: Etwa zwei Drittel aller Maßnahmen betreffen Rauschgiftdelikte. In diesem Bereich sind alternative, weniger belastende Aufklärungsmaßnahmen in der Regel nicht vorhanden. In nahezu allen geprüften Fällen waren die gewonnenen Erkenntnisse für die Ermittlungsarbeit zumindest förderlich. Missbräuchliche Nutzungen der Maßnahmen waren nicht festzustellen.

– Auch das Problem der Aufzeichnung von Verteidigertelefonaten ist noch nicht zufrieden stellend gelöst worden. Die eingesetzte digitalisierte Technik hat zunächst Erwartungen geweckt, dass es hier eine technische Lösung dergestalt geben könnte, Telefonate mit Anschlüssen, die einem der Polizei bekannten Strafverteidiger zuzuordnen sind, technisch von der Aufzeichnung auszunehmen. Nunmehr hat sich allerdings ergeben, dass in den meisten Fallkonstellationen die Verbindungsdaten erst nach der Gesprächsführung, zeitlich also nachdem die Inhaltsdaten bereits aufgezeichnet worden sind, an die Schnittstelle der polizeilichen Telekommunikationsüberwachung übermittelt werden. Zu den technischen Einzelheiten s. unten Tz.21.2.11.2.

Dies bleibt aus der Sicht des LfD unbefriedigend.

7.4 Parlamentarische Kontrolle von Lauschangriffen in den Bundesländern

Zur Begleitung des sog. „Großen Lauschangriffes“ ist insbesondere auch eine Berichtspflicht der Staatsanwaltschaften an ihre jeweils zuständige oberste Justizbehörde sowie der Bundes- und Landesregierungen an die für sie zuständigen Parlamente geschaffen worden (Art. 13 Abs. 6 GG, § 100 e StPO). Eine Meinungsverschiedenheit zwischen den Landesjustizverwaltungen einerseits und den Datenschutzbeauftragten (teilweise auch den Landesparlamenten) andererseits hat sich an der Frage entzündet, ob und in welchem Umfang die Landesjustizminister verpflichtet sind, ihren Landtagen über den Einsatz des Großen Lauschangriffs zu Strafverfolgungszwecken Bericht zu erstatten. Die Landesjustizminister sind der Auffassung, nur auf konkrete An-

forderung hin den Landtag unterrichten zu müssen; die Gegenauffassung meint, aus den zitierten Rechtsgrundlagen ergebe sich eine Pflicht der Justizministerien bzw. Landesregierungen, den Landtagen von Amts wegen ohne besondere Aufforderung regelmäßig Bericht zu erstatten.

Die Auffassung der Datenschutzbeauftragten zu dieser Frage ist in der Anlage 16 dargestellt.

Aus Sicht des LfD hat diese Differenz in den Auffassungen keine wesentliche Auswirkung: Der Minister der Justiz des Landes hat bereits deutlich erklärt, dass er auf Aufforderung des Landtags jederzeit bereit ist, diesem über den Einsatz des Großen Lauschangriffs zu Strafverfolgungszwecken zu berichten. Die Frage, ob dies nur auf Aufforderung oder von Amts wegen regelmäßig erfolgen soll, ist demgegenüber von eher nachrangiger Bedeutung.

Bedeutsamer ist die Frage, ob die Berichte des Justizministers Gegenstand einer öffentlichen Erörterung sein können oder ob der Landtag Vorkehrungen zur Geheimhaltung treffen muss.

Der LfD ist der Auffassung, dass – soweit anonymisierte Informationen ohne Personenbezug zur Verfügung stehen – diese in öffentlichen Sitzungen der Parlamente zum Gegenstand der Diskussion gemacht werden sollten. Die Frage, ob die gesetzlichen Ermächtigungsgrundlagen in diesem Zusammenhang für die Strafverfolgungsbehörden geeignet, angemessen und im engeren Sinne auch verhältnismäßig eingesetzt werden, ist für Fragen der künftigen Gesetzgebung von erheblicher Bedeutung. Dies sollte so weit wie möglich öffentlich erörtert werden. Wenn einzelfallbezogene Informationen allerdings personenbeziehbar sein sollten, ist es auch nach seiner Auffassung angemessen, Schutzvorkehrungen zu treffen, damit diese Informationen nicht in die Öffentlichkeit gelangen.

Auch insoweit dürfte kein grundsätzlicher Meinungsunterschied mit dem Justizministerium bestehen.

Im Übrigen obliegt die Datenschutzkontrolle insoweit nicht dem LfD, sondern dem Ältestenrat des Landtags.

7.5 DNA-Analyse in Strafverfahren

Seit dem Urteil des Landgerichts Berlin vom 14. Dezember 1988 (NJW 1989, S. 787) hat die Rechtsprechung die DNA-Vergleichsanalyse als ein grundsätzlich zulässiges Beweismittel anerkannt. Aus datenschutzrechtlicher Sicht wurden von Beginn an folgende Forderungen formuliert:

- Da die DNA-Analyse die Gefahr in sich birgt, überschießende Erkenntnisse über die Identität von Spur- und Vergleichsmaterial hinaus zu ergeben, wurde eine gesonderte gesetzliche Grundlage für erforderlich gehalten, die den Einsatz dieses Beweismittels insbesondere im Strafverfahren regeln sollte.
- Dabei wurde neben einer restriktiven Formulierung der Voraussetzungen des Einsatzes dieses Beweismittels gefordert, dass ein Verbot der Gewinnung von Zusatzerkenntnissen statuiert werden sollte.
- Auch die Aufnahme von DNA-Daten in Dateien sollte nur zugelassen werden, wenn ein Richter dies unter engen materiellen Voraussetzungen für zulässig erklärt hat.
- Es sollten sowohl Regelungen für die Aufbewahrung der Untersuchungsmaterialien wie technisch-organisatorische Schutzmaßnahmen bei der Untersuchung selbst und der anschließenden Speicherung in Dateien formuliert werden.

Diesen Anliegen ist der Gesetzgeber zum größten Teil gefolgt. Zwar hat die Rechtsprechung auch ohne besondere gesetzliche Grundlage eine Reihe von Zweifelsfragen in diesem Zusammenhang geklärt: So hat sich das Bundesverfassungsgericht beispielsweise mit der Durchführung von DNA-Analysen auf freiwilliger Basis und auch auf der Grundlage des § 81 a StPO befasst (Beschluss vom 2. August 1996, Az.: 2 BvR 1511/96, NJW 1996, S. 3071; Beschluss vom 18. September 1995, Az.: 2 BvR 103/92, NJW 1996, S. 771). Der Gesetzgeber hat dennoch zur Klarstellung des Erlaubten in diesem Zusammenhang folgende Gesetze geschaffen:

- §§ 81 e und f StPO, eingefügt durch StVÄG vom 17. März 1997.
- DNA-Identitätsfeststellungsgesetz vom 7. September 1998, BGBl. I S. 2646.
- Gesetz zur Änderung des DNA-Identitätsfeststellungsgesetzes vom 2. Juni 1999, BGBl. I S. 1242.
- Für die Dateispeicherung von DNA-Daten sind – in Ergänzung zu § 3 DNA-IFG – § 8 BKAG sowie die Errichtungsanordnung des BKA vom August 1998 (BKA-Blatt Nr. 161 vom 24. August 1998) maßgeblich.

Mit diesen Vorschriften ist Folgendes klargestellt:

a) Zur Feststellung von Tatsachen, die für ein laufendes Verfahren von Bedeutung sind, dürfen auch molekulargenetische Untersuchungen an Körpermaterialien durchgeführt werden, die von Beschuldigten oder anderen Personen (i. S. d. § 81 c Abs. 1 StPO) stammen (§ 81 e Abs. 1 StPO). Die molekulargenetischen Untersuchungen dürfen nur so weit durchgeführt werden, wie sie zur Feststellung der Abstammung oder der Tatsache, ob aufgefundenes Spurenmaterial von Beschuldigten oder Verletzten stammt, erforderlich sind. Feststellungen über andere als diese Tatsachen dürfen nicht erfolgen. Hierauf gerichtete Untersuchungen sind unzulässig.

b) Eine solche Untersuchung bedarf der Anordnung durch den Richter (§ 81 a Abs. 2 StPO).

c) Entsprechende Untersuchungen dürfen auch an Spurenmaterial durchgeführt werden. Auch dafür gilt der Richtervorbehalt (§ 81 e Abs. 2 StPO; trotz des klaren Gesetzeswortlauts wird dies neuerdings bestritten, vgl. Sprenger/Fischer, NJW 1999, 1830, Zur Erforderlichkeit der richterlichen Anordnung von DNA-Analysen).

d) Für Zwecke künftiger Strafverfahren dürfen die Entnahme von Körpermaterial und entsprechende molekulargenetische Untersuchungen bei einem Beschuldigten ebenfalls durchgeführt werden. Voraussetzung ist aber, dass dem Beschuldigten eine Straftat von erheblicher Bedeutung, insbesondere ein Verbrechen, ein Vergehen gegen die sexuelle Selbstbestimmung, eine gefährliche Körperverletzung, ein Diebstahl in besonders schwerem Fall oder eine Erpressung vorgeworfen wird (§ 81 g Abs. 1 StPO).

e) Schließlich dürfen solche Untersuchungen auch an Verurteilten durchgeführt werden, wenn sie wegen einer der genannten Straftaten rechtskräftig verurteilt oder nur wegen erwiesener oder nicht auszuschließender Schuldunfähigkeit, auf Geisteskrankheit beruhender Verhandlungsunfähigkeit oder fehlender oder nicht ausschließbar fehlender Verantwortlichkeit nicht verurteilt worden sind und die entsprechende Eintragung im Bundeszentralregister oder Erziehungsregister noch nicht getilgt ist (§ 2 DNA-IFG). Auch bezüglich der Untersuchung Verurteilter gilt der Richtervorbehalt, § 2 Abs. 2 DNA-IFG.

f) Die erhobenen DNA-Identifizierungsmuster dürfen unter der Voraussetzung in einer Datei beim BKA gespeichert werden, dass entweder Beschuldigte oder Verdächtige betroffen sind, soweit dies erforderlich ist, weil Grund zur Annahme besteht, dass gegen sie Strafverfahren zu führen sind; für andere Personen als Beschuldigte oder Verdächtige müssen bestimmte Tatsachen die Annahme rechtfertigen, dass die Betroffenen Straftaten von erheblicher Bedeutung begehen werden (§ 3 DNA-IFG, § 8 Abs. 2 und 5 BKAG).

g) Zur Feststellung, welche verurteilten Personen in Betracht kommen, einer entsprechenden DNA-Analyse unterzogen zu werden, darf das Bundeszentralregister Auswertungen mit Straftaten als Suchkriterium durchführen; der Klarstellung dieser Befugnis dienen die §§ 2 a bis 2 e DNA-IFG mit einem ausführlichen Straftatenkatalog, der in der Anlage zu § 2 c aufgeführt ist.

h) Der Gesetzgeber hat auch technisch-organisatorische Sicherungsmaßnahmen vorgegeben, um Missbräuchen vorzubeugen: So hat er eine unverzügliche Vernichtungspflicht des untersuchten Körperzellenmaterials in § 81 g StPO angeordnet; dies gilt für die Fälle, in denen die DNA-Analyse bei Beschuldigten oder Verurteilten zum Zweck der künftigen Straftatenverfolgung erfolgt ist. Außerdem ist ausdrücklich geregelt, dass die die Untersuchung durchführenden Stellen organisatorisch und sachlich getrennt von den ermittlungsführenden Behörden tätig sein müssen (§ 81 f Abs. 2 StPO). Eine Sicherungsmaßnahme stellt letztendlich auch die Vorgabe dar, dass den Sachverständigen das Untersuchungsmaterial ohne Mitteilung des Namens, der Anschrift und des Geburtstages und -monates des Betroffenen zu übergeben ist (§ 81 f Abs. 2 StPO).

Mit all diesen Vorgaben wird datenschutzrechtlichen Vorstellungen weitgehend entsprochen. Unklar sind allerdings folgende Fragen geblieben:

a) Ist vor Aufnahme eines DNA-Profils in die DNA-Datenbank beim BKA in jedem Fall eine entsprechende richterliche Prognose und Entscheidung erforderlich?

   Dies ist für den Fall zweifelhaft, dass zur Aufklärung von Straftaten gem. § 81 e Abs. 1 StPO eine molekulargenetische Untersuchung durchgeführt wird und das Ergebnis dieser Untersuchung anschließend gem. § 3 Satz 3 DNA-IFG in die BKA-Datei eingespeist werden soll. Die Vorschrift verweist nicht ausdrücklich für die Frage der Dateieinspeicherung und Prognosestellung auf den Richtervorbehalt in § 81 a Abs. 2 StPO. Daraus könnte geschlossen werden, dass die Prognose von den Polizeibehörden, nicht aber vom Richter vorzunehmen sei. Der LfD hält auch in diesem Fall eine richterliche Entscheidung für angemessen: Es ist nicht einsichtig, warum die entsprechende Prognose bei Verurteilten und bei Beschuldigten, deren DNA-Analyse zur konkreten Verdachtsabklärung nicht gebraucht wird, vom Richter, bei anderen Beschuldigten aber von der Polizei durchgeführt werden sollte.

b) Unklar ist weiter, in welchem Umfang das Einverständnis Betroffener als ausreichende Grundlage für Maßnahmen in diesem Zusammenhang angesehen werden kann: Ist die Probeentnahme, die Analyse und der Abgleich in konkreten Verfahren und ist die Dateispeicherung auf freiwilliger Basis zulässig?

   Hierzu enthält das Gesetz keine Aussage. Der LfD vertritt in Übereinstimmung mit der Landesregierung die Auffassung, dass zwar die Probeentnahme – möglicherweise auch die Analyse und der Abgleich in einem konkreten Strafverfahren –, keinesfalls aber die Dateispeicherung zur künftigen Strafverfolgung auf der Basis der Einwilligung zulässig ist (s. das Schreiben der Konferenz der Datenschutzbeauftragten des Bundes und der Länder an den Vorsitzenden der Innenministerkonferenz, Anlage 19; zur Gegenansicht vgl. Sprenger/Fischer, NJW 1999, 1830). Er hat sich an der datenschutzgerechten Formulierung entsprechender Formular-Einwilligungserklärungen im Land beteiligt.

c) Reicht die Regelung der Speichervoraussetzungen und Modalitäten in § 3 Abs. 1 DNA-IFG und § 8 BKAG sowie in der dazu gem. § 34 BKAG erlassenen Errichtungsanordnung aus oder muss es für die DNA-Datei ein besonderes Gesetz geben, in dem diese Voraussetzungen geregelt werden?

Hier vertritt der LfD die Auffassung, dass die wesentlichen Vorgaben der Errichtungsanordnung (insbesondere zur Löschung von Eintragungen und Protokollierung von Abrufen) durch den Gesetzgeber erfolgen sollten: Abgesehen davon, dass die Errichtungsanordnung „VS-nfD“ eingestuft und damit der Öffentlichkeit entzogen ist, sind dies für die Grundrechte der Betroffenen maßgebliche Festlegungen, für die der Gesetzgeber die Verantwortung übernehmen sollte.

Im praktischen Vollzug sind weiterhin folgende Fragen problematisiert worden:

a) Dürfen die Daten aus der landeseigenen DNA-Datei, die beim LKA eingerichtet worden ist, ohne erneute richterliche Entscheidung in die DNA-Datei des Bundes überführt werden?

Mit der Landesregierung ist der LfD der Auffassung, dass die neue Rechtslage eine solche Nachholung richterlicher Anordnungen erfordert.

b) In welcher Form dürfen die Proben gekennzeichnet werden, um dem Sachverständigen eine eindeutige Zuordnung zu ermöglichen und um insbesondere auch beim Rücklauf an die auftraggebenden Dienststellen Verwechslungen zu vermeiden? Ist es zulässig, hier die Initialen der Betroffenen zu verwenden?

Der LfD sieht in der Verwechslungsgefahr bei Proben und Analyseergebnissen ein ernst zu nehmendes, die Betroffenen ggf. stark belastendes Risiko. Um diese Gefahr möglichst gering zu halten, hat er keine Bedenken gegen die Nutzung der Initialen der Betroffenen bei der Probenkennzeichnung erhoben.

c) In welcher Form dürfen die Polizeibehörden darüber unterrichtet werden, dass über bestimmte Verdächtige ein DNA-Analysemuster in der BKA-Datei vorhanden ist? Darf dies durch einen Merker im sog. „INPOL-Verfahren“ erfolgen?

Auch hiergegen hat der LfD keine Bedenken erhoben: Die Vermeidung doppelter und damit überflüssiger Datenerhebungen hat auch datenschutzrechtliche Bedeutung.

d) Gibt es „Vorstadien“ molekulargenetischer Untersuchungen, für die noch kein richterlicher Beschluss erforderlich ist? Wo liegt die Grenze zur gesetzlichen Schwelle, ab der eine richterliche Anordnung vorliegen muss?

Der LfD hat deutlich herausgestellt, dass das Gesetz an jede molekulargenetische Untersuchung unabhängig von ihrer Intensität das Erfordernis der richterlichen Anordnung knüpft, da das hier eingesetzte wissenschaftlich-technische Analyse-Instrumentarium als für das Persönlichkeitsrecht gefährdend angesehen wird. Damit fallen auch „Voruntersuchungen“ unter Nutzung dieses Instrumentariums unter die gesetzlichen Anforderungen.

Die Streitfrage, welches Gericht konkret für die jeweilige Entscheidung zuständig ist, hat geringere datenschutzrechtliche Bedeutung, hat aber in der Praxis zu erheblichen Diskussionen geführt.

Aus datenschutzrechtlicher Sicht ist zusammenfassend festzustellen:

Die Nutzung der DNA-Analyse zu Zwecken des Strafverfahrens ist gesetzlich besonders geregelt worden, wobei Fragen von einiger Bedeutung offen geblieben sind. Datenschutzrechtliche Defizite lassen sich allerdings durch Auslegung der vorhandenen Rechtsgrundlagen einigermaßen zufrieden stellend beheben. Im Ergebnis ist nicht erkennbar, dass bürgerliche Freiheitsrechte durch dieses neue Analysemittel der Strafverfolgungsbehörden entscheidend beschnitten oder eingeschränkt worden wären. Der Bundesgesetzgeber sollte die bestehenden Regelungsdefizite allerdings schnellstmöglich beseitigen.

7.6 Täter-Opfer-Ausgleich und Datenschutz

Kernstück der datenschutzrechtlichen Überlegungen zum Täter-Opfer-Ausgleich ist die Frage, ob in diesem Zusammenhang privatrechtliche Institutionen zur Durchführung des Ausgleichsverfahrens Informationen insbesondere über Opfer von Straftaten erhalten und dann den Kontakt mit dem Opfer aufnehmen dürfen, ohne dass die Betroffenen davon Kenntnis oder darin eingewilligt haben.

Ein datenschutzrechtlich relevanter und unverhältnismäßiger Eingriff liegt dann vor, wenn ohne Kenntnis und möglicherweise sogar gegen den Willen des betroffenen Opfers Informationen an privatrechtlich organisierte Dritte übermittelt werden. Auf der Grundlage des geltenden Rechts hält der LfD dies für nicht zulässig; entsprechend hat er sich gegenüber dem Justizministerium wiederholt geäußert. Dieses vertritt – auch im Hinblick auf die derzeitigen Bemühungen des Bundesgesetzgebers zur Schaffung einer gesetzlichen Grundlage für dieses Verfahren – die entgegengesetzte Auffassung; der LfD kann der Begründung des Ministeriums allerdings nicht folgen.

Soweit der nunmehr vorliegende Gesetzentwurf der Bundesregierung (BR-Drs. 325/99 vom 28. Mai 1999) in diesem Zusammenhang in § 155 a Satz 3 StPO vorsieht, dass nur der ausdrücklich geäußerte entgegenstehende Wille des Verletzten dazu führt, dass

keine Datenübermittlungen an Opferausgleichsstellen erfolgen sollen, hält er dies für nicht ausreichend. Aus datenschutzrechtlicher Sicht sollte geregelt werden, dass vor Einleitung des Ausgleichsverfahrens das betroffene Opfer über die dahin gehende Absicht der Strafverfolgungsbehörden zu unterrichten ist und dass der ausdrücklich geäußerte entgegenstehende Wunsch des Opfers zwingend dazu führt, dass keine Daten an Dritte übermittelt werden.

Das Justizministerium hat im Gegensatz hierzu aus folgenden Gründen abgelehnt, diesen Vorschlag zu unterstützen: Eine vor der Einschaltung privater Schlichtungsstellen von den Justizstellen einzuholende Einwilligung führe dazu, dass dieses kriminalpolitisch wichtige Institut nicht genutzt werde. Erst die professionelle Tätigkeit der Schlichter mit ihrem Selbstverständnis als „objektive Dritte mit dem Gebot der Unterstützung jeder Partei“ könnten wirksame Überzeugungsarbeit leisten; nur dann könne der Rechtsfriede dauerhafter als bei herkömmlichen Verfahren sichergestellt werden, wenn durch die „fachlich geleitete Auseinandersetzung“ der „am strafrechtlich relevanten Konflikt beteiligten Parteien im Idealfall Verständnis und wechselseitige Toleranz geweckt werden“.

Dem kann sich der LfD nicht anschließen: Im Strafverfahren geht es gerade nicht um eine Auseinandersetzung zwischen gleichberechtigten Parteien; mit dieser Argumentation wird der vom Rechtsstaat zu betonende Unterschied zwischen Täter und Opfer verwischt. Das Opfer ist zu unterstützen. Es darf nicht so weit kommen, dass in die Rechte des Opfers eingegriffen wird, damit ihm seitens der Vermittlungsstellen erklärt werden kann, dass und wie er für den Täter Toleranz und Verständnis aufzubringen habe. Der LfD fordert deshalb mit Entschiedenheit, dass an der Voraussetzung der Einwilligung vor solchen Datenübermittlungen festgehalten wird.

7.7 Anspruch eines Geschädigten auf die Bekanntgabe der Berufs-Haftpflichtversicherung eines Rechtsanwaltes durch die Rechtsanwaltskammer

Der LfD wird nicht selten auch dann angerufen, wenn Bürger den Eindruck haben, ihnen werde zu Unrecht unter Berufung auf Datenschutz eine Information vorenthalten, die für sie von wesentlicher Bedeutung ist. In einer solchen Situation hat sich ein Gewerbetreibender verzweifelt an den LfD gewandt: Er war von seinem Rechtsanwalt betrogen worden. Diesem war zwischenzeitlich die Anwaltszulassung entzogen worden, er hielt sich an einem unbekannten Ort auf. Der Geschädigte bemühte sich nun herauszufinden, bei welcher Berufs-Haftpflichtversicherung der Anwalt versichert war. Er hoffte, durch eine unmittelbare Geltendmachung seines Schadens bei der Haftpflichtversicherung etwas erreichen zu können. Weder das Oberlandesgericht, das für die Zulassung eines Rechtsanwalts zuständig ist, noch die Rechtsanwaltskammer, die die standesrechtliche Aufsicht über den Anwalt führt, waren bereit, diesem Anliegen zu entsprechen. Beide beriefen sich auf den Datenschutz.

Der LfD war und ist der Auffassung, dass dies im vorliegenden Zusammenhang zu Unrecht geschah: Nach dem LDSG ist es zulässig, Daten an eine Privatperson zu übermitteln, wenn diese ein rechtliches Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft macht und kein Grund zur Annahme besteht, dass überwiegende schutzwürdige Interessen der Betroffenen entgegenstehen (§ 16 Abs. 1 Nr. 3 LDSG). Diese Konstellation war vorliegend gegeben: Der Versuch, einen durch Betrug verursachten Schaden ersetzt zu erhalten, begründet ein rechtliches Interesse; die Rechtsordnung bietet hierfür eine Reihe von Wegen an, um dieses Interesse durchzusetzen. Ein überwiegendes schutzwürdiges Interesse des Schädigers an der Geheimhaltung seiner Haftpflichtversicherung ist nicht ersichtlich: Diese ist für Fälle abgeschlossen, in denen durch das Handeln des Versicherten ein Schaden entsteht. Schutzwürdige Interessen waren und sind in diesem Zusammenhang nicht ersichtlich.

Es war nicht ganz leicht, die Anwaltskammer von dieser Rechtsauffassung zu überzeugen. Letztlich hat sie dem Anliegen des geschädigten Bürgers aber entsprochen. Eine Datenübermittlung durch das Oberlandesgericht in diesem Zusammenhang wäre in gleicher Weise zu beurteilen gewesen.

7.8 Die datenschutzrechtlichen Ergänzungen des Strafvollzugsgesetzes

Aufgrund des 4. Änderungsgesetzes zum Strafvollzugsgesetz vom 26. August 1998 (BGBl. I S. 2461) sind insbesondere folgende konkrete datenschutzrechtlich relevante neue Anforderungen an die Strafvollzugspraxis gestellt worden:

Die Überwachung von Unterhaltungen des Strafgefangenen mit Besuchern darf nur aufgrund einer jeweiligen Einzelfallentscheidung erfolgen, § 27 Abs. 1 Satz 2. Im Falle einer Telefongesprächsüberwachung ist der Gesprächspartner des Gefangenen vor der beabsichtigten Überwachung hierüber zu unterrichten. Der Strafgefangene selbst ist ebenfalls rechtzeitig vor dem beabsichtigten Telefongespräch über die vorgesehene Überwachung zu unterrichten, § 32 Sätze 3 und 4. Für die Informationen, die bei der Besuchs- und Postüberwachung gewonnen worden sind, gilt eine besondere Zweckbindung gem. § 180 Abs. 8. Die bei erkennungsdienstlichen Maßnahmen erlangten Daten unterliegen einer besonderen Zweckbindung (insbesondere für Fahndung und die Durchführung von Straf- und Ordnungswidrigkeitenverfahren), § 86 Abs. 2 Satz 3. Für erkennungsdienstliche Materialien besteht eine besondere Vernichtungspflicht bei Entlassung des Strafgefangenen, wenn dieser die Vernichtung beantragt; der Gefangene ist über sein Antragsrecht zu unterrichten, § 86 Abs. 3. Bei der Datenerhebung besteht gegenüber den Betroffenen eine Erstbefragungspflicht, § 179 Abs. 2 Satz 1. Daten über Dritte (nicht Gefangene) dürfen nur erhoben werden, wenn diese Daten „unerlässlich“ sind, § 179 Abs. 3. Für diese Daten besteht eine besonders enge Zweckbindung, § 180 Abs. 9. Eine Datenerhebung bei Dritten darf nur dann erfolgen, wenn die Voraussetzungen des § 13 Abs. 2 BDSG vorliegen, § 179 Abs. 2. Der Gefangene ist über diese Datenerhebung bei Dritten zu unterrichten, § 179 Abs. 4. Für Daten der Strafvollzugsbehörden gilt generell eine Bindung an enumerativ in § 180 Abs. 2 und 4 aufgezählte Zwecke. Die Mitteilung über den Aufenthaltsort des Gefangenen an

öffentliche Stellen und an private Empfänger ist unter jeweils besonderen Voraussetzungen zulässig, § 180 Abs. 5. Der Gefangene ist vor den Mitteilungen anzuhören. Für alle Daten, die von den Strafvollzugsbehörden übermittelt worden sind, gilt beim Empfänger eine besondere Zweckbindung, § 181 Satz 1. Private Datenempfänger sind darauf besonders hinzuweisen, § 181 Satz 2. Gesundheitsdaten sowie Daten über das religiöse und weltanschauliche Bekenntnis dürfen innerhalb der Anstalt nicht allgemein kenntlich gemacht werden, § 182 Abs. 1. Unter bestimmten Voraussetzungen darf der Anstaltsarzt dem Arztgeheimnis unterliegende Daten weitergeben. Vor der ärztlichen Untersuchung sind Gefangene darauf hinzuweisen, § 182 Abs. 2. Für in Dateien gespeicherte personenbezogene Daten gelten besondere (zweijährige) Löschungsfristen, § 184 Abs. 1. Für Gefangenenpersonalakten, Gesundheitsakten und Krankenblätter gilt eine generelle zwanzigjährige maximale Aufbewahrungsfrist; für Gefangenenbücher beträgt die Frist dreißig Jahre, § 184 Abs. 2. Die Betroffenen haben einen Auskunftsanspruch, ausnahmsweise (bei einem besonderen rechtlichen Interesse) auch einen Akteneinsichtsanspruch, § 185. Es besteht eine Pflicht zur Anlegung von Geräte- und Dateiverzeichnissen gem. § 18 Abs. 2 BDSG, § 187.

7.8.1 Defizite des Gesetzes aus datenschutzrechtlicher Sicht

Zunächst bedeutet die ergänzende Anwendung des Bundesdatenschutzgesetzes an Stelle der jeweiligen Landesdatenschutzgesetze einen erheblichen Bedeutungsverlust für die Landesdatenschutzgesetze.

Die vorgesehenen Löschungspflichten für Akten sind aus der Sicht des LfD insgesamt zu großzügig bemessen; es fehlen differenzierte Regelungen für besonders sensitive Aktenbestandteile, beispielsweise Listen von Telefonverbindungsdaten, Informationen über Brief- und Telefonüberwachungen, Daten, die Dritte betreffen.

Die Unterscheidung zwischen dem Begriff der Erforderlichkeit und dem der Unerlässlichkeit von Daten führt zu einer Aufweichung des Erforderlichkeitsbegriffs (§§ 179 Abs. 3, 182 Abs. 2).

Die Voraussetzungen der Ausnahmen für die Unterrichtungspflicht gegenüber dem Gefangenen gem. § 179 Abs. 4 Nr. 3 sind zu unklar. Aus datenschutzrechtlicher Sicht wird vertreten, dass eine Zweckänderung nur bei unmittelbar drohender Gefahr (also nicht bei jeder Gefahr) und nicht zur Verfolgung aller, sondern nur besonders schwerer Straftaten zulässig sein sollte.

Die Regelung über die wissenschaftliche Forschung (§ 186) sieht völlig davon ab, die Einwilligung der Betroffenen als den Regelfall bei einer Datenerhebung zu erwähnen.

Die Restriktionen für das Akteneinsichtsrecht sind aus datenschutzrechtlicher Sicht unangemessen und nicht konform mit Artikel 10 der Europäischen Datenschutz-Richtlinie.

7.8.2 Folgerungen für den LfD

Der LfD wird auf die praktische Umsetzung der datenschutzrechtlichen Errungenschaften des Gesetzes hinwirken. Auf Länderebene wird er in Abstimmung mit den anderen Landesdatenschutzbeauftragten Konkretisierungen im Sinne von Differenzierungen und Verkürzungen der Aktenaufbewahrungsdauer anregen.
Im Übrigen werden die Datenschutzbeauftragten des Bundes und der Länder die praktischen Folgen des Gesetzesvollzugs mit dem Ziel beobachten, zu gegebener Zeit konkrete Nachbesserungsforderungen zu erheben.

7.9 Eingaben von Strafgefangenen

Die Eingaben von Strafgefangenen wegen angeblicher Verletzung ihrer Datenschutzrechte in der Justizvollzugsanstalt haben sich zahlenmäßig etwa im gleichen Rahmen wie in den vergangenen Jahren gehalten.

Sie betrafen beispielsweise folgende Fragen:

- Weitergabe von Gesundheitsdaten durch den Anstaltsarzt an andere Anstaltsbedienstete;
- die Nutzung von Erkenntnissen des Anstaltspsychologen im Rahmen von Gnadenentscheidungen, auch wenn der betroffene Strafgefangene kein Gnadengesuch gestellt hatte;
- die Einschaltung eines privaten Fotokopiergeschäftes für die Fertigung von Fotokopien für Gefangene;
- Fehlläufe von Postsendungen bzw. Fehladressierungen durch gerichtliche Geschäftsstellen;
- Einsichtnahme in Verteidigerschreiben durch Vollzugsbedienstete anlässlich einer Zellenrevision;
- Mithören von Justizbediensteten bei Nutzung des Kartentelefons; Fertigung und Aufbewahrung entsprechender Listen über geführte Telefonate;
- Fertigung von Lichtbildern für einen internen Ausweis;
- Abgabe beschriebener Einmalfarbbänder (Karbonbandkassetten) aus Schreibmaschinen als Voraussetzung eines Neukaufs.

In einigen Fällen führten diese Eingaben zu Verbesserungen des Verfahrensablaufs bzw. zu Hinweisen an die betroffenen Bediensteten, künftig größere Sorgfalt im Datenschutzinteresse zu beachten. In anderen Fällen konnte der LfD aus datenschutzrechtlicher Sicht keine Verstöße gegen den Datenschutz feststellen.

8. Schulen, Hochschulen, Wissenschaft

8.1 Schulen

8.1.1 Elternbefragung zur Errichtung einer Regionalen Schule

Aufgrund einer Eingabe betroffener Eltern ist dem LfD folgender Sachverhalt bekannt geworden:

Eine Verbandsgemeindeverwaltung hatte als Schulträger die Errichtung einer Regionalen Schule beantragt. Im Zuge dieses Antragsverfahrens hatte die Verbandsgemeindeverwaltung alle Eltern von Grundschülern bestimmter Klassen angeschrieben und Folgendes ausgeführt: Damit die Regionale Schule eingerichtet werden könne, müsse gewährleistet sein, dass auf absehbare Zeit eine ausreichende Zahl von Schülerinnen und Schülern diese Schule besuchen werde. Die Eltern würden also befragt, ob sie die Regionale Schule für ihr Kind zu wählen gewillt seien. Es handele sich hierbei um eine Bekundung mit richtungsweisender Bedeutung für die Region. Die Elternbefragung sei eine der notwendigen Voraussetzungen zur Errichtung der Regionalen Schule und solle Ausdruck geben über die Akzeptanz dieser Schulform in der Verbandsgemeinde. Die Elternbefragung erfolge in Abstimmung mit der Bezirksregierung.

Die Zulässigkeit dieser Elternbefragung hat der LfD wie folgt beurteilt:

Es bestand keine gesetzliche Pflicht der befragten Eltern, gegenüber der Verbandsgemeindeverwaltung darüber Auskunft zu erteilen, ob sie die Einrichtung einer Regionalen Schule befürworten. Ebenso wenig bestand eine entsprechende Pflicht der Befragten anzugeben, welche ihrer Kinder die Grundschule in welchem Ortsteil der Verbandsgemeinde bzw. welchen Kindergarten in welchem Jahrgang besuchten.

Damit war aus datenschutzrechtlicher Sicht eine entsprechende Befragung mit Angaben des Namens der befragten Personen nur aufgrund einer Einwilligung der Befragten zulässig. Diese konnte grundsätzlich zwar konkludent durch die Rücksendung des Fragebogens erteilt werden. Voraussetzung dafür aber, die Rücksendung als Einwilligungserklärung zu werten, wäre gewesen, dass die Befragten umfassend über die Freiwilligkeit der Datenpreisgabe, den Verwendungszweck der Daten, deren konkret beabsichtigte Nutzung (einschließlich des vorgesehenen Löschungszeitpunktes) und den möglichen Empfängerkreis aufgeklärt worden wären. Dabei waren sie auch darauf hinzuweisen, dass sie die Einwilligung verweigern oder mit Wirkung für die Zukunft widerrufen konnten. Ohne eine solche Einwilligung war eine Befragung nur in anonymisierter Form zulässig.

Die Verbandsgemeindeverwaltung hat eingeräumt, diese Anforderungen bei der Elternbefragung nicht erfüllt zu haben. Damit war die Datenerhebung in der erfolgten Form unzulässig. Dem datenschutzrechtlichen Anliegen, dass personenbezogene oder personenbeziehbare Daten, die in unzulässiger Weise erhoben worden sind, nicht weiter verwendet oder genutzt werden, wurde mit der Vernichtung der Originalfragebögen Rechnung getragen. Eine Nutzung der Daten in aggregierter, nicht personenbeziehbarer Form blieb im vorliegenden Zusammenhang zulässig.

Da die Verbandsgemeindeverwaltung erklärt hat, künftig die datenschutzrechtlichen Vorgaben zu beachten, wurde von einer Beanstandung gem. § 25 Abs. 1 LDSG abgesehen.

8.1.2 Zahngesundheitspflege in der Grundschule

Durch verschiedene Anfragen von Eltern und Schulleitern ist der LfD auf das Verfahren bei der Zahngesundheitspflege in Grundschulen aufmerksam geworden. Im Rahmen der zahnmedizinischen Gruppenprophylaxe sollen bei versicherten Kindern bis zum zwölften Lebensjahr Zahnerkrankungen erkannt und verhütet werden. Hierzu gehört nicht nur die Einbeziehung der Zahnpflege in den Unterricht, sondern auch die jährliche Untersuchung der Kinderzähne durch den Zahnarzt. Das Land Rheinland-Pfalz hatte mit Bekanntmachung vom 11. August 1997 die Landesarbeitsgemeinschaft zur Förderung der Zahnmedizinischen Vorsorge e. V. (LAGZ), in der sich die zuständigen Institutionen zusammengeschlossen haben, mit der Durchführung von solchen gruppenprophylaktischen Maßnahmen im Rahmen der Zahngesundheitspflege beauftragt. Zahnärztliche Untersuchungen in der Schule selbst finden nur noch in den ersten Klassen statt. Im Rahmen der Einschulungsuntersuchung werden die Kinder von Vertragszahnärzten der LAGZ in der Schule untersucht. Hält der Zahnarzt eine Behandlung für erforderlich, werden die Eltern in einem Schreiben, das den Kindern mitgegeben wird, aufgefordert, das Kind beim Hauszahnarzt in Behandlung zu geben. Eine Bestätigung, dass eine Behandlung stattgefunden hat, soll der Zahnarzt über die Schule an die LAGZ zurückschicken. Trifft eine solche Bestätigung nicht ein, werden die Eltern von der LAGZ nochmals an die zahnärztliche Behandlung erinnert. Die LAGZ erhält hierzu von der Schule Klassenlisten mit Schülernamen, anhand derer die Überprüfung der eingehenden Bestätigungsschreiben stattfindet und die nach statistischer Auswertung vernichtet werden. Die Elternanschreiben werden von der LAGZ an die Schule geschickt, die diese dann weiterleitet, so dass der LAGZ die Anschriften nicht mitgeteilt werden müssen. Anders das Verfahren in den Klassen zwei bis vier: Hier werden die Eltern gebeten, ihre Kinder beim Hauszahnarzt zur Untersuchung vorzustellen, eine Untersuchung in der Schule findet nicht statt. Auch hier kann der Zahnarzt bestätigen, dass die Untersuchung stattgefunden hat. Geht eine solche Bestätigung nicht ein, wird durch die LAGZ daran erinnert.

Der LfD hat gegen diese Verfahrensweise grundsätzlich keine datenschutzrechtlichen Bedenken, denn Schüler sind gem. § 52 Abs. 2 SchulG verpflichtet, sich im Rahmen der Schulgesundheitspflege schulärztlich untersuchen zu lassen. Eine solche Untersuchung stellt auch die zahnärztliche Untersuchung dar. Diese Untersuchungen werden hier jedoch nicht vom Gesundheitsamt durchgeführt, sondern in den ersten Klassen von Vertragszahnärzten der LAGZ. Grundsätzlich spricht jedoch nichts dagegen,

die zahnärztliche Untersuchung an private Zahnärzte zu vergeben, soweit sichergestellt ist, dass diese über die notwendige Qualifikation verfügen. Datenschutzrechtliche Gründe sprechen zumindest nicht gegen eine solche Aufgabenübertragung, da auch private Zahnärzte an die ärztliche Schweigepflicht gebunden sind. Bei den Schülern der Klassen zwei bis vier könnte die Untersuchung ebenfalls als Verpflichtung nach dem Schulgesetz ausgestaltet werden. Daher ist die Bitte, die Kinder beim Zahnarzt vorzustellen, weniger belastend als die verpflichtende Untersuchung beim Schulzahnarzt, zumal den Eltern die Wahl des Zahnarztes freigestellt wird.

Zur Vorbereitung dieser Untersuchungen ist es auch erforderlich, dass die mit der Organisation und Durchführung vom Land betraute LAGZ Klassenlisten mit den Schülernamen erhält, um ihre Aufgabe zu erfüllen.

Die Erinnerung an die Untersuchung in den Klassen zwei bis vier ist eine Folge der Bitte, die Kinder beim Zahnarzt vorzustellen. Da die Untersuchung auch verpflichtend sein könnte und damit zwangsweise durchsetzbar wäre, ist eine Erinnerung, die bei Nichtbefolgung keinerlei Konsequenzen nach sich zieht, als weniger belastender Eingriff ebenfalls zulässig.

Dagegen war fraglich, auf welcher gesetzlichen Grundlage die Erinnerung an die angeregte Zahnbehandlung der Erstklässler beruht. Behandlungen können im Gegensatz zu Untersuchungen den Schülern nach dem Schulgesetz nicht zur Pflicht gemacht werden, da sie in der Regel mit einem Eingriff in die körperliche Unversehrtheit verbunden sind, was nach § 52 Abs. 2 SchulG nicht zulässig ist. Als andere gesetzliche Grundlage hätte § 21 SGB V in Betracht kommen können, der es den Krankenkassen zusammen mit den Zahnärzten und den für die Zahngesundheitspflege zuständigen Stellen der Länder zur Aufgabe macht, die zahnmedizinische Gruppenprophylaxe zu betreiben. Gruppenprophylaxe bedeutet – wie bereits oben dargestellt – Maßnahmen zur Erkennung und Verhütung von Zahnerkrankungen, wobei insbesondere die Untersuchung der Mundhöhle, die Erhebung des Zahnstatus, Zahnschmelzhärtung, Ernährungsberatung und Mundhygiene im Vordergrund stehen. Für Kinder mit besonders hohem Kariesrisiko sind dabei spezifische Programme zu entwickeln.

§ 21 SGB V ist eine Vorschrift, die den Krankenkassen eine besondere Aufgabe überträgt. Die Krankenkassen sind zwar verpflichtet, die Gruppenprophylaxe anzubieten, aber eine Pflicht der Versicherten, dieses Angebot anzunehmen, besteht nicht. Zudem würde § 21 SGB V auch nur für die Kinder versicherungspflichtiger Eltern gelten. Schließlich steht die Behandlung von Zahnerkrankungen nicht im Vordergrund, sondern das frühzeitige Erkennen, das bereits durch die Untersuchung gewährleistet wird.

Daher ist nur eine Erinnerung zulässig, die die Freiwilligkeit der Behandlung durch den Zahnarzt betont. Die Freiwilligkeit sollte bereits bei der Bitte, das Kind zum Zahnarzt in Behandlung zu geben, betont werden. Eine entsprechende Änderung der Formulierung wurde angeregt.

Da der LfD vor Einführung des Vorhabens vom zuständigen Ministerium für Bildung, Wissenschaft und Weiterbildung leider nicht beteiligt wurde, konnte eine datenschutzrechtliche Beurteilung erst erfolgen, nachdem das Verfahren bereits in Gang gesetzt worden war.

8.1.3 Antragsverfahren für Lernmittelgutscheine

Bereits Mitte des Jahres 1988 hatte die Umstellung des Verfahrens zur Erteilung von Lernmittelgutscheinen zu einer größeren Zahl von datenschutzrechtlichen Fragen geführt. So erfolgten das Einsammeln der Lernmittelanträge und das Austeilen der entsprechenden Gutscheine „klassenöffentlich“. Der LfD konnte damals erreichen, dass das Verfahren so geändert wurde, dass nunmehr aus dem Bereich der Schule niemand Kenntnis über den Inhalt der Lernmittelanträge erhält (vgl. 12. Tb., Tz. 10.1.2.2).

Heute ist das Verfahren so ausgestaltet, dass die Schüler die Anträge im verschlossenen Umschlag im Schulsekretariat abgeben. Dort wird außen auf dem Umschlag bestätigt, dass der Schüler Angehöriger der Schule ist. Dann sollen die Umschläge an den Schulträger zur weiteren Bearbeitung weitergeleitet werden. Die Lernmittelgutscheine können sich die Eltern zusenden lassen oder beim Schulträger abholen.

Ein gewisser Interessenkonflikt für alle Beteiligten ergibt sich dann, wenn ausnahmsweise die Schulsekretärin die Lernmittelanträge bearbeitet. Denn für die Eltern ist die Schulsekretärin nach dem äußeren Anschein Teil der Schulorganisation und damit der Schule zuzurechnen, auch wenn sie generell Mitarbeiterin des Schulträgers ist, der sie an die Schule als Arbeitskraft „entleiht“.

Der LfD hat hierzu die Ansicht vertreten, dass aus datenschutzrechtlicher Sicht die Übertragung der Bearbeitung der Lernmittelanträge auf die Schulsekretärin nicht von vornherein ausgeschlossen ist, wenn sichergestellt wurde, dass weder Lehrer noch Schulleiter Kenntnis vom Inhalt der Anträge nehmen können und organisatorische Maßnahmen getroffen wurden, um die Bearbeitung der Anträge von der Bearbeitung der Schulverwaltungsangelegenheiten räumlich zu trennen. Darüber hinaus setzt eine solche Verfahrensgestaltung die umfassende Information der Eltern über die rechtliche und tatsächliche Situation voraus. Öffentliche Stellen müssen auch den Anschein vermeiden, gegen den Datenschutz zu verstoßen.

8.1.4 Was darf in die Schülerakte?

In der Akte einer Schülerin befanden sich bei der weiterführenden Schule die Halbjahres- und Jahreszeugnisse der Grundschulen einschließlich des Abschlusszeugnisses der Grundschule, diagnostische Rechtschreibtests sowie Briefe der Grundschule an die Eltern wegen nicht gefertigter Hausaufgaben. Die betroffenen Eltern vertraten die Ansicht, dass sich diese Unterlagen zu Unrecht in der Schülerakte befanden und baten den LfD um eine entsprechende Stellungnahme.

Der LfD ging davon aus, dass die Unterlagen – mindestens zu Dokumentationszwecken – in die Schülerakte der Grundschule aufgenommen werden durften, da die genannten Unterlagen zur Aufgabenerfüllung der Grundschule zur pädagogischen und schulverwaltungsrechtlichen Betreuung der Schülerin erforderlich waren (§ 54 a Abs. 1 SchulG).

Weiterhin war zu beurteilen, ob die Unterlagen auch an die weiterführende Schule übermittelt werden durften. Dies war dann zulässig, wenn die in Rede stehenden Unterlagen für die schulische Arbeit notwendige Daten enthielten. Für diese Beurteilung waren primär pädagogische Gesichtspunkte maßgeblich. Eine datenschutzrechtliche Überprüfung hatte sich bei der Beurteilung derartiger unbestimmter Rechtsbegriffe, die in einem fachspezifischen Zusammenhang Verwendung finden, darauf zu beschränken nachzuprüfen, ob die zulässigen Grenzen einer solchen Beurteilung überschritten waren. Mit anderen Worten, die entsprechende Beurteilung der zuständigen Fachbehörde (hier der Schule) wäre vom LfD nur dann beanstandet oder gerügt worden, wenn sie willkürlich, offensichtlich falsch oder aus sachfremden Gründen so getroffen worden ist, wie sie getroffen wurde.

Aus Sicht des LfD waren die zulässigen Grenzen der hier zu treffenden Beurteilung durch die Schule nicht überschritten worden. Es war durchaus vertretbar, die Notwendigkeit der Kenntnis der hier in Rede stehenden Informationen damit zu begründen, dass der Entwicklungsweg eines Kindes auch für die weiterführende Schule nachvollziehbar sein musste, insbesondere um beurteilen zu können, ob etwa auftretende Störungen im Schulverhältnis bereits eine längere Vorgeschichte hatten oder ob sie auf neu hinzutretende aktuelle Gründe zurückgeführt werden mussten.

Vor diesem Hintergrund sah der LfD keine Möglichkeit, das Anliegen der betroffenen Eltern in diesem Zusammenhang zu unterstützen.

8.1.5 Diagnoseangaben auf Entschuldigungsschreiben

Eine Grundschule hatte durch einen Elternbrief die Mitteilung der Diagnose bei Krankmeldungen von Schülerinnen und Schülern gefordert. Die Diagnose wurde gewünscht, um die Abwesenheit und das Nachholen von Lernstoffen besser einschätzen zu können. Grundsätzlich wollte die Schule auf der Angabe der Diagnose aber nicht bestehen. Diese hätte aber angegeben werden müssen, wenn es sich um eine ansteckende Krankheit nach dem Bundesseuchengesetz gehandelt hätte.

Aus datenschutzrechtlicher Sicht hat der LfD dies wie folgt beurteilt:

Die Diagnoseangabe bei Krankmeldungen ist zur Erfüllung schulbezogener Aufgaben nicht stets erforderlich. Erforderlich sind Angaben nur, wenn ohne ihre Kenntnis die Aufgabenerfüllung nicht oder nur unter Überwindung unzumutbarer Schwierigkeiten möglich wäre.

Der Aspekt der schulischen Betreuung während der Krankheit rechtfertigt nicht das generelle Verlangen nach Angabe der Diagnose. Eine schulische Betreuung während der Krankheit kann ohnehin nur unter enger Abstimmung mit den Eltern erfolgen. Die Frage, ob sie sinnvoll ist, hängt in erster Linie von Dauer und Schwere der Erkrankung, erst in zweiter Linie von ihrer Art ab. Dies ist im Einzelfall mit den Eltern abzuklären, kann aber nicht als hinreichender Grund einer generellen entsprechenden Datenerhebung angesehen werden.

Die seuchenrechtliche Beurteilung obliegt zunächst und in erster Linie dem behandelnden Arzt. Dieser ist auch primär zur Unterrichtung des Gesundheitsamtes verpflichtet. Bei Erkrankungen von Schülern trifft die ergänzende seuchenrechtliche Pflicht zur Benachrichtigung des Gesundheitsamtes die Sorgeberechtigten (§ 54 Abs. 4 GrundschulO i. V. m. § 45 Abs. 4 BSeuchG). Da jedoch bei solchen schweren ansteckenden Krankheiten häufig auch eine schnelle Reaktion der Schule erforderlich ist, hat der LfD es als zulässig erachtet, dass die Schulleitung hier die Diagnose fordern durfte.

Im Übrigen ist die Angabe der Diagnose nur auf freiwilliger Basis zulässig. Dies setzt eine umfassende Information der Eltern sowie den deutlichen Hinweis auf die Freiwilligkeit der erbetenen Angaben über die Diagnose der Krankheit des Kindes voraus. Die Löschung der Angaben hat spätestens mit Beendigung der Krankheit, also mit Rückkehr des erkrankten Kindes in die Schule zu erfolgen.

Der Elternbrief wurde mittlerweile entsprechend geändert. Um die Eltern darüber aufzuklären, welche Krankheiten in den Anwendungsbereich des Bundesseuchengesetzes fallen, wurde eine entsprechende Aufzählung im Elternbrief aufgenommen.

8.1.6 Schülerausweise

Der LfD wurde wiederholt auf die Frage angesprochen, unter welchen Voraussetzungen es datenschutzrechtlich zulässig sei, dass Schulen private Unternehmen mit der Erstellung digitaler Schülerausweise mit Geldkartenfunktion und codierbarem Magnetstreifen beauftragen. Zu diesem Zweck sollte die zu beauftragende Firma Fotos von den Schülern machen und von der Schule entsprechende Klassenlisten zur Verfügung gestellt bekommen.

Dazu hat der LfD die Auffassung vertreten, dass vor Fertigung entsprechender Bilder und vor der Datenübermittlung an das auftragnehmende Unternehmen die Eltern der noch nicht volljährigen Schüler und Schülerinnen über die beabsichtigte Verfahrensweise umfassend zu informieren sind. Bilder sollten erst dann gefertigt und personenbezogene Daten erst dann übermittelt werden, wenn die Eltern und die betroffenen Schüler hierin eingewilligt haben. Der LfD hat hierzu weiter angeregt, sich vor

Auftragsvergabe mit der für das in Frage kommende Unternehmen zuständigen Datenschutzaufsichtsbehörde in Verbindung zu setzen und zu klären, ob das Unternehmen seiner Anmeldepflicht nach § 32 BDSG nachgekommen ist und ob dort Hinweise vorliegen, die gegen die Zuverlässigkeit der fraglichen Firma sprechen. Schließlich ist nur dann die Freiwilligkeit bezüglich der Entscheidung der betroffenen Eltern und Schüler gegeben, wenn diesen die Möglichkeit eingeräumt wird, statt des digitalisierten Schülerausweises mit Geldkartenfunktion und codierbarem Magnetstreifen auch den herkömmlichen Schülerausweis über die Schule zu erhalten, worauf die Schüler und Eltern ebenfalls hinzuweisen sind. Letztlich ist auch darüber zu informieren, ob es sich um eine kontogebundene oder eine kontoungebundene Geldkarte handelt und welche Daten auf dem Magnetstreifen gespeichert werden sollen.

8.1.7 Präsentation von Klassenfotos und personenbezogenen Daten im Internet

Die Frage nach der Veröffentlichung von Daten im Internet wurde in letzter Zeit gerade im Schulbereich vermehrt gestellt.

Für die Veröffentlichung von Lehrer-, Schüler- und Elterndaten gilt Folgendes:

– Bei Lehrkräften dürfen grundsätzlich ohne deren Einwilligung Name, Lehrbefähigung und Funktion veröffentlicht werden. Veröffentlichungen weiterer Daten, wie Adresse und Telefonnummer, bedürfen der Einwilligung. Das Ministerium für Bildung, Wissenschaft und Weiterbildung hat zur Stärkung der Rechte der Bediensteten empfohlen, bei Lehrerinnen und Lehrern, die nicht der Schulleitung angehören, die Einwilligung zur Veröffentlichung auch von Name, Lehrbefähigung und Funktion einzuholen. Stimmt die Lehrkraft nicht zu, sollen ihre Daten nicht im Internet veröffentlicht werden. Diese Verfahrensweise ist aus datenschutzrechtlicher Sicht nicht zu beanstanden.

– Auch bei Eltern- und Schülervertretern gilt die sog. „Amtsträgertheorie“. Danach sind Funktionsträger in der öffentlichen Verwaltung, welche die Institution nach außen hin vertreten, in ihrem informationellen Selbstbestimmungsrecht in Bezug auf ihre öffentliche Funktion eingeschränkt. Dies trifft auf Mitglieder der Schulelternvertretung bzw. der Schülervertretung zu, nicht aber auf Klasseneltern- und Klassenschülersprecher, die die Institution Schule nicht nach außen vertreten. Dies bedeutet konkret, dass nur Namen und Funktionen der Mitglieder der Schulelternvertretung und der Schülervertretung ohne deren Einwilligung veröffentlicht werden dürfen. Für alle anderen Daten gilt ebenfalls der Einwilligungsvorbehalt.

Das Nennen von Namen in Berichten im Internet über besondere Ereignisse ist ebenfalls nur dann ohne Einwilligung des Betroffenen zulässig, wenn derjenige in seiner Eigenschaft als Funktionsträger der Schule an diesem Ereignis teilhatte. Andernfalls bedarf es wiederum der Einwilligung.

Eine Veröffentlichung des Namens, des Geburtsdatums und der Jahrgangsstufe (sowie der Funktion z. B. in der Schülervertretung und Klasse) von Schülerinnen und Schülern im Internet kann nach Ansicht des LfD nicht auf § 52 Abs. 5 GrundschulO oder § 76 Abs. 6 der Übergreifenden Schulordnung gestützt werden. Danach ist es zulässig, in Dokumentationen oder Jahresberichten die entsprechenden Daten zu veröffentlichen, wenn und soweit diese für die Schüler und Eltern herausgegeben werden. Hier wird eine besondere Art der Veröffentlichung geregelt, nämlich die Veröffentlichung in Dokumentationen und Jahresberichten für Schüler und Eltern. Der Verordnungsgeber hat damit eine eng auszulegende Sonderregelung geschaffen, die sich auf eine begrenzte Öffentlichkeit bezieht, wobei ausschließlich Printmedien vorstellbar waren, die zudem zeitlich begrenzt (zu besonderen Anlässen) erscheinen sollten. Diese Ausnahmevorschrift ist aus Sicht des LfD dagegen nicht auf die Veröffentlichung im Internet ausdehnbar; die Herstellung einer unbegrenzten Öffentlichkeit, wie sie durch das Internet und dessen Nutzer repräsentiert wird, lag außerhalb des Regelungswillens des Verordnungsgebers (und wohl auch außerhalb seiner Regelungskompetenz, die durch § 54 a Abs. 4 SchulG bestimmt wird). Vor diesem Hintergrund hielt es der LfD für bedenklich, mit dem Argument der Regelung in § 52 Abs. 5 GrundschulO bzw. § 76 Abs. 6 der Übergreifenden Schulordnung eine entsprechende Veröffentlichung im Internet zu rechtfertigen.

Bilder von Schülern und Lehrern dürfen im Internet nur mit Zustimmung der Betroffenen veröffentlicht werden.

8.1.8 Videoaufzeichnungen des Unterrichts

In einer Grundschule beabsichtigte man, zu Zwecken der Ausbildung Lehrversuche auf Video aufzuzeichnen.

Eine solche Aufzeichnung berührt das informationelle Selbstbestimmungsrecht der Lehrpersonen (im Regelfall also das der Referendarin oder des Referendars sowie der ausbildenden Lehrerin bzw. des Lehrers) sowie der anwesenden Schüler.

Die Aufzeichnung ist – mangels zwingender Erforderlichkeit zur schulischen Aufgabenerfüllung – nur zulässig, wenn die Eltern der betroffenen Schüler einwilligen. Eine solche Einwilligung wiederum ist nur wirksam, wenn die Eltern diese Einwilligung schriftlich erteilen und sie deutlich auf die Freiwilligkeit ihrer Einwilligung hingewiesen worden sind. Gleiches gilt auch für die betroffenen Lehrpersonen.

Unabhängig von der Voraussetzung der jeweils erteilten Einwilligungen ist zu beachten, dass die entsprechenden Videoaufzeichnungen nur in dem Umfang gefertigt werden dürfen, in dem dies zur Unterstützung der schulischen Aufgaben dienlich ist. Dies bedeutet, dass relativ kurze Löschungsfristen vorzusehen sind. Jedenfalls sind auch die Betroffenen im Rahmen der ihnen vor der Einwilligung zu erteilenden Informationen über die Speicherungsdauer der jeweiligen Aufzeichnungen zu unterrichten.

8.2 Hochschulen

8.2.1 Gesetz zur Änderung des Verwaltungsfachhochschulgesetzes und des Landesgesetzes über die Zentrale Verwaltungsschule Rheinland-Pfalz

Bei der Änderung des Verwaltungsfachhochschulgesetzes sowie des Landesgesetzes über die Zentrale Verwaltungsschule Rheinland-Pfalz war vorgesehen, dass die Prüfungsstellen sowie die zuständigen Ministerien personenbezogene Daten verarbeiten durften, soweit dies zur Erfüllung verwaltungshochschulbezogener Aufgaben erforderlich war. Diese geplante Regelung differenzierte nicht, wessen personenbezogene Daten danach verarbeitet werden durften. Der LfD hat diese Regelung insgesamt für überflüssig gehalten. Für den Fall der Beibehaltung empfahl er, diese Regelung auf die Studierenden zu beschränken, für Lehrkräfte das Landesbeamtengesetz bzw. § 31 LDSG und für Dritte das allgemeine Datenschutzrecht zur Anwendung kommen zu lassen. Weiterhin regte der LfD an klarzustellen, dass eine Übermittlung personenbezogener Daten an Dienstherren und Arbeitgeber nur dann zulässig wäre, soweit dies zur rechtmäßigen Erfüllung der Aufgaben der empfangenden Stelle zur Durchführung der Ausbildung oder des Arbeits- bzw. des Beamtenverhältnisses erforderlich ist. Schließlich empfahl der LfD, die Datenübermittlung an sonstige öffentliche Stellen sowie an private Stellen bzw. Personen nicht in der vorgesehenen Form, die einem Rückschritt gegenüber dem allgemeinen Datenschutzrecht gleichgekommen wäre, zu regeln, sondern auf die Vorschriften des LDSG zurückzugreifen.

Der Gesetzgeber hat diese Anregungen im Wesentlichen verwirklicht. Die vorgesehene Ausgestaltung ist ein Beispiel dafür, dass sog. „bereichsspezifische Regelungen“ angesichts der differenzierten Bestimmungen des LDSG auch entbehrlich sein können.

8.3 Wissenschaft

8.3.1 Krebsregister

Das Landeskrebsregistergesetz ist zum 1. Juli 1997 in Kraft getreten (vgl. hierzu 16. Tb., Tz. 8.3.2), und das Krebsregister hat seine Arbeit aufgenommen. Das Krebsregister gliedert sich in eine Vertrauensstelle, die beim Tumorzentrum Rheinland-Pfalz als beliehene Einrichtung angesiedelt ist, und in eine Registerstelle, eingerichtet beim Institut für Medizinische Statistik und Dokumentation (IMSD). Die Vertrauensstelle nimmt die Meldungen der Ärzte und Krankenhäuser entgegen, verschlüsselt die personenbeziehbaren Angaben und gibt diese zusammen mit den epidemiologischen Daten an die Registerstelle weiter. Zurzeit ist das Krebsregister noch im Aufbau befindlich. Die für eine fundierte Arbeit mit den Krankheitsdaten erforderliche Meldedichte ist noch nicht erreicht. Ferner haben sich im Laufe der bisherigen praktischen Arbeit einige Schwierigkeiten aufgrund der bisherigen Regelungen gezeigt: So können beispielsweise Angaben wie die Mehrlingseigenschaft erhoben werden, die für die praktische Arbeit nicht relevant sind. Da mit Ablauf des Jahres 1999 das Bundeskrebsregistergesetz außer Kraft tritt, wird eine Neuregelung auf Landesebene erforderlich, so dass hier die Erfahrungen aus der bisherigen Arbeit des Krebsregisters berücksichtigt werden können. Der Entwurf hierzu sieht im Wesentlichen die Übernahme der bisherigen bundesgesetzlichen Bestimmungen vor, ergänzt durch die bestehenden Regelungen im Landeskrebsregistergesetz. Der LfD hat sich dazu geäußert und dabei auch die Verbesserungswünsche des Krebsregisters in seine Überlegungen einbezogen.

In dem vorliegenden Entwurf ergeben sich folgende datenschutzrechtlich relevante Änderungen:

Die Meldemöglichkeit der Ärzte an das Register soll nun zur Meldepflicht unter Beibehaltung der Informationspflicht und des Widerspruchsrechts des Patienten werden. Neu wird auch die Meldemöglichkeit der Pathologen sein. Diese sollen nicht selbst den Patienten über die Meldung informieren, sondern es wird die Information durch den einsendenden Arzt auf Hinweis des Pathologen vorgesehen. Diese Änderungen werden auf Wunsch des Krebsregisters aufgenommen, um so eine größere Meldedichte zu erreichen. Datenschutzrechtliche Bedenken bestehen gegen diese Regelungen nicht, da das Widerspruchsrecht des Patienten bestehen bleiben wird.

Weiterhin soll die Möglichkeit einer elektronischen Datenübermittlung vom Arzt zum Krebsregister eingeführt werden. Hierfür gilt die datenschutzrechtliche Anforderung zu verhindern, dass bei der Übertragung personenbezogener Daten diese unbefugt gelesen, kopiert, verändert oder gelöscht werden können (Transportkontrolle gem. § 9 Abs. 2 Nr. 9 LDSG). Daraus folgt aus Sicht des LfD, dass entsprechende Daten bei der Übermittlung in öffentlichen Netzen zu verschlüsseln sind.

Ebenfalls soll die Möglichkeit der „Umverschlüsselung“ der Daten eingeführt werden, wenn dies nach dem Stand der Technik erforderlich wird. Hier wird das gleiche Verfahren wie bei einer genehmigten Entschlüsselung vorgesehen. Dabei ist zu gewährleisten, dass weder die Vertrauensstelle noch Dritte den Schlüssel missbräuchlich verwenden können.

Die Entschlüsselungskomponenten werden beim DIZ aufbewahrt. Hierfür wird zukünftig eine technikoffenere Formulierung gewählt, so dass begrifflich nicht mehr auf einen „Computer“ und ein „Computerprogramm“ abgestellt wird (vgl. hierzu 16. Tb., Tz. 8.3.2). Dies wird auch den Einsatz anderer Techniken ermöglichen, wie z. B. die Speicherung des Schlüssels auf einer Chipkarte. Dabei sind entsprechende technisch-organisatorische Sicherheitsvorkehrungen zu treffen.

Weder das bestehende noch das geplante Gesetz sehen nähere Regelungen vor, wie das Entschlüsselungsverfahren praktisch ablaufen soll. Diese Frage hatte bisher keine praktische Relevanz, da es noch nicht zu Entschlüsselungen gekommen ist. Es besteht aber aus Sicht des Datenschutzes unbedingt das Erfordernis einer entsprechenden Regelung, die jedoch nicht im Gesetz selbst vor-

genommen werden muss. Es ist vorstellbar, dass das zuständige Ministerium diese Festlegungen trifft. Auf eine entsprechende datenschutzgerechte Lösung wirkt der LfD derzeit hin. In diesem Zusammenhang wurden Gespräche mit dem DIZ, der Vertrauens- und der Registerstelle geführt, um gemeinsam ein gesetzeskonformes und handhabbares Verfahren zu entwickeln.

8.3.2 Allgemeines zu Forschungsvorhaben im Schulbereich

Zur Qualitätssicherung des Unterrichts in Schulen sowohl im Land als auch länderübergreifend und auf internationaler Ebene werden Befragungen in der Regel vom Ministerium für Bildung, Wissenschaft und Weiterbildung des Landes Rheinland-Pfalz oder auch von der Kultusministerkonferenz bundesweit in Auftrag gegeben. Als Beispiele für internationale Vergleichsstudien seien die OECD-Studie PISA (vgl. Tz. 8.3.3) und die Civic Education-Studie (vgl. Tz. 8.3.4) genannt, die beide im Auftrag durch das Max-Planck-Institut für Bildungsforschung in Berlin als Auftragnehmer durchgeführt werden und im Ergebnis die Qualität von Schulen im internationalen Vergleich belegen sollen. Solche Datenerhebungen finden ihre Rechtsgrundlage in § 54 a Abs. 1 SchulG. Danach dürfen personenbezogene Daten der Schüler, Eltern und Lehrer durch die Schulen, die Schulbehörden und die Schulträger erhoben und verarbeitet werden, soweit dies zur Erfüllung der ihnen durch Rechtsvorschrift zugewiesenen schulbezogenen Aufgaben erforderlich ist. Dies umfasst auch die Datenerhebung und -verarbeitung durch Dritte, wenn diese im Auftrag der o. g. Stellen tätig werden. Einer Einwilligung der Betroffenen bedarf es in diesen Fällen folglich nicht.

Befragungen von Schülerinnen und Schülern, Eltern, Lehrerinnen und Lehrern sind auch geeignete Instrumente, um Erkenntnisse für Diplomarbeiten oder Dissertationen in einschlägigen Studiengängen wie Pädagogik oder Sozialwissenschaften zu sammeln. Diese Befragungen fallen je nach Thema ganz unterschiedlich aus: Manchmal werden Schüler lediglich nach Lerngewohnheiten befragt, hin und wieder dringen diese Fragen aber auch sehr weit in die Privatsphäre der Befragten vor, etwa wenn nach der politischen Einstellung oder dem eigenen Gewaltverhalten gefragt wird. Die Erhebung solcher Daten, die nicht schulbezogenen Aufgaben dient, richtet sich nach § 54 a Abs. 3 SchulG: Danach bedarf die Erhebung von Daten in der Schule und die Verarbeitung dieser Daten der Genehmigung der obersten Schulbehörde (Ministerium für Bildung, Wissenschaft und Weiterbildung) und der Einwilligung der Betroffenen. Bei solchen Erhebungen ist es erforderlich, dass die Betroffenen über Inhalt, Art und Weise der Befragung und den Verwendungszweck der Daten sowie den möglichen Empfängerkreis aufgeklärt werden (§ 5 Abs. 2 LDSG, Grundsatz der informierten Einwilligung). Oftmals ist es bei umfangreichen Befragungen sinnvoll, den Fragebogen in der Schule zur Einsicht zur Verfügung zu stellen. Bei der Einholung der Einwilligung der Betroffenen ist darauf hinzuweisen, dass diese ohne Nachteile verweigert oder widerrufen werden kann. Betroffene sind dabei die Befragten selbst, bei minderjährigen Schülern in der Regel auch die Eltern als Erziehungsberechtigte. Deren Einwilligung ist zumindest dann notwendig, wenn die Kinder aufgrund der erfragten Themen und ihres Alters noch nicht die nötige Entscheidungsreife besitzen. Zudem sollte stets erklärt werden, was mit den personenbeziehbaren Fragebögen nach der Auswertung geschieht, also wann und wie sie vernichtet werden und ob die Daten in automatisierter Form verarbeitet werden. Wenn Letzteres der Fall und die verarbeitende Stelle als öffentliche Stelle des Landes Rheinland-Pfalz anzusehen ist, ist eine Anmeldung zum Datenschutzregister beim LfD Rheinland-Pfalz notwendig. Vielen Forschern sind diese datenschutzrechtlichen Erfordernisse nicht bewusst, die regelmäßig mit einfachen Mitteln umzusetzen sind und keine übermäßige Belastung darstellen. Anfragen von Eltern beim LfD zeigen, dass mit solchen Befragungen durchaus sensible Bereiche des Privatlebens betroffen werden und Zweifel hinsichtlich des Datenschutzes aufkommen können.

Im Folgenden werden exemplarisch einige Forschungsvorhaben kurz vorgestellt.

8.3.3 PISA-Studie

Die OECD plant eine internationale Schulleistungsstudie PISA (Programme for International Student Assessment), deren Ziel es ist herauszufinden, wie gut die Schulen ihre Schülerinnen und Schüler auf die Herausforderungen der Zukunft vorbereiten. Diese Studie ist Teil des Indikatorenprogrammes INES (Indicators of Educational Systems) der OECD. Ziel dieses Programmes wiederum, an dem sich auch die Bundesrepublik Deutschland beteiligt, ist es, den OECD-Mitgliedstaaten vergleichende Daten über die Effektivität ihrer Bildungssysteme zur Verfügung zu stellen. Es ist beabsichtigt, alle drei Jahre in rund 30 Industriestaaten Leistungen von 15-jährigen Schülerinnen und Schülern in den Bereichen Leseverständnis, Mathematik und Naturwissenschaften zu testen. Das Max-Planck-Institut für Bildungsforschung (MPI) wurde federführend mit der Durchführung beauftragt. Begonnen wurde Mitte 1999 mit einer ersten Feldstudie, die auch in Rheinland-Pfalz stattfinden sollte. Dabei sollten je Schule 35 Schülerinnen und Schüler getestet werden. Ebenso sollten die Eltern in einem Elternfragebogen zusätzliche Angaben machen.

Die Befragungen konnten nicht als völlig anonym angesehen werden, da mit zugänglichen Hilfsmitteln wie Schülerlisten Rückschlüsse auf die Antwortenden möglich waren. Einerseits wurde dabei Wissen von den Schülern abgefragt, um eine Qualitätsmessung vornehmen und damit schulbezogenen Aufgaben nachkommen zu können. Andererseits wurden aber auch Informationen erbeten, die nicht nur der Erkenntnisgewinnung über schulische Themen dienten und damit gem. § 54 a Abs. 1 SchulG ohne Einwilligung der Betroffenen erhoben werden konnten. Darüber hinaus wurden auch Themen angesprochen, die nicht mehr der schulischen Erkenntniserlangung dienten. Für diese Datenerhebung war die informierte Einwilligung der Betroffenen, also der Eltern und Kinder notwendig.

Das Ministerium für Bildung, Wissenschaft und Weiterbildung wurde gebeten, dafür Sorge zu tragen, dass eine entsprechende informierte Einwilligung der Betroffenen durch das MPI eingeholt wird. Auch die Landesdatenschutzbeauftragten der anderen Länder haben sich bzgl. der in ihrem Land geplanten Maßnahmen in diesem Sinne geäußert.

8.3.4 Civic Education-Studie

Ebenso wie die PISA-Studie der OECD ist auch die Civic Education-Studie eine internationale Studie, die die politische Bildung der Schülerinnen und Schüler untersucht. Sie ist ein kooperatives Projekt der IEA (International Association for the Evaluation of Educational Achievement), das in 27 Ländern durchgeführt werden soll, u. a. auch in der Bundesrepublik Deutschland, hier wiederum durch das MPI.

Auch bei dieser Studie musste davon ausgegangen werden, dass diese nicht anonym durchgeführt würde, sondern noch ein Personenbezug herstellbar war. Im Übrigen waren hier dieselben datenschutzrechtlichen Anforderungen wie bei der PISA-Studie zu stellen: Ein Teil der Fragen diente der Qualitätssicherung in den Schulen und konnte damit ohne Einwilligung der Betroffenen gem. § 54 a Abs. 1 SchulG gestellt werden, der andere Teil ermittelte jedoch auch das soziale Umfeld und die politische Einstellung der Schüler, wofür wiederum die informierte Einwilligung der Betroffenen erforderlich war. Die dem LfD vorgelegte Einverständniserklärung entsprach weitgehend datenschutzrechtlichen Anforderungen. Das MPI wurde gebeten, die fehlenden Informationen zu ergänzen und auch die Schüler ausreichend über die Befragung zu informieren.

8.3.5 Befragung von Schulkindern zur Lebensqualität

Eine Universität hatte insgesamt 428 Kinder und deren Eltern in insgesamt sechs verschiedenen Schulen einer ausgewählten Stadt zu deren Lebensqualität in personenbeziehbarer Form befragt. Dabei wurden Fragen zum familiären Umfeld, zur Religion, zur Schule, zum Geld, zur Freizeit, zu Freunden und zur Gesundheit gestellt. Zuvor wurden die Eltern über die geplante Befragung und deren Freiwilligkeit informiert. Dieser Information lag eine sog. „Nicht-Einverständnis-Erklärung“ bei, die die Eltern dann unterzeichnen sollten, wenn sie nicht wollten, dass ihr Kind an der Befragung teilnimmt.

Der LfD wurde erst nach erfolgter Durchführung von der Befragung in Kenntnis gesetzt, obwohl das Ministerium für Bildung, Wissenschaft und Weiterbildung in seinem Genehmigungsschreiben vor Beginn der Befragung auf die evtl. bestehende Anmeldepflicht zum Datenschutzregister hingewiesen hatte.

Es blieb nichts anderes übrig als die Befragung im Nachhinein datenschutzrechtlich zu bewerten:

Die vor einer solchen Befragung einzuholende Einwilligung musste ausdrücklich erfolgen und konnte nicht aus einem Schweigen zu dem Vorgang abgeleitet werden, da eine solche Einwilligung eine deutlich geäußerte Willenserklärung voraussetzt. Diese Voraussetzung war hier nicht erfüllt. Der LfD ging jedoch aufgrund der Zusicherung der Universität davon aus, dass bei zukünftigen Vorhaben die Anmeldung zum Datenschutzregister rechtzeitig vorgenommen und die Einwilligungserklärung entsprechend formuliert werden würde. Er hat daher von einer förmlichen Beanstandung abgesehen.

8.3.6 Multikulturelle Gesellschaft, Ernährung, Fitness, Aussehen – eine Frage der Einstellung?

In dieser Studie sollten die Einstellungen von Jugendlichen und jungen Erwachsenen zu verschiedenen aktuellen Themen erfragt werden. Die Befragung sollte in den Klassenstufen 8 bis zur jeweiligen Abgangsklasse an Hauptschulen, Realschulen und Gymnasien durchgeführt werden. Da detaillierte Angaben zu Alter, Größe, Gewicht, Geschlecht, Klassenstufe, Religionszugehörigkeit, Nationalität, ethnische Herkunft, Geburtsland und Beruf der Eltern gefordert waren, ging der LfD von einer personenbeziehbaren Befragung aus, die wiederum die informierte Einwilligung der Betroffenen voraussetzte. Eine entsprechende Aufklärung erfolgte nur sehr kursorisch. Zudem wurde mitgeteilt, dass Rückschlüsse auf einzelne Personen nicht möglich seien, was so nicht zutraf. Außerdem hätte auf den Zeitpunkt der vorgesehenen Anonymisierung hingewiesen werden müssen. Schließlich kritisierte der LfD, dass die Einverständniserklärungen der Eltern an die Projektleiter weitergegeben wurden und nicht bei der Schulleitung verbleiben sollten.

Nachdem der LfD auf diese Gesichtspunkte hingewiesen hatte, wurde zugesichert, diese bei einer evtl. Fortsetzung der Befragung zu berücksichtigen. Die Einverständiserklärungen wurden an die Schulleitungen zurückgegeben.

8.3.7 Fremdenfeindlichkeit, Antisemitismus und Rechtsextremismus und deren Hintergründe

Angesichts des Anstiegs rechtsextremistischer, fremdenfeindlicher und antisemitischer Straftaten in Deutschland im Jahr 1997 beabsichtigte das Bundesministerium des Innern, eine im Jahr 1994 durchgeführte Analyse zu fremdenfeindlich motivierten Straftätern fortzusetzen und zu vertiefen. Die Gesamtanalyse sollte sich auf drei Teilbereiche beziehen, nämlich die Analyse der polizeilichen Ermittlungsakten zu fremdenfeindlichen, antisemitischen und rechtsextremistischen Tatverdächtigen, die Analyse von Gerichtsentscheidungen zu Jugendlichen, die in bestimmten Jahren wegen rechtsextremistischer, antisemitischer und fremdenfeindlicher Straftaten verurteilt worden waren und schließlich die Durchführung qualitativer Interviews mit jugendlichen, wegen fremdenfeindlicher, rechtsextremistischer und antisemitischer Delikte verurteilten Straftätern.

Im ersten Teilbereich sollten über das Landeskriminalamt an die Polizeidienststellen Fragebögen verteilt werden, in welche die Polizeibehörden personen- und tatbezogene Daten aus den Akten übertragen sollten. Zur Realisierung des zweiten Teilbereichs war beabsichtigt, sich mit Unterstützung des Justizministeriums einen möglichst systematischen Zugang zu Amts- und ggf. Landgerichten zu verschaffen. Im dritten Teilbereich schließlich sollte mit Hilfe der Justizvollzugsanstalten eine gezielte Kontaktaufnahme mit zu interviewenden Straftätern vorbereitet werden. In allen Teilbereichen sollten Erkenntnisse über biographische und familiäre Zusammenhänge, Milieueinflüsse und Einstellungen sowie Tatmotive gewonnen werden.

Es war davon auszugehen, dass die Fragebögen grundsätzlich personenbeziehbare Daten enthielten, da die projektdurchführende Stelle, die die Fragebögen erhalten sollte, Zugriff auf eine Datei mit tat- und täterbezogenen Angaben aus dem Bereich der Staatsschutzdelikte hatte, so dass eine Reidentifizierbarkeit zumindest in Einzelfällen möglich schien.

Die Übermittlung personenbeziehbarer Daten aus dem Bereich strafverfolgender Tätigkeiten der Polizei war aus Sicht des LfD nur unter Einhaltung der Voraussetzungen des Strafverfahrensrechtes zulässig. Die Strafprozessordnung enthielt und enthält bislang noch keine ausdrückliche Regelung über die Nutzung entsprechender Daten für wissenschaftliche Zwecke. Bislang ist in diesem Zusammenhang auf Nr. 185 der Richtlinien über das Straf- und Bußgeldverfahren abgestellt worden. Diese untergesetzliche Regelung kann jedoch nicht als ausreichende Grundlage für die Datenübermittlung angesehen werden (vgl. auch Urteil des OLG Koblenz, NJW 1987, 855). Dennoch hält der LfD es für vertretbar (und zur Wahrung der von der Verfassung anerkannten Rechtsgüter letztlich auch unverzichtbar), vor Erlass einer ausreichenden bereichsspezifischen gesetzlichen Rechtsgrundlage in diesem Zusammenhang wissenschaftliche Forschung auch unter Nutzung personenbeziehbarer Daten aus Strafverfahren ohne Einwilligung der Betroffenen zu ermöglichen (vgl. OLG Hamburg, NJW 1995, 1440). Die im Strafverfahrensänderungsgesetzentwurf, der vom Bundeskabinett bereits beschlossen worden war und dessen Zuleitung an den Bundesrat unmittelbar bevorstand, enthaltenen Regelungen über die Nutzung von Daten aus der Strafverfolgung für die wissenschaftliche Forschung konnten aus Sicht des LfD als Grundlage dafür herangezogen werden, einen Ausgleich der hier betroffenen verfassungsrechtlich geschützten Güter herbeizuführen.

§ 476 des o. g. StVÄG-Entwurfs enthält dazu folgende Voraussetzungen:

- Die Übermittlung muss für die Durchführung bestimmter wissenschaftlicher Forschungsarbeiten erforderlich sein;
- der Forschungszweck kann durch die Nutzung anonymisierter Daten nicht erreicht werden;
- das öffentliche Interesse an der Forschungsarbeit muss das schutzwürdige Interesse des Betroffenen am Ausschluss der Übermittlung erheblich überwiegen.

Zur Darlegung der Erforderlichkeit für die Durchführung einer bestimmten wissenschaftlichen Forschungsarbeit gehört insbesondere die thematische Festsetzung, die Umgrenzung der benötigten Informationen und die Festlegung des Personenkreises, der das Forschungsvorhaben durchführen und dabei Zugang zu den personenbezogenen Informationen haben soll (vgl. die amtl. Begründung zu § 476 StVÄG-E).

Die personenbezogenen Informationen dürfen nur für die Forschungsarbeit verwendet werden, für die sie übermittelt worden sind. Dies bedeutet, dass auch innerhalb der forschenden Stelle Vorkehrungen getroffen sein müssen, damit die Einhaltung der Zweckbindung gesichert ist. Der Gesetzentwurf sieht ausdrücklich vor, dass die Stelle, die wissenschaftliche Forschung betreibt, dafür zu sorgen hat, dass die Verwendung der personenbezogenen Informationen räumlich und organisatorisch getrennt von der Erfüllung solcher Verwaltungsaufgaben oder Geschäftszwecke erfolgt, für die diese Informationen gleichfalls von Bedeutung sein können.

Sobald es der Forschungszweck erlaubt, sind die personenbezogenen Informationen zu anonymisieren. Solange dies noch nicht möglich ist, sind die Merkmale gesondert aufzubewahren, mit denen Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person zugeordnet werden können. Dies betraf hier aus Sicht des LfD in erster Linie die Auswertungsliste aus der Datei mit tat- und täterbezogenen Angaben, die dementsprechend gesondert aufzubewahren war und mit den Einzelangaben nur zusammengeführt werden durfte, soweit der Forschungszweck dies erforderte. Eine entsprechende Auflage hätte durch die datenübermittelnde Stelle formuliert werden sollen.

Bei Einhaltung dieser Kautelen hielt der LfD die hier geplante Aktenauswertung und Datenübermittlung an die Forschungsprojektverantwortlichen für zulässig. Vergleichbares galt für die Aktenauswertung bei den Gerichten. Auch hier waren die gleichen Voraussetzungen zu beachten. Soweit rheinland-pfälzische Strafgefangene von der im dritten Teil der Untersuchung beabsichtigten Datenerhebung betroffen sein sollten, wies der LfD auf die besondere Bedeutung des Grundsatzes der Freiwilligkeit und der informierten Einwilligung vor der Datenerhebung hin. Auch hier waren besondere Vorkehrungen zu treffen, damit die Zweckbindung der Daten (ausschließlich für die wissenschaftliche Forschung) auch innerhalb der JVA sichergestellt wurden.

8.3.8 Erhebung zur Jugendhilfeplanung

Eine rheinland-pfälzische Stadt hatte eine Erhebung zur Jugendhilfeplanung beim LfD zu einem Zeitpunkt angemeldet, zu dem die Befragung bereits abgeschlossen war. Die entsprechende Anmeldung wäre jedoch gem. § 27 Abs. 1 LDSG so rechtzeitig vorzunehmen gewesen, dass der LfD vor der erstmaligen Speicherung personenbezogener Daten seiner gesetzlichen Überwachungspflicht hätte nachkommen können.

Gewichtiger allerdings war die Tatsache, dass die Eltern der befragten Kinder im vorliegenden Zusammenhang nicht ausreichend über die Bedeutung der Einwilligung aufgeklärt wurden, obwohl im Fragebogen höchst sensible Angaben gefordert wurden. So ist beispielsweise danach gefragt worden, ob die Jugendlichen schon einmal Drogen genommen oder wie oft sie andere im letzten halben Jahr beleidigt hätten. Diese Angaben konnten zu einer strafrechtlich relevanten Selbstbelastung der betroffenen Jugendlichen führen. Bei solch sensiblen Fragen ist, wenn – wie auch im vorliegenden Fall – das Risiko der Reidentifizierung besteht, eine umfassende deutliche Information der einwilligungsbefugten Personen (hier die Kinder und die Eltern) unabdingbar.

Das städtische Jugendamt hat sich, wenn auch erst nach einigem Zögern, der Auffassung des LfD angeschlossen, so dass von einer Beanstandung abgesehen werden konnte.

8.3.9 Katamnese-Studie zum rheinland-pfälzischen Maßregelvollzug

Eine Maßregelvollzugseinrichtung beabsichtigte die Durchführung einer Katamnese-Studie. Da bereits in Nordrhein-Westfalen ein ähnliches Projekt durchgeführt worden war, wurde das dort tätig gewordene Institut auch mit der Durchführung der rheinland-pfälzischen Studie beauftragt.

Ziel der Untersuchung war es, Informationen über die Rückfallproblematik zu gewinnen und geeignete Strategien zur Verminderung von Rückfällen zu entwickeln. Verschiedene psychiatrische Kliniken sollten Listen von Patienten erstellen, die in bestimmten Jahren aus der Behandlung entlassen wurden.

Für jeden Patienten sollte nach den Vorgaben des Instituts eine Nummer erzeugt und mit dem Namen verknüpft werden. Es hätte sich insoweit um eine sprechende Nummer gehandelt, als die Einrichtung erkennbar gewesen wäre. Die Patientennamen wären dem Institut durch die Einrichtungen nicht bekannt gegeben worden.

Die Einrichtungen sollten die Listen an das Bundeszentralregister geben. Dieses sollte für die Patienten Zentralregisterauszüge erstellen, die Informationen über Verurteilungen usw. vor der Aufnahme in die Einrichtungen und nach der Entlassung enthalten. In diesen Zentralregisterauszügen sollte nicht der Name des Patienten, sondern nur die von der Einrichtung erzeugte Nummer enthalten sein. Zu den Angaben über Strafverfahren hätte auch das Aktenzeichen der Verfahrensakte gehört. Die Auszüge sollten an das Institut übermittelt werden.

Das Institut sollte die vom Bundeszentralregister zur Verfügung gestellten Informationen auswerten, wobei eine Gruppenbildung vorgenommen werden sollte:
1. leichte Fälle, z. B. Nichtbeachtung von Bewährungsauflagen;
2. mittelschwere Fälle, z. B. Straftat, die Verurteilung zur Folge hatte;
3. schwere Fälle, einschlägige – im Verhältnis zum Maßregelvollzug – oder schwer wiegende Straftaten.

In den der dritten Gruppe zugehörigen Fällen wollte das Institut die Strafakten beiziehen – unter Verwendung des Aktenzeichens – und ergänzende Auswertungen vornehmen. Schließlich sollte bei Patienten dieser Fallgruppe eine Auswertung der Behandlungsakten erfolgen. Zweckmäßigerweise sollte die Auswertung durch Personal des Instituts durchgeführt werden, evtl. auch durch Personal der Einrichtungen.

Grundlage für die Studie war das Maßregelvollzugsgesetz, das auf § 35 PsychKG verweist. Die Datenübermittlung für Zwecke der wissenschaftlichen Forschung ist hier sehr restriktiv geregelt: Es kam nur eine Datenübermittlung mit Einwilligung der Betroffenen in Betracht. Die Übermittlung anonymisierter Aktenauswertungen wäre ohne wissenschaftlichen Wert gewesen, weil eine Verknüpfung mit den Informationen aus den Strafakten und dem BZR nicht möglich gewesen wäre.

Vom LfD wurde problematisiert, ob die Übermittlung anonymisierter Daten aus dem BZR auch dann zulässig gewesen wäre, wenn im weiteren Verfahren – durch Zugriff auf die Strafakten – eine Deanonymisierung vorgenommen worden wäre. Die Justizverwaltung hätte bei der Einsichtsgewährung in die Akten zu berücksichtigen gehabt, dass sie gegenüber dem Betroffenen als die Stelle erkennbar geworden wäre, die eine Deanonymisierung ermöglicht hätte.

Dieses Problem hätte schon bei der Anforderung der BZR-Auszüge durch die Einrichtungen bestanden. Mittelbar wären personenbezogene Daten – Tatsache des Vollzugs, Entlassung – von den Einrichtungen an das Institut übermittelt worden, denn es wäre von vornherein bekannt gewesen, dass einzelne Betroffene zuverlässig identifiziert worden wären. Es wäre also nicht nur zu klären gewesen, ob eine Rechtsgrundlage für die Weitergabe personenbezogener Daten an das BZR bestand, sondern ebenfalls, ob nicht auch die spätere Feststellung einzelner Betroffener in dem beschriebenen Verfahren die Anwendung von § 35 PsychKG schon für die erste Datenweitergabe forderte.

Der LfD erhielt nach Aufzeigen dieser datenschutzrechtlichen Fragen keine weitere Nachricht über die Durchführung des Projekts.

8.3.10 Evaluation von Erhebungs- und Messmethoden

Eine Universität plante die Durchführung einer wissenschaftlichen Untersuchung im Auftrag der Bundesanstalt für Straßenwesen. Dabei sollten unterschiedliche Erhebungstechnologien im Bereich der Verkehrszählung miteinander verglichen werden. Eine dieser Erhebungstechniken war die Videotechnik, mit der Kfz-Kennzeichen an verschiedenen Stellen des Stadtgebietes bzw. des Campus erhoben und zum Zweck des Abgleichs gespeichert werden sollten. Die Videoaufnahmen der erfassten Fahrzeuge sollten über den Zeitraum der gesamten Untersuchung hinweg manuell ausgewertet werden, um jeweils die Zuverlässigkeit der unterschiedlichen Erfassungsmethoden prüfen und um nachweisen zu können, welche Fehlerquellen bei welcher Methode aus welchem Grund bestehen.

In Praxisverfahren, die nicht mehr der Evaluation bestimmter Methoden dienten, sondern in denen es auf konkrete Ergebnisse der Verkehrszählung ankam, konnte unmittelbar bei der Erfassung der Kfz-Kennzeichen eine digitale Umwandlung im Wege der Einwegverschlüsselung erfolgen.

Der LfD hat die beabsichtigte Datenerhebung gem. § 12 Abs. 2 Nr. 3 LDSG als zulässig erachtet, wenn auf den gefertigten Aufnahmen nicht die Fahrzeuginsassen, sondern nur die Kennzeichen erkennbar sein würden. Außerdem war zur Wahrung der schutzwürdigen Belange der Betroffenen eine möglichst frühzeitige Löschung, nämlich unmittelbar nach Abschluss des Forschungsvorhabens, erforderlich.

8.3.11 Was macht die rheinland-pfälzische Elite?

Die Universität Mainz plante aus Anlass des fünfzigjährigen Bestehens des Landes Rheinland-Pfalz eine wissenschaftliche Untersuchung der Eliten im Land. Dabei wurden die Inhaber von Führungspositionen über ihren Werdegang und ihre Einstellungen befragt. Der LfD wurde bereits im Vorfeld der Studie um Mitteilung gebeten, welche datenschutzrechtlichen Bestimmungen zu beachten seien. Es wurde darauf hingewiesen, dass die Befragten umfassend über die Bedingungen der Datenerhebung und Datenverarbeitung informiert und darüber aufgeklärt werden sollten, dass die Befragung freiwillig sei und bei Nichtteilnahme keinerlei Nachteile entstehen würden. Trotz frühzeitiger Beteiligung musste der LfD feststellen, dass der Hinweis auf die Freiwilligkeit und Angaben über die Vernichtung der Fragebögen und die vollständige Anonymisierung der Daten fehlten. Er hat daraufhin nochmals an diese Voraussetzungen erinnert.

8.3.12 Befragung zu Karriereverläufen und Mobilitätsprozessen von Wissenschaftlern

Aufgrund einer Eingabe wurde der LfD auf eine Befragung zu Karriereverläufen und Mobilitätsprozessen durch eine Universität aufmerksam. Hierbei sollten Erkenntnisse über Karriereverläufe von Professorinnen und Professoren und die Situation des Mittelbaus in verschiedenen Disziplinen erlangt werden. Dazu sollten Fragen über Studium, Promotion, Habilitation, die gegenwärtige Tätigkeit und bisherige Laufbahn sowie über biographische Hintergründe beantwortet werden.

Die Anonymität der Befragung sollte dadurch gewährleistet werden, dass die Fragebögen vom Datenschutzbeauftragten der Universität verschickt werden sollten. Zudem war die Eingabe der gewonnenen Daten der Befragung durch eine externe Stelle beabsichtigt.

Aufgrund der geforderten Angaben und des eingrenzbaren Personenkreises, auf den die Befragung ausgerichtet war (alle Professorinnen und Professoren dieser Universität) konnte nach Ansicht des LfD ein Personenbezug, z. B. unter Zuhilfenahme des aktuellen Vorlesungsverzeichnisses, hergestellt werden, auch wenn die Fragebögen durch einen Dritten verschickt werden sollten. Daher war die Befragung datenschutzrechtlich nur zulässig, soweit die Betroffenen informiert darin eingewilligt hatten. Zudem hätten die Befragten auch darüber informiert werden müssen, dass die Eingabe durch Externe vorgenommen werden sollte. Daran fehlte es jedoch. Nachdem der LfD seine diesbezüglichen Bedenken mitgeteilt hatte, wurden in einem Erinnerungsschreiben die notwendigen Informationen nachgeholt.

8.3.13 Absolventenbefragung

Eine rheinland-pfälzische Universität führte zusammen mit dem Ministerium für Bildung, Wissenschaft und Weiterbildung sowie einem Zentrum für Hochschulentwicklung in Nordrhein-Westfalen ein Projekt „Fachbereichsentwicklung durch Zielvereinbarungen“ durch. Im Rahmen diese Projekts wurden Absolventen der Fachbereiche Architektur, Raum- und Umweltplanung sowie Bauingenieurwesen mit Hilfe eines umfangreichen Fragebogens befragt. Einer der befragten Absolventen machte den LfD auf die Befragung aufmerksam.

Der LfD hielt die Befragung für verbesserungsbedürftig und -fähig. Da vier Wochen nach dem Versand der Fragebögen die Absolventen, von denen noch keine Antwort vorlag, an die Rücksendung erinnert wurden, musste der Rücklauf offensichtlich personenbezogen registriert worden sein. Damit handelte es sich vorliegend um die Erhebung personenbeziehbarer Daten. Vor diesem Hintergrund waren die Anforderungen des § 5 Abs. 3 LDSG einzuhalten. Danach waren die Betroffenen ausdrücklich auf die Freiwilligkeit der Teilnahme hinzuweisen. Auch die Bedeutung der Einwilligung, die im vorliegenden Fall konkludent durch die Rücksendung der Fragebögen erteilt worden war, hätte im Anschreiben deutlicher erläutert werden müssen. Dazu hätte die Information gehört, wer die ausgefüllten Fragebögen wie lange unter welchen Nutzungsbeschränkungen erhalten hätte und wann sie hätten vernichtet werden sollen.

Der LfD wies auf diese Gesichtspunkte hin und forderte deren künftige Beachtung. Von einer Beanstandung wurde jedoch abgesehen, da diese Punkte nicht von solch erheblichem Gewicht waren, dass eine derartige Sanktion angemessen erschien.

8.4 jugendschutz.net

Mit dem Fortschreiten der neuen Medien – insbesondere des Internets – wachsen nicht nur die Informationsmöglichkeiten, sondern auch die Gefahren für die Rechte Betroffener. Hier gilt es, entsprechende staatliche Maßnahmen zu ergreifen, um solchen Inhalten vorzubeugen bzw. sie zu bekämpfen. Eine Organisation, die dieser Aufgabe nachgeht, ist das jugendschutz.net. Durch öffentlich zugängliche Quellen auf den neuen Sitz des jugendschutz.net in Mainz auf diese Stelle aufmerksam geworden, führte der LfD ein Informationsgespräch mit den Mitarbeitern des jugendschutz.net.

Durch Vereinbarung der Bundesländer vom 20. Juni 1997 wurde das jugendschutz.net initiiert und ihm die Aufgabe übertragen, im Auftrag und unter der Aufsicht der Jugendschutzbehörden der Länder das Internet auf jugendgefährdende Inhalte zu durchsuchen und darauf hinzuwirken, dass solche Inhalte aus dem Internet entfernt werden. Zu diesem Zweck erhebt und speichert das jugendschutz.net personenbezogene Daten von Anbietern. Dadurch wird das informationelle Selbstbestimmungsrecht der Anbieter beschränkt. Es stellte sich die Frage, ob eine Ländervereinbarung ausreicht, um eine Zentralstelle mit dieser Aufgabe zu betrauen. Da auf der Ebene der Zentralstelle keine wechselseitige Nutzung der die einzelnen Länder betreffenden Datenbestände erfolgt und damit die gespeicherten Daten nicht länderübergreifend genutzt werden, hielt der LfD die Vereinbarung – in Abstimmung mit den Landesdatenschutzbeauftragten – für ausreichend: Die hier erfolgende Aufgabenwahrnehmung konnte als

zulässige Form einer solchen durch einen Dritten etwa in Form der technischen Erfüllungshilfe oder der Auftragsdatenverarbeitung im datenschutzrechtlichen Sinn angesehen werden, wofür eine spezielle gesetzliche Grundlage entbehrlich ist.

Unter einem anderen Aspekt wäre allerdings eine solche gesetzliche Grundlage (etwa in einem Staatsvertrag) auch aus datenschutzrechtlicher Sicht wünschenswert:

Als Einrichtung der Länder ist das jugenschutz.net eine öffentliche Stelle mit Sitz in Rheinland-Pfalz, so dass – nach dem Sitzlandprinzip – die Vorschriften des LDSG Rheinland-Pfalz auf deren Datenverarbeitung Anwendung finden. Wenn das jugendschutz.net aber Datenverarbeitung im Auftrag der Bundesländer durchführt, hätte es zusätzlich jeweils die landesdatenschutzgesetzlichen Vorschriften des jeweils betroffenen Bundeslandes zu beachten. Hier könnte eine staatsvertragliche Regelung (inhaltlich in Anlehnung etwa an die Formulierung in § 16 des ZDF-Staatsvertrages) Klarheit schaffen.

Der LfD wird die Arbeit des jugendschutz.net weiter begleiten.

9. Umwelt

9.1 Einzelfragen zum Umweltinformationsgesetz

Im Berichtszeitraum wurden an den LfD zahlreiche Fragen zur gegenwärtigen Ausgestaltung des Informationszugangs im Umweltbereich herangetragen.

Als nationale Umsetzung der Richtlinie 90/313 EWG des Rates vom 7. Juni 1990 über den freien Zugang zu Informationen über die Umwelt erließ der Bundesgesetzgeber am 8. Juli 1994 das Umweltinformationsgesetz. Darin wurden erstmals im Bundesrecht Informationsfreiheitsrechte der Bürger und Datenschutzansprüche zu einander in Verhältnis gesetzt. Ziel dieses Gesetzes ist es, den freien Zugang zu den bei den Behörden vorhandenen Informationen über die Umwelt sowie die Verbreitung dieser Informationen zu gewährleisten und die grundlegenden Voraussetzungen festzulegen, unter denen derartige Informationen zugänglich gemacht werden sollen (vgl. auch 15. Tb., Tz. 9.1). Der vom Gesetzgeber zu Grunde gelegte Umweltbegriff ist sehr weit gefasst und umfasst alle Informationen über den Zustand der Gewässer, der Luft, des Bodens, der Tier- und Pflanzenwelt und der natürlichen Lebensräume.

Als grundsätzlich bedeutsam haben sich folgende Feststellungen erwiesen:

- Nach § 3 Abs. 1 UIG hat jede natürliche oder juristische Person des Privatrechts, unabhängig von ihrer Nationalität, einen Informationsanspruch. Auch ausländische juristische oder natürliche Personen können unabhängig von ihrem Sitz bzw. Wohnsitz dieses Recht in Anspruch nehmen. Der Nachweis eines rechtlichen, wirtschaftlichen oder sonstigen Interesses ist nicht erforderlich.
- Das Umweltinformationsgesetz gilt für Informationen über die Umwelt, die bei den Behörden im Sinne des § 3 Abs. 1 UIG aufgrund deren Zuständigkeit zur Durchführung umweltrechtlicher Vorschriften vorhanden sind („Aufgaben des Umweltschutzes wahrnehmen“). Von der Informationspflicht sind unter anderem Behörden ausgenommen, die ebenso wie andere natürliche und juristische Personen die umweltrechtlichen Vorschriften beachten müssen; denn hier fehlt es insoweit an der sachlichen Zuständigkeit für die Umweltpflege.
- Umweltinformationen sind auch dann zugänglich zu machen, wenn sie bei Privaten vorhanden sind, die öffentliche Aufgaben im Bereich des Umweltschutzes wahrnehmen (§ 2 Nr. 2 UIG). Der Beliehene, d. h. natürliche oder juristische Personen, die hoheitliche Kompetenzen im eigenen Namen wahrnehmen (etwa TÜV oder Schornsteinfeger), wird bereits von § 2 Nr. 1 UIG erfasst. Informationspflichtig sind ferner u. a. privatrechtlich organisierte, aber staatlich beherrschte Abfallentsorgungsbetriebe, Flughafenverwaltungen, Energieversorgungsunternehmen und Sachverständige im Rahmen ihrer Überwachungstätigkeit nach § 52 BlmSchG. Verwaltungshelfer, die als „technische Werkzeuge“ zur Erledigung staatlicher Aufgaben eingesetzt werden, scheiden als Auskunftspflichtige aus, da die öffentlich-rechtliche Aufgabenerfüllung funktional der Behörde und nicht dem Verwaltungshelfer zugerechnet wird.
- Das Begehren der Informationssuchenden muss sich auf Umweltinformationen i. S. v. § 3 Abs. 2 UIG richten. In diesem Zusammenhang ist häufig Diskussionsbedarf vorhanden. So werden nach Auffassung des Gesetzgebers entfernte Tätigkeiten oder Maßnahmen mit nur mittelbarem Bezug zum Umweltschutz nicht erfasst, sondern nur solche, die eine direkte Verbesserung der Umwelt bezwecken (vgl. Bundesratsdrucksache 797/93 vom 5. November 1993, S. 29). Damit bezweckt beispielsweise das Erstellen und die Übermittlung eines Verzeichnisses keine direkte Verbesserung der Umwelt, so dass ein Anspruch auf Übermittlung einer Liste (z. B. von Grundstücken) ausscheiden würde. Die Regelung des § 4 Abs. 1 UIG verschafft also nicht jedermann voraussetzungslos einen Anspruch auf Herstellung eines registerartigen Verzeichnisses, das es als öffentliches Register gerade nicht gibt.
- Hinsichtlich der Ausschlussgründe, die im öffentlichen oder privaten Interesse liegen (§§ 7 und 8 UIG), ist von besonderer Bedeutung, dass Daten, die von Dritten an die Behörde freiwillig gegeben werden, vom Informationsanspruch nicht umfasst sind. Im Bereich der Ausschlussgründe zum Schutz privater Belange ist von erheblicher Praxisrelevanz der Schutz der Betriebs- und Geschäftsgeheimnisse, die der Gesetzgeber allerdings nicht definiert hat. In der Gesetzesbegründung wird auf die Konkretisierung in Rechtsprechung und Literatur verwiesen. Wenn die Behörde Betriebs- und Geschäftsgeheimnisse offenbaren will, muss sie nach § 8 Abs. 2 Satz 1 UIG den Betroffenen anhören. Hierbei handelt es sich um eine gegenüber § 28 VwVfG speziellere Regelung, so dass insbesondere die dort geregelten Gründe, wann von einer Anhörung abgesehen werden kann, nicht eingreifen.

9.2 Die Århus-Konvention: Erweiterung des Informationszugangs im Bereich der Umwelt

Die Bundesregierung hat am 21. Dezember 1998 die UN-Konvention über den Zugang zu Informationen, die Öffentlichkeitsbeteiligung an Entscheidungsverfahren und den Zugang zu Gerichten in Umweltangelegenheiten, die sog. Århus-Konvention, gezeichnet.

Die Århus-Konvention besteht aus den drei „Säulen“:
– Zugang zu Informationen
– Öffentlichkeitsbeteiligung an Entscheidungsverfahren und
– Zugang zu den Gerichten.

Sie begründet einen umfassenden Anspruch von jedermann auf den ungehinderten Zugang zu Umweltinformationen bei Behörden, wobei von einem weiten Behördenbegriff ausgegangen wird. Es ist vorgesehen, dass eine Behörde einen Antrag auf Informationszugang nur unter bestimmten, im Einzelnen bezeichneten und eng auszulegenden Voraussetzungen ablehnen darf. Darüber hinaus verpflichtet die Konvention die Vertragsstaaten dazu, auch ohne entsprechenden Antrag bestimmte Umweltinformationen zugänglich zu machen. In diesem Zusammenhang werden z. T. auch bestimmte Formen, wie der Zugang vollzogen werden kann, geregelt.

Die Konvention sieht zunächst eine Öffentlichkeitsbeteiligung im Hinblick auf die Zulassung von Projekten mit erheblichen Umweltauswirkungen vor (insbesondere Industrieanlagen, Infrastrukturprojekte sowie sonstige raumbedeutsame Vorhaben). Diese sind in einem Anhang aufgelistet, ohne dass diese Auflistung jedoch abschließend zu verstehen ist. Hierbei schreibt die Konvention im Einzelnen vor, auf welche Weise die Öffentlichkeitsbeteiligung durchzuführen ist.

Darüber hinaus ist eine Öffentlichkeitsbeteiligung während der Vorbereitung umweltbezogener Pläne, Programme und Politiken vorgesehen. Hier werden aber lediglich allgemeine Vorgaben mit zum Teil nur empfehlendem Charakter gemacht.

Im Bereich Gerichtszugang regelt die Konvention Widerspruchsverfahren und Klagerechte für Einzelpersonen und Umweltverbände im Falle der Verweigerung des Informationszugangs im Hinblick auf Entscheidungen, die der Öffentlichkeitsbeteiligung unterliegen sowie im Hinblick auf Verstöße gegen umweltrechtliche Vorschriften allgemein.

Eine Anpassung des deutschen Rechts ist erst sinnvoll, wenn die EU ihre entsprechenden (EG-)Richtlinien an die Erfordernisse der Konvention angepasst hat; denn die Bestimmungen der Konvention fallen weitgehend in die Kompetenz der EG und werden somit über EG-Recht für Deutschland verbindlich sein (vgl. in diesem Zusammenhang auch Tz. 3.6).

Eine Zeichnung der Konvention begründet grundsätzlich noch keine völkerrechtlichen Verpflichtungen. Die Ratifikation der Konvention kann erst dann erfolgen, wenn die nationale Rechtslage den Erfordernissen der Konvention entspricht. Vor einer Ratifikation muss also das deutsche Recht an die Vorgaben der Konvention angepasst werden. Eine solche Anpassung ist aber erst dann sinnvoll, wenn die EU, die die Konvention ebenfalls gezeichnet hat, ihre entsprechenden Richtlinien an die Erfordernisse der Konvention angepasst hat. Vor diesem Hintergrund wird Deutschland die Konvention erst dann ratifizieren, wenn auf EU-Ebene die Ratifikation erfolgt ist.

9.3 Fragebogen zur Freistellung von der Überlassungspflicht für Bioabfälle

In einer Reihe von Eingaben wurde beklagt, dass seitens des Abfallwirtschaftsbetriebes eines Landkreises im Rahmen des Antrags auf Befreiung von der Biotonne ein Fragebogen verschickt worden war, der nach Auffassung der Petenten auch unzulässige, in den persönlichen Lebensbereich reichende Fragen enthalten hat.

Der Inhalt des verwendeten Fragebogens war aus datenschutzrechtlicher Sicht insbesondere deshalb problematisch, weil er – jedenfalls auf den ersten Blick – nicht nachvollziehbare Fragen enthielt, beispielsweise zur Gesamtgröße des Grundstücks oder zur Art der kompostierten Materialien.

Zum gesetzlichen Hintergrund:

Nach § 13 Abs. 1 KrW-/AbfG sind die Besitzer und Erzeuger von Abfällen aus privaten Haushalten verpflichtet, diese den öffentlich-rechtlichen Entsorgungsbetrieben zu überlassen. Eine Überlassungspflicht für Abfälle zur Verwertung besteht nicht, wenn der Abfallbesitzer oder -erzeuger zur Verwertung in der Lage ist. § 5 LAbfWAG ermächtigt und verpflichtet die entsorgungspflichtigen Körperschaften durch Satzung unter anderem, den Anschluss- und Benutzungszwang für die Einrichtungen der Abfallentsorgung zu regeln. Der Landkreis hatte hiervon mit der Abfallwirtschaftssatzung Gebrauch gemacht. Nach § 10 der Satzung ist von der Überlassungspflicht ausgenommen, wer gem. § 10 Abs. 1 Satz 1 KrW-/AbfG eine ordnungsgemäße und schadlose Abfallverwertung vornimmt. In solchen Fällen ist ein entsprechender Nachweis gegenüber dem Abfallwirtschaftsbetrieb zu führen. Nach § 12 der Satzung ist der Abfallbesitzer zur Auskunft über Art, Umfang, Herkunft, Beschaffenheit und Menge der Abfälle verpflichtet.

Der Abfallwirtschaftsbetrieb äußerte sich zu der Frage der Erforderlichkeit einer solchen Datenerhebung wie folgt: „Bei der Verwendung des selbst hergestellten Komposts besteht leicht die Gefahr der Überdüngung des Bodens. Insbesondere wenn neben der Grünschnittkompostierung auch noch Küchenabfälle der Kompostierung zugeführt werden, kann es vorkommen, dass dem

Boden mehr Nährstoffe zugeführt werden als durch die natürlichen Umsetzungsprozesse verloren gehen.“ Von daher ist im Sinne der §§ 13 und 5 des KrW-/AbfG die Prüfung notwendig, ob die Aufbringungsfläche für den fertigen Kompost in ausreichendem Verhältnis zur angefallenen Menge steht.

Des Weiteren wies der Abfallwirtschaftsbetrieb darauf hin, dass die entsorgungspflichtige Körperschaft die ordnungsgemäße und schadlose Eigenverwertung gem. § 5 KrW-/AbfG kontrollieren müsse und führte aus, dass in dem Fragebogen keine Angaben oder Verknüpfungen von Angaben vorgesehen seien, die Rückschlüsse auf individuelle Verhaltensweisen, wie z. B. Essgewohnheiten zulassen. Die Stoffe, die als Beispiele angeführt werden, seien heute in der Gesellschaft Standardprodukte, die außer in spezifischen Ausnahmefällen (z. B. Allergien) in nahezu jedem Haushalt bzw. Garten Verwendung fänden.

Die Ausführungen zur Erforderlichkeit konnten zumindest nicht widerlegt werden. Die Ausfüllung eines Fragebogens ist zudem als geringerer Eingriff in die Persönlichkeitssphäre des Abfallbesitzers zu werten, als dies beim Betreten des Grundstücks zur Prüfung der Befragungsvoraussetzungen der Fall wäre. Nach § 12 Abs. 3 der Abfallwirtschaftssatzung wäre dies jedoch zulässig gewesen.

Bei der datenschutzrechtlichen Bewertung des Fragebogens war ebenfalls von Bedeutung, dass die erhobenen Daten nicht automatisiert verarbeitet wurden. Der Abfallwirtschaftsbetrieb hatte hierzu mitgeteilt, dass die Fragebögen dem jeweiligen Vorgang lediglich beigefügt würden. Damit waren beispielsweise Abgleiche und Auswertungen mittels einer Datenverarbeitungsanlage im Hinblick auf personenbeziehbare Merkmale, wie Gattung des zu kompostierenden Materials oder Grundstücksgröße, ausgeschlossen.

Nach allem war aus der Sicht des Datenschutzes die Verwendung des Fragebogens nicht zu beanstanden.

10. Gesundheitswesen

10.1 Neuordnung des öffentlichen Gesundheitsdienstes

Mit dem Landesgesetz über den öffentlichen Gesundheitsdienst, dem Landesgesetz über die Eingliederung der Gesundheitsämter in die Kreisverwaltungen und dem Landesgesetz für psychisch kranke Personen – alle vom 17. November 1995 – hat der Gesetzgeber den öffentlichen Gesundheitsdienst im Lande Rheinland-Pfalz neu geordnet. Aus der Sicht der Landesregierung „war die Eingliederung der staatlichen Gesundheitsämter in die Kreisverwaltungen Voraussetzung für eine deutliche Effizienzsteigerung und ein Mehr an Bürgernähe der Gesundheitsverwaltung“ (Unterrichtung durch die Landesregierung; Drs. 13/4384, S. 8). Von den Landkreisen werde die Eingliederung des Gesundheitsamtes in die Kreisverwaltung durchweg positiv bewertet. Die hierzu abgegebenen Kommentare reichten von „logisch und konsequent“ über „sinnvoll“, „erfolgreich abgeschlossen“, „grundsätzlich positiv“ oder „positiv“ bis hin zu „sehr positiv“ und „ausgezeichnet“ (a. a. O.).

Die Entwicklung des Datenschutzes wurde aus der Berichterstattung der Landesregierung ausgeklammert. Kein Wort findet sich zu den Problemen, die schon seit längerer Zeit in der Diskussion (16. Tb., Tz. 10.1.1) oder aufgrund örtlicher Feststellungen in neuerer Zeit zu Tage getreten sind und mit den zuständigen Ressorts erörtert werden.

10.1.1 Arztpost auf dem Schreibtisch des Landrats

Im 16. Tb. berichtete der LfD unter Tz. 10.1.1, dass sich einzelne Landräte die gesamte eingehende Post vorlegen ließen und sie erst nach Kenntnisnahme an den Gesundheitsamtsleiter weitergaben. Der auf der Regelung in § 11 Abs. 6 ÖGdG beruhende Vorschlag des LfD, dass alle an das Gesundheitsamt gerichtete Postsendungen unmittelbar, d. h. ohne den Umweg über den Landrat, dem Amtsarzt vorgelegt werden, wurde nicht überall realisiert. Das Ministerium des Innern und für Sport hielt es für ausreichend, 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. Der Vorsitzende des Landkreistages wurde gebeten, die Kreisverwaltungen entsprechend zu informieren.

Der LfD äußerte sich skeptisch zu diesem Lösungsvorschlag. Er machte darauf aufmerksam, dass es kaum möglich ist, das Problem in der Weise zuverlässig zu lösen, dass die Empfänger von Briefen darauf hingewiesen werden, wie diese vom Absender zu adressieren sind.

Örtliche Feststellungen in einer Kreisverwaltung ergaben: Der Lösungsvorschlag des Ministeriums funktioniert nicht. In der dem Landrat zugeleiteten Post befanden sich, weil der Adressierungszusatz sowohl auf Postsendungen von Bürgern und Ärzten als auch von Behörden fehlte, Vorgänge, die eindeutig dem durch das Arztgeheimnis geschützten Bereich zuzuordnen waren. Es wurde auch eine Postsendung festgestellt, die in der Registratur geöffnet worden war, obwohl sie die Kennzeichnung „Vertrauliche Arztsache“ enthielt.

Eine Umfrage des LfD und weitere Prüfungen führten zu dem Ergebnis, dass wohl nur eine Minderzahl der Kreisverwaltungen das vom Ministerium vorgeschlagene Verfahren praktiziert. Die meisten Landräte lassen sich die eingehende Post nur dann und insoweit vorlegen, als nach der Öffnung im Gesundheitsamt festgestellt wird, dass es sich nicht um Arztsachen handelt. Probleme sind bei dieser Verfahrensweise nicht bekannt geworden.

Im Übrigen erhielt der LfD auch bei der erwähnten Umfrage die Bestätigung, dass sogar Untersuchungsaufträge von Behörden selten den Vermerk „Vertraulich“ oder „Arztsache“ enthalten. Tatsächlich seien aber rund 80 v. H. der an das Gesundheitsamt gerichteten Postsendungen als Arztsachen einzustufen.

Bei der Problemlösung müssen die gegenüber der Leitungs- und Organisationsbefugnis eines Landrats höherwertigen Rechtsgüter, nämlich das Grundrecht auf Datenschutz und das Arztgeheimnis, Vorrang haben. Nach § 11 Abs. 6 ÖGdG ist die innerbehördliche Organisation der Kreisverwaltung so zu gestalten, dass Geheimhaltungspflichten, insbesondere die ärztliche Schweigepflicht, gewahrt werden können. Gestützt auf diese gesetzliche Regelung fordert der LfD, dass die von ihm vorgeschlagene Verfahrensweise praktiziert wird. In der Sache wird er erneut an das Ministerium des Innern und für Sport herantreten.

10.1.2 Online-Zugriff eines Landrates auf die medizinischen Daten des Gesundheitsamtes

Örtliche Feststellungen in einer Kreisverwaltung ergaben, dass der Landrat – über ein Terminal in seinem Vorzimmer – und der Zentralabteilungsleiter im automatisierten Verfahren auf Daten des Gesundheitsamtes zugreifen können. Ohne dass dies im Gesundheitsamt auch nur bemerkt wird, können personenbezogene medizinische Daten in Bereiche gelangen, in dem sie durch das Arztgeheimnis nicht mehr geschützt sind und strafprozessuale Beschränkungen von Informationszugängen, wie das Zeugnisverweigerungsrecht oder Beschlagnahmeverbot, nicht gelten.

Der Landrat vertrat die Auffassung, dass der Online-Zugang deshalb berechtigt sei, weil er als Dienstvorgesetzter die Amtsärzte zu beurteilen habe.

Der LfD teilt diese Auffassung nicht. Die Datenspeicherung und -nutzung zu Aufsichts- und Kontrollzwecken ist nur dann zulässig, wenn sie zur Aufgabenerfüllung erforderlich ist und überwiegende schutzwürdige Interessen der betroffenen Person nicht entgegenstehen (§ 11 Abs. 2 Nr. 7 ÖGdG). Die danach gebotene Einzelfallprüfung der Nutzungsvoraussetzungen verträgt sich nicht mit dem Online-Zugriff, der dadurch gekennzeichnet ist, dass der Datenabruf ohne Prüfung der Verarbeitungsvoraussetzungen im Einzelfall erfolgt. Es stellt sich weiter die Frage nach der Verhältnismäßigkeit – Geeignetheit – einer Nutzung medizinischer Daten zu den genannten Zwecken durch den Landrat oder den Dezernenten. Wiederum ist es aber auch § 11 Abs. 6 Satz 2 ÖGdG, der mit der Forderung, bei der innerbetrieblichen Organisation die ärztliche Schweigepflicht zu wahren, Online-Zugriffen einen Riegel vorschiebt.

10.1.3 Eingliederung des Sozialpsychiatrischen Dienstes in das Gesundheitsamt

Der o. a. Unterrichtung durch die Landesregierung ist zu entnehmen, dass zwei Landkreise die Gesundheitsämter als Referate in die Kreisverwaltung eingegliedert haben. Örtliche Feststellungen in diesen beiden Landkreisen ergaben, dass die Sozialpsychiatrischen Dienste ebenfalls als selbständige Referate bestehen.

Der LfD hält dies für unzulässig, denn § 5 Abs. 1 Satz 1 PsychKG bestimmt, dass die Sozialpsychiatrischen Dienste bei den Gesundheitsämtern eingerichtet werden. Danach ist es zwingend, dass dem Leiter des Gesundheitsamtes Aufsichtsbefugnisse sowohl in rechtlicher als auch in dienst- und fachaufsichtlicher Hinsicht übertragen werden. Nur so können die Voraussetzungen geschaffen werden, dass sensible medizinische Informationen nur solchen Personen bekannt werden, die der Strafandrohung des § 203 Abs. 1 StGB unterliegen, und dass diese Informationen durch prozessuale Zeugnisverweigerungsrechte geschützt werden.

Das Ministerium für Arbeit, Soziales und Gesundheit bestätigte diese Rechtsauffassung im Wesentlichen. Es entspräche, so das Ministerium, den gesetzlichen Vorgaben kaum, wenn der gesamte Sozialpsychiatrische Dienst oder wesentliche seiner Teile außerhalb des Bereichs Gesundheitsamt angesiedelt würden. „Nehmen Sozialarbeiterinnen und Sozialarbeiter neben ihren eigentlichen Aufgaben im Rahmen des Sozialpsychiatrischen Dienstes nach dem Landesgesetz für psychisch kranke Personen auch in sonstigen Bereichen der Kreisverwaltung Aufgaben wahr – gegebenenfalls auch mit anderen Vorgesetzten –, könnte die datenschutzrechtliche ‚Zweckbindung‘ der erhobenen Daten gefährdet werden.“

Zum Berichtszeitpunkt sind die Vorgänge noch nicht abgeschlossen. Der LfD wird, sofern seine Rechtsauffassung von den Landkreisen nicht anerkannt wird, die gewählte Organisationsform beanstanden und darauf hinwirken, dass eine den gesetzlichen Bestimmungen entsprechende Organisationsform im Aufsichtswege durchgesetzt wird.

10.2 Warnmeldungen der Gesundheitsämter

Wie den Datenschutzbeauftragten bekannt wurde, unterrichten die Gesundheitsämter bzw. deren Fachaufsichtsbehörden (in Rheinland-Pfalz die Bezirksregierungen) die zuständigen Stellen anderer Bundesländer über die Erteilung, die Rücknahme und den Widerruf von Erlaubnisurkunden im Bereich der ärztlichen und nichtärztlichen Heilberufe. Die bundesweite gegenseitige Unterrichtung wird in erster Linie mit dem Schutz der Patienten begründet. Andernfalls könne die Berufsausübung in einem anderen Bundesland trotz Rücknahme, Widerrufs oder Ruhens nicht verhindert bzw. eine Neubeantragung von Approbationen und Berufserlaubnissen nicht angemessen beurteilt werden.

Nach Auffassung des LfD ist eine Rechtsgrundlage für diese Datenübermittlungen nicht ersichtlich. Auch stellt die Speicherung der übermittelten Daten in den Fällen, in denen der Betroffene sich rechtstreu verhält und die untersagte Tätigkeit in keinem anderen Bundesland wieder aufnimmt, eine unzulässige Vorratsdatensammlung dar. Der LfD favorisiert ebenso wie andere Datenschutzbeauftragte eine Lösung des Problems unter Nutzung des Bundeszentralregisters und hat sich daher seinerseits wiederholt an das Ministerium für Arbeit, Soziales und Gesundheit gewandt. Die Thematik wird derzeit wegen ihrer bundesweiten Bedeutung in der Arbeitsgruppe „Berufe des Gesundheitswesens“ der Arbeitsgemeinschaft der obersten Landesgesundheitsbehörden erörtert.

10.3 Tonbandaufzeichnungen bei Prüfungsgesprächen

Im 15. Tb., Tz. 10.2.3, hatte der LfD unter Hinweis auf die Rechtsprechung des Bundesverwaltungsgerichts (Urteil vom 3. August 1990 – 7 C 14/90 – NJW 1991, 118) die Auffassung vertreten, dass Tonbandaufzeichnungen als Informationseingriffe zu qualifizieren seien. Zugleich wies er aber auch darauf hin, dass gegen eine gesetzgeberische Entscheidung, Tonbandaufnahmen in Prüfungsverfahren zu verwenden, keine durchgreifenden verfassungsrechtlichen Bedenken bestünden, wenn die gesetzgeberische Grundentscheidung durch verfahrenssichernde Maßnahmen (Zweckbindung, gesicherte Aufbewahrung, Löschung) flankiert würde.

Im Berichtszeitraum wurde die Thematik im Blick auf die Entscheidung des Bundesverwaltungsgerichts vom 31. März 1994 – 6 B 65/93 – erneut mit einem Gesundheitsamt diskutiert.

Der Begründung dieser Entscheidung ist freilich nichts darüber zu entnehmen, was als eine Abkehr von der bisherigen Rechtsprechung des Bundesverwaltungsgerichts gewertet werden könnte. Insbesondere wird der Einsatz von Video- und Tonbandgeräten nicht für zulässig gehalten. Im Gegenteil: Es wird zum Ausdruck gebracht, dass deren Einsatz für eine ordnungsmäßige Dokumentation des Prüfungsgeschehens nicht geboten ist. Für das Gericht bestand kein Anlass für eine vertiefte Erörterung der Frage, inwieweit durch Tonbandaufzeichnungen in Persönlichkeitsrechte der Prüflinge eingegriffen wird. Gleichwohl knüpft es mit dem Satz „Insbesondere eine mit technischen Hilfsmitteln wie Tonband- und Videogerät etwa mögliche Perfektionierung der Aufnahme des Prüfungsgeschehens hätte auch offensichtliche Nachteile, weil dadurch die Prüfungsatmosphäre in aller Regel negativ beeinflusst sein wird und als Folge davon sowohl Prüfer als auch Prüflinge nicht mehr unbefangen und konzentriert wären, sondern abgelenkt oder gar verunsichert werden könnten“ an seine frühere Rechtsprechung an.

Noch dichter an der Sache liegt ein Urteil des VGH München vom 15. März 1995 (NJW 1996, 1614): Prüfung zur Erlangung der Facharztanerkennung. Der Begründung dieses Urteils ist folgender Satz zu entnehmen: „Noch weniger geeignet, weil die Atmosphäre von vornherein belastend, wäre es, würde ein Tonband mitlaufen oder würde das Gespräch gar mittels einer Videokamera aufgenommen.“

Im Ergebnis vertritt der LfD also auch weiterhin, dass die Tonbandaufzeichnung von Prüfungsgesprächen ohne normenklare gesetzliche Eingriffsgrundlage unzulässig ist.

10.4 Neufassung der Berufsordnung für Ärzte in Rheinland-Pfalz

Im 16. Tb. (Tz. 10.6.1) wurde bereits über die bevorstehende Novellierung der Berufsordnung für Ärzte berichtet. Der LfD hat hierzu gegenüber der Landesärztekammer rechtzeitig vor der Umsetzung der Musterberufsordnung in das Satzungsrecht Stellung genommen. Er hielt u. a.

- die Aufnahme von Bestimmungen über die Einführung und Verwendung von Patientenchipkarten,
- eine den gesetzlichen Vorschriften und den Vorgaben der Rechtsprechung entsprechende Regelung über das Akteneinsichtsrecht der Patienten
- sowie einen klarstellenden Hinweis auf die Zuständigkeit der Ärztekammer bei fehlender Praxisnachfolge oder fehlender Zustimmung des Patienten in die Übernahme von Behandlungsunterlagen durch den Praxisnachfolger

für angezeigt.

Letztlich wurde jedoch keiner der Änderungs- bzw. Ergänzungsvorschläge des LfD bei der Neufassung der Berufsordnung berücksichtigt. Dies ist insbesondere im Hinblick auf die Patientenchipkarten bedauerlich, zumal der Gesetzgeber, einer Empfehlung des LfD folgend, im HeilBG die Möglichkeit, diesbezügliche Regelungen in der Berufsordnung zu treffen, ausdrücklich vorgesehen hat (§ 23 Ziff. 3 HeilBG).

10.5 Vernichtung von ärztlichen Unterlagen

Ein Arzt hatte nach Ablauf der Aufbewahrungsfrist nach § 10 Abs. 3 der Berufsordnung seine Aufzeichnungen „einem Bekannten“ zum Zwecke der Entsorgung übergeben. Dieser lagerte die in Kartons verpackten Materialien bis zum Zeitpunkt der Vernichtung in einem Bereich, in dem sie für Unbefugte zugänglich waren. Tatsächlich wurden einzelne Blätter mit Aufzeichnungen über Patienten entnommen und einer an den LfD gerichteten Beschwerde beigefügt.

Der Arzt wurde über den Sachverhalt informiert, die Materialien wurden sofort gesichert und es ist wohl kein größerer Schaden eingetreten.

Der LfD wandte sich gleichwohl an die Landesärztekammer mit der Bitte, ihre Mitglieder auf die Sorgfaltspflichten bei der Vernichtung ärztlicher Unterlagen hinzuweisen. Einer Anregung der Ärztekammer folgend hat der LfD in einem im Ärzteblatt veröffentlichten Beitrag zu der Problematik wie folgt Stellung genommen:

„Nach § 10 Abs. 3 der Berufsordnung sind die Ärzte verpflichtet, ihre Aufzeichnungen für die Dauer von zehn Jahren nach Abschluss der Behandlung aufzubewahren, soweit nicht nach gesetzlichen Vorschriften eine längere Aufbewahrungspflicht besteht. Eine solche gesetzliche Regelung ist beispielsweise § 32 Abs. 2 der Strahlenschutzverordnung, wonach Aufzeichnungen über die Behandlung mit radioaktiven Stoffen 30 Jahre aufbewahrt werden müssen. Nach § 28 Abs. 4 Nr. 1 der Röntgenverordnung müssen Aufzeichnungen über Röntgenbehandlungen ebenfalls 30 Jahre nach der letzten Behandlung aufbewahrt werden. Hierbei handelt es sich um Mindestfristen.

Aus datenschutzrechtlicher Sicht wäre es im Hinblick auf die Interessen von Ärzten an einer möglichst umfassenden und langfristigen Patientenbetreuung einerseits, auf die Patienteninteressen an einem langfristigen Nachvollzug erfolgter Behandlungen andererseits (u. U. auch im Zusammenhang mit Arzthaftungsprozessen) nicht unangemessen, wenn ärztliche Unterlagen grundsätzlich für die Zeitdauer von dreißig Jahren aufbewahrt würden. Nach Ablauf dieser Frist sind Unterlagen zu vernichten und Daten zu löschen, denn das Zivilrecht kennt keine über die Zeitdauer von dreißig Jahren hinausgehende Verjährungsfrist.

Im Anwendungsbereich des Bundesdatenschutzgesetzes (Dateiverarbeitung in oder aus Dateien einschließlich der automatisierten Datenverarbeitung) ist allerdings zu beachten, dass Daten zu sperren sind, wenn ihre Kenntnis für die Erfüllung des Zweckes der Speicherung nicht mehr erforderlich ist (etwa nach Abschluss der Behandlung), gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen aber entgegenstehen (§ 35 Abs. 2 Nr. 3 i. V. m. Abs. 3 Nr. 1 BDSG). Für gesperrte Daten gilt, dass eine Übermittlung oder Nutzung der Daten nur dann zulässig ist, wenn es zu wissenschaftlichen Zwecken, zur Behebung einer bestehenden Beweisnot oder aus sonstigen im überwiegenden Interesse der speichernden Stelle oder eines Dritten liegenden Gründen unerlässlich ist und die Daten hierfür übermittelt oder genutzt werden dürften, wenn sie nicht gesperrt wären (§ 35 Abs. 7 BDSG).

Für die Vernichtung und Löschung von Datenträgern mit personenbezogenen Daten (dies sind sowohl Papierdatenträger wie auch magnetische – z. B. Disketten – , optische – z. B. MOD, magneto-optical disc – und sonstige – z. B. Carbon-Kassetten –) wurden in DIN 32 757 (01/1995) und DIN 33 858 (04/1993) Sicherheitsstufen festgelegt. Diese bestimmen je nach Sensitivitätsgrad des zu vernichtenden Materials unterschiedliche Grenzwerte für Zustand, Form und Größe der nach der Vernichtung verbleibenden Materialteilchen. Bei Informationsträgern mit besonders sensiblen personenbezogenen Daten (hierzu gehören medizinische Daten) soll nach der Empfehlung des Landesbeauftragten für den Datenschutz mindestens eine Vernichtung nach Stufe 4 sichergestellt sein. Dies bedeutet, dass eine Reproduktion unter Verwendung gewerbeüblicher Einrichtungen bzw. Sonderkonstruktionen ausgeschlossen ist. Wenn irgend möglich, sollte die Vernichtung indessen so erfolgen, dass eine Reproduktion nach dem Stand der Technik unmöglich ist (Stufe 5). Für magnetische Datenträger ist eine Löschdämpfung von mind. 45 dB gefordert; 90 dB sollten angestrebt werden. Bei der Beschaffung von Geräten (Schreddern usw.) sollten diese DIN-Anforderungen beachtet werden.

Ein Arzt muss die Datenträger mit Patientendaten nicht selbst vernichten oder löschen, er kann diese Arbeiten auch zuverlässigen Praxismitarbeiterinnen und -mitarbeitern übertragen oder Unternehmen beauftragen, die sich auf die Vernichtung und Löschung von Datenträgern spezialisiert haben. Im letztgenannten Falle folgt aber aus § 203 Abs. 1 StGB, dass der Arzt die Verfügungsgewalt über die Datenträger bis zur durchgeführten Vernichtung oder Löschung behalten muss. Dieser gesetzlichen Forderung kann nur dadurch entsprochen werden, dass sowohl der Transport der Datenträger wie auch deren Vernichtung durch den Arzt selbst oder einen Mitarbeiter oder eine Mitarbeiterin überwacht werden. Unabhängig davon fordert § 11 BDSG, dass solche Unternehmen unter besonderer Berücksichtigung der Eignung der von ihnen getroffenen technischen und organisatorischen Maßnahmen sorgfältig ausgewählt werden. Der Auftrag zur Datenträgervernichtung oder -löschung ist schriftlich zu erteilen, wobei die Datenverarbeitung oder -nutzung sowie die technischen und organisatorischen Maßnahmen festzulegen sind. Üblicherweise verwenden die Entsorgungsunternehmen standardisierte Auftragstexte; es sollte beachtet werden, dass die Einhaltung der oben erwähnten DIN-Anforderungen zugesichert wird.

Die Verantwortung für die ordnungsmäßige Durchführung der Löschung oder Vernichtung verbleibt bei dem Arzt (§ 11 Abs. 1 BDSG).

Wichtig ist, dass sich die Datenträger, die extern vernichtet oder gelöscht werden, zu keinem Zeitpunkt bis zur Vernichtung oder Löschung außerhalb der Kontrolle des verantwortlichen Arztes oder eines Arztgehilfen/einer Arztgehilfin befinden. Hieraus folgt z. B., dass sie auch bis zu diesem Zeitpunkt so gelagert werden, dass Unbefugte keinen Zugang haben."

10.6 Besuchskommission nach § 29 PsychKG; Berichterstattung an den Stadtrat oder Kreistag

Die nach dem PsychKG in einer psychiatrischen Einrichtung untergebrachten Personen sind in besonderem Maße schutzbedürftig. Der Gesetzgeber hat daher die Bildung von Besuchskommissionen durch die kommunalen Vertretungskörperschaften (Stadtrat bzw. Kreistag) vorgesehen. Die Besuchskommissionen haben die Aufgabe, die Einrichtungen regelmäßig zu besichtigen

und hierbei die Wahrung der Rechte der untergebrachten Personen zu überprüfen. Den untergebrachten Personen ist bei diesen Besichtigungen Gelegenheit zu geben, Wünsche und Beschwerden vorzutragen. Die Besuchskommission legt dem Stadtrat oder dem Kreistag nach jeder Besichtigung einen Bericht mit dem Ergebnis der Überprüfung vor (§ 29 Abs. 3 PsychKG).

Eine Kreisverwaltung wollte wissen, ob die Erörterung des Berichts in öffentlicher oder nicht öffentlicher Kreistagssitzung zu erfolgen habe. Der LfD sieht in § 29 Abs. 3 PsychKG keine Rechtsgrundlage für einen Eingriff in das informationelle Selbstbestimmungsrecht der Betroffenen und hält es daher für unzulässig, den Stadt- bzw. Kreistag in öffentlicher oder nicht öffentlicher Sitzung über Wünsche und Beschwerden untergebrachter Personen in personenbezogener Form zu unterrichten, es sei denn, die Personen hätten konkret dieser Datenweitergabe in einer rechtlich wirksamen Weise zugestimmt.

Zu klären war auch die Frage, ob die Besuchskommission vom Träger der Einrichtung verlangen kann, dass ihr zur Vorbereitung eines Kontrollbesuchs personenbeziehbare medizinische Daten zur Verfügung gestellt werden. In einem konkreten Falle verlangte sie die Datenübermittlung in folgender Gliederung: Alter des Patienten, Geschlecht, Art der Erkrankung, vorgesehene bzw. durchgeführte Therapie, Behandlungsplan.

Der LfD vertritt die Auffassung, dass das Besichtigungsrecht der Besuchskommission nicht die Befugnis umfasst, im Vorfeld eines Besuchs personenbezogene Daten der Heiminsassen zu erheben, denn diese Daten unterliegen dem Arztgeheimnis und es fehlt an einer normenklaren Rechtsgrundlage für dessen Durchbrechung.

10.7 Sanitätsdienst in Justizvollzugsanstalten

§ 182 Abs. 1 Satz 1 StVollzG bestimmt, dass personenbezogene Daten, die den in § 203 Abs. 1 Nr. 1, 2 und 5 StGB genannten Personen von einem Gefangenen als Geheimnis anvertraut oder über einen Gefangenen sonst bekannt geworden sind, gegenüber der Vollzugsbehörde der Schweigepflicht unterliegen. Um der Gefahr zu begegnen, dass der Schutz höherwertiger Rechtsgüter und die Erfüllung von gesetzlichen Aufgaben der Vollzugsbehörde in nicht hinnehmbarer Weise tangiert werden, hat der Gesetzgeber in den Sätzen 2 und 3 jedoch Ausnahmen zugelassen. Von besonderer Bedeutung ist Satz 2, der den in § 203 Abs. 1 Nr. 1, 2 und 5 StGB genannten Personen eine Offenbarungspflicht gegenüber dem Anstaltsleiter auferlegt, soweit dies für die Aufgabenerfüllung der Vollzugsbehörde oder zur Abwehr von erheblichen Gefahren für Leib oder Leben des Gefangenen oder Dritter erforderlich ist.

§ 182 Abs. 3 trifft ergänzende Regelungen. Er bestimmt, dass die offenbarten Daten nur für den Zweck, für den sie offenbart wurden oder für den eine Offenbarung zulässig gewesen wäre, und nur unter denselben Voraussetzungen verarbeitet oder genutzt werden dürfen, unter denen eine in § 203 Abs. 1 Nr. 1, 2 und 5 StGB genannte Person selbst hierzu befugt wäre. Beim Vorliegen dieser Voraussetzungen kann der Anstaltsleiter die unmittelbare Offenbarung gegenüber bestimmten Anstaltsbediensteten allgemein zulassen.

Das Ministerium der Justiz traf in Nr. 8 Abs. 3 seines Rundschreibens „Sanitätsdienst in Justizvollzugsanstalten“ vom 8. Februar 1999 folgende ergänzende Regelung: „Eine Schweigepflicht besteht nicht gegenüber der medizinischen Fachberaterin oder dem medizinischen Fachberater, ebenso wenig gegenüber dem Ministerium der Justiz, das im Benehmen mit dem Ministerium für Arbeit, Soziales und Gesundheit die Fachaufsicht führt.“

Der LfD vertrat in einer Stellungnahme hierzu die Auffassung, dass § 203 Abs. 1 StGB aufsichtsfest ist. Die Ausübung der Dienst- und Fachaufsicht begründet keine Befugnis im Sinne dieser Vorschrift. Dies gilt nicht nur für Ärzte und die in der Vorschrift genannten sonstigen Berufsangehörigen, sondern auch für Personen, die durch Gesetz in den Anwendungsbereich des § 203 Abs. 1 einbezogen wurden, im konkreten Falle den Anstaltsleiter. Der Anstaltsleiter darf private Geheimnisse i. S. von § 203 StGB nur beim Vorliegen der allgemeinen Rechtfertigungsgründe – Einwilligung, rechtfertigender Notstand usw. – oder dann offenbaren, wenn dies gesetzlich zugelassen ist. Aus dienstrechtlichen Pflichten folgt keine Offenbarungsbefugnis, weil solche Pflichten kein Recht zum Eingriff in die Rechtsgüter unbeteiligter Dritter gewähren.

Darüber hinaus sah er das Ministerium der Justiz aufgrund des Wortlautes von § 182 Abs. 3 Satz 2 gehindert zu bestimmen, dass die Schweigepflicht gegenüber der medizinischen Fachberaterin oder dem medizinischen Fachberater nicht gilt. Die Befugnis, die unmittelbare Offenbarung gegenüber bestimmten Anstaltsbediensteten allgemein zuzulassen, steht nur dem Anstaltsleiter zu.

Die Wahrnehmung von Aufsichtsbefugnissen bleibt im Übrigen unberührt. Dies gilt auch für das Selbsteintrittsrecht bzw. die Übertragung der Funktion des Anstaltsleiters auf eine andere Person. Der jeweilige Funktionsinhaber bleibt Normadressat. Er darf durch § 203 Abs. 1 geschützte personenbezogene Daten nur unter den Voraussetzungen des § 182 Abs. 3 StVollzG und nicht für Aufsichtszwecke weitergeben.

Auch die Tatsache, dass der in die Vertrauensbeziehung zwischen Arzt und Patient Eindringende selbst schweigepflichtig ist, kann nicht als Grundlage für eine Weitergabe von Geheimnissen angesehen werden (OVG Lüneburg, NJW 1975, 2261; Dreher/Tröndle § 203 Rndr. 26;). Dass die ärztliche Schweigepflicht mit der Schweigepflicht eines Amtsträgers nicht zu vergleichen ist, ergibt sich bereits aus der ausdrücklichen gesetzlichen Differenzierung zwischen § 203 Abs. 1 und Abs. 2 StGB. Die

Beziehungen, die § 203 Abs. 1 erfasst, sind in der Regel dadurch geprägt, dass ein Privater freiwillig und im eigenen Interesse einer dritten Person Geheimnisse offenbaren muss, um eine sachgerechte Behandlung seiner Probleme zu erfahren, während durch die Schweigepflicht der Amtsträger nach § 203 Abs. 2 dienstlich erlangte Geheimnisse, die nicht einem bestimmten Amtsträger, sondern vielmehr dem Repräsentanten der Behörde gegenüber offenbart wurden, geschützt werden sollen (Heintzen/Lilie, NJW 1997, S. 1601 ff.; Lenkner in: Schönke/Schröder, § 203 Rdnr. 45).

Auch das Urteil des BAG vom 13. Januar 1987 (RDV 1987, S. 136) zur Telefondatenerfassung eines bei einem Landkreis angestellten Psychologen geht in die vom LfD vertretene Richtung. Das Gericht hielt die Zielnummernerfassung für Zwecke der Dienst- oder Fachaufsicht für unzulässig.

Die Erörterungen der Sache mit dem Ministerium der Justiz waren zum Zeitpunkt der Berichtsabfassung noch nicht abgeschlossen.

10.8 Datenschutz im Krankenhaus

10.8.1 Zugriff des Landesrechnungshofs auf Patientendaten

Im Rahmen einer Prüfung der Wirtschaftsführung eines Krankenhauses in öffentlicher Trägerschaft beabsichtigte der Rechnungshof, auch nähere Feststellungen darüber zu treffen, ob die Art und Dauer der Behandlung von Patienten angemessen war (sog. Fehlbelegungsprüfungen). Zu diesem Zweck wollten die Prüfungsbeamten Patientenakten einsehen, die nach bestimmten Vorgaben (Verweildauer, Indikation usw.) ausgewählt werden sollten.

Von der Leitung des Krankenhauses wurde die rechtliche Zulässigkeit einer solchen Prüfung in Frage gestellt.

Der LfD wies in seiner Stellungnahme darauf hin, dass bei der Beurteilung der Rechtsfragen die verfassungsrechtliche Aufgabenzuweisung des Rechnungshofs (Art. 120 LV) berücksichtigt werden muss, die durch einfachgesetzliche Bestimmungen konkretisiert ist. Nach § 95 LHO besteht für die der Prüfungskompetenz des Rechnungshofs unterliegenden Stellen die – nach dem Wortlaut der Vorschrift unbeschränkte – Pflicht, die Unterlagen, die der Rechnungshof zur Erfüllung seiner Aufgaben für erforderlich hält, auf Verlangen innerhalb einer von ihm zu bestimmenden Frist zu übersenden oder seinen Beauftragten vorzulegen. Diese Vorlagepflicht kann mit dem Recht auf informationelle Selbstbestimmung kollidieren, dem gleichfalls Verfassungsrang zukommt (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG). Geht es um Patientendaten, so ist zu berücksichtigen, dass hier ein besonders hohes Schutzbedürfnis besteht. Durch die Strafbewehrung nach § 203 StGB wird dies unterstrichen.

Die Rechtsprechung erkennt an, dass Patientenakten der Vorlagepflicht an den Rechnungshof nicht grundsätzlich entzogen sind (BVerwG, Urteil vom 11. Mai 1989 – 3 C 68/85; BVerfG, Beschluss vom 29. April 1996 – 1 BvR 1226/89). In beiden Entscheidungen wird aber auch der Verfassungsgrundsatz der Verhältnismäßigkeit hervorgehoben. Wesentliche Elemente dieses Grundsatzes sind neben der Zweck/Mittel-Relation die Erforderlichkeit und die Geeignetheit.

Im konkreten Falle war insbesondere der letztgenannte Aspekt zu hinterfragen. Konkret ging es darum, ob die Vorlage von Patientenakten an den Rechnungshof ein geeignetes Mittel ist, um zu beurteilen, ob und ggf. in welchem Umfange Fehlbelegungen vorkommen.

Um in der Sache zu gesicherten Erkenntnissen zu gelangen, schlug der LfD vor, zunächst eine Prüfung unter Verwendung anonymisierter Patientenakten vorzunehmen. Er wies darauf hin, dass das Patientengeheimnis nicht verletzt wird, wenn aufgrund der Vorgaben des Rechnungshofs aus den Patientenakten Stichproben gezogen, diese kopiert, die Kopien durch Schwärzung des Patientennamens und der Anschrift anonymisiert und in dieser Form dem Rechnungshof vorgelegt werden.

Die Krankenhausleitung teilte mit, dass in dieser Weise verfahren worden sei. Es ist indessen noch nicht bekannt, wie die Frage der Verhältnismäßigkeit vom Rechnungshof abschließend beurteilt wird.

10.8.2 Informationen zum Datenschutz; Heft 4 – Datenschutz im Krankenhaus

Vor etwas mehr als zehn Jahren hat die Datenschutzkommission Rheinland-Pfalz in der Schriftenreihe „Informationen zum Datenschutz“ ein Heft „Datenschutz im Krankenhaus“ herausgegeben. Wenn die Nachfrage als Indikator für den Nutzen angesehen werden könnte, dann müsste dieser groß gewesen sein, denn es war notwendig, mehrere Neuauflagen herzustellen.

Immer deutlicher zeichnete sich indessen ab, dass eine grundlegende Überarbeitung geboten war. Zwar blieben die Datenschutzbestimmungen im Landeskrankenhausgesetz unverändert; andere Gesetze, die für den Datenschutz im Krankenhaus gleichfalls bedeutsam sind, wurden aber novelliert – z. B. das Sozialgesetzbuch –, die Rechtsprechung entwickelte sich und die Datenschutzkontrolle erbrachte neue Erkenntnisse.

Bei der Überarbeitung von Heft 4 „Datenschutz im Krankenhaus“ stand der Praxisbezug im Vordergrund. Ärzte und andere Bedienstete in Krankenhäusern bewegen sich bei ihrer Arbeit – auch – in einem rechtlich schwierigen Umfeld. Die Veröffentlichung will Hilfestellungen geben und dazu beitragen, dass der Datenschutz unter gewandelten Arbeitsbedingungen den Stellenwert behält, den er traditionell im medizinischen Bereich hat.

An der Veröffentlichung haben nicht nur Mitarbeiterinnen und Mitarbeiter aus der Behörde des LfD mitgewirkt; es wurden auch Ergebnisse der Datenschutzkontrolle in anderen Ländern sowie Hinweise aus der Praxis einbezogen und es konnte auf Vorarbeiten aus Arbeitskreisen der Datenschutzbeauftragten zurückgegriffen werden.

Auch die Nachfrage zu der Neufassung von Heft 4 ist wieder groß. Sein Bezug ist kostenfrei. Der Inhalt steht im Format Word 97 auf der Homepage des LfD (www.datenschutz.rlp.de) zum Download zur Verfügung.

10.9 Patientenchipkarten; Modellversuch Neuwied/Rhein

Über den Modellversuch zur Einführung und Nutzung einer Patientenchipkarte berichtete der LfD im 15. Tb., Tz. 10.8 und im 16. Tb., Tz. 10.6.2. An der Einschätzung, dass das Projektziel – Verbesserung der ärztlichen und medikamentösen Versorgung – wegen mangelnder Akzeptanz sowohl bei den Ärzten und Apotheken wie auch bei Patienten und Kunden gefährdet ist, hat sich in der seit der letzten Berichterstattung vergangenen Zeit nichts geändert.

Die Ergebnisse einer Befragung von Patienten, Ärzten und Apothekern zur Akzeptanz von medizinischen Patientenkarten/Apothekenkarten im ambulanten Gesundheitswesen wurde in einem Positionspapier zum Thema „Ergebnisse und Konsequenzen aus Feldversuchen mit Medizinischen Patientenkarten für die Erprobung mit der gesetzlichen Krankenversichertenkarte“ wie folgt zusammengefasst:

> „Im Ergebnis zeigt der Modellversuch, dass die Idee der Einführung einer zur gesetzlichen Krankenversicherten komplementären, freiwilligen Patientenkarte – trotz hohem Werbeaufwand – die vollständige Durchdringung in der Region nicht erreicht. Der Nutzen der Karte kann sich deshalb nicht voll entfalten. Dies bedeutet, dass der Routineeinsatz von Patientenkarten auf freiwilliger Basis nicht weiter verfolgt werden sollte. Verfolgt werden sollte aber die Idee der Integration von wenigen wichtigen medizinischen Befunddaten für Notfallzwecke in die gesetzliche Krankenversichertenkarte. Die Krankenversichertenkarte hat wegen ihres obligatorischen Gebrauchs eine hohe Verbreitung. Auf der Krankenversichertenkarte sollte in Zukunft durch gesetzliche Änderungen auch die Möglichkeit geschaffen werden, die technischen Voraussetzungen vorzuhalten, damit auf einem gesonderten Datenspeicher mit gesonderter Zugriffsberechtigung auf freiwilliger Basis medizinische Daten und Arzneimitteldaten gespeichert und von zugriffsberechtigten Ärzten und Apothekern gelesen werden können.“
>
> Parallel zur Verfolgung dieser Ziele wird auch die Diskussion um die rechtlichen Schranken solcher Eingriffe wieder aufleben, die mit der strikten Beschränkung des Inhalts der Krankenversichertenkarte auf Identifikationsdaten und Grundinformationen über das Versicherungsverhältnis durch § 291 SGB V unterbrochen war.
>
> Im Blick auf mögliche funktionale Erweiterungen mit dem Ziel, den Modellversuch Neuwied/Rhein doch noch zu einem befriedigenden Abschluss zu bringen, haben die Projektverantwortlichen vorerst davon abgesehen, die vorhandene technische Infrastruktur zu beseitigen. Der Modellversuch befinde sich, so teilten sie dem LfD mit, in einer „Standby-Phase“.

11. Sozialdatenschutz

11.1 Gesetzliche Änderungen im Sozialgesetzbuch

11.1.1 Gesundheitsreform 2000

Die Bundesregierung hat im Sommer 1999 den Entwurf eines Gesetzes zur Reform der gesetzlichen Krankenversicherung ab dem Jahr 2000 (GKV-Gesundheitsreform 2000) vorgelegt. Der umfangreiche Entwurf beinhaltete auch zahlreiche datenschutzrechtlich bedenkliche Änderungen. So war u. a. vorgesehen, im ambulanten Bereich die Abrechnungsdaten von den Kassenärztlichen Vereinigungen nicht nur fallbezogen, sondern auch versichertenbezogen an die Krankenkassen zu übermitteln. Die Krankenkassen hätten Versichertenkonten anlegen und Krankheitsverläufe für einzelne Versicherte dokumentieren können. Bei den Krankenkassen wäre der „gläserne Patient“ entstanden. Auch die Beratungsaufgaben der Krankenkassen sollten nach dem Entwurf deutlich ausgeweitet werden. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat sich in einer Entschließung zu dem Gesetzentwurf geäußert (Anlage 18). Der LfD hat zum Entwurf gegenüber dem Ministerium für Arbeit, Soziales und Gesundheit ausführlich Stellung genommen. Zwischenzeitlich hat das Bundesgesundheitsministerium signalisiert, den Entwurf unter Einbeziehung der datenschutzrechtlichen Forderungen zu überarbeiten.

11.1.2 Änderung des § 68 SGB X durch das Medizinproduktegesetz

„Unter dem – zumindest irreführenden – Titel ‚Änderung des Medizinproduktegesetzes‘ hat der Deutsche Bundestag in einem parlamentarischen Schnellverfahren am 18. Juni 1998 (der Bundesrat am 10. Juli 1998) einer Änderung des § 68 SGB X zugestimmt (1. MPG-ÄndG vom 6. August 1998; BGBl. I S. 2005). Der Datenkatalog des Absatzes 1 Satz 1 wurde u. a. um das Merkmal ‚derzeitiger oder zukünftiger Aufenthalt‘ erweitert und es wurden die Worte ‚im Einzelfall auf Ersuchen‘ eingefügt. Damit ist die über ein Jahrzehnt währende Diskussion um Richtigkeit oder Unrichtigkeit des Berliner Urteils beendet: Die Tatsache, dass sich ein Sozialleistungsempfänger oder Antragsteller gerade in der Dienststelle aufhält, darf der Polizei und allen anderen in der Überschrift des § 68 genannten Behörden mitgeteilt werden. Und nicht nur dies: Auch der zukünftige Aufenthalt ist ein übermittlungsfähiges Merkmal, das heißt, auch Terminvereinbarungen können von der Polizei zur Vorbereitung von Festnahmen genutzt werden. Jugendämter, Arbeitsämter, gesetzliche Krankenkassen und Berufsgenossenschaften sind ebenso betroffen wie Sozialämter. Sie werden, wie es Datenschutzbeauftragte in einer Presseerklärung ausdrückten, zu ‚Hilfsbeamten von Strafverfolgungs- und Vollstreckungsbehörden‘.

Ohne Zweifel schafft die Neufassung Rechtsklarheit in einem Bereich, der seit vielen Jahren umstritten ist. Dies liegt grundsätzlich auch im Interesse der Mitarbeiterinnen und Mitarbeiter der Sozialleistungsbehörden, die sich wegen der früheren unklaren Rechtslage in derartigen Fällen je nach ihrem Verhalten entweder dem Vorwurf der Verletzung des Sozialgeheimnisses oder dem Vorwurf der Strafvereitelung ausgesetzt sahen. Zugleich kann sie aber auch die Ursache bilden für nachhaltige Störungen des Verhältnisses zwischen Leistungsträger und Leistungsempfänger. Besonders deutlich wird dies im Bereich der Jugendhilfe. Nach § 64 Abs. 2 SGB VIII ist die Zulässigkeit einer auf § 69 SGB X beruhenden Datenübermittlung zwar auch weiterhin danach zu beurteilen, ob durch diese Übermittlung der Erfolg einer zu gewährenden Leistung in Frage gestellt wird. § 68 SGB X kennt eine solche Differenzierung aber nicht, das heißt, die Gefährdung des Erfolgs einer zu gewährenden Leistung bildet kein Übermittlungshindernis. Zwar dürfen schutzwürdige Interessen Betroffener einer Übermittlung nicht entgegenstehen, aber das Interesse, staatlicher Strafverfolgung zu entgehen, ist kein solches Interesse. Auch die Ausgestaltung der Vorschrift als Übermittlungsbefugnis (... ist es zulässig ... zu übermitteln) hilft im Blick auf die grundsätzliche Amtshilfepflicht nicht weiter. Wenn die Voraussetzungen des § 68 SGB X vorliegen, haben die Sozialleistungsträger die in der Vorschrift genannten Behörden zu unterrichten.

Hervorzuheben ist freilich auch, dass eine Datenübermittlung ohne Ersuchen im Einzelfall unzulässig ist. Die Sozialbehörden dürfen also nicht von sich aus tätig werden; dies ist nur beim Vorliegen der Voraussetzungen der §§ 69 Abs. 1 Nr. 1 und 71 Abs. 1 Nr. 1 SGB X erlaubt. Auch ein Ersuchen, das darauf gerichtet ist, alle der Sozialbehörde bekannt werdenden Fälle zu melden, darf nicht beachtet werden. Wie schon bisher gilt, dass die ersuchte Stelle zur Datenübermittlung nicht verpflichtet ist, wenn sich die ersuchende Stelle die Angaben auf andere Weise beschaffen kann. Über das Übermittlungsersuchen hat der Leiter der ersuchten Stelle, sein allgemeiner Stellvertreter oder ein besonders bevollmächtigter Bediensteter zu entscheiden (§ 68 Abs. 2 SGB X).

Wichtig ist es, auf Beschränkungen der Übermittlungsbefugnis hinzuweisen, die sich nicht unmittelbar aus § 68 SGB X ergeben, gleichwohl aber zu beachten sind. Die besonderen Geheimhaltungsvorschriften nach § 203 StGB (z. B. für Sozialarbeiter) und nach § 65 SGB VIII (Beratungsgeheimnis in der Jugendhilfe) verbieten es den hier genannten Funktionsträgern, einem Auskunftsersuchen zu entsprechen. Als speziellere Vorschriften gehen sie § 68 SGB X vor.

Die Gesetzesänderung kennzeichnet eine tief greifende Änderung des Sozialdatenschutzes. Aus der Sicht vieler Datenschutzbeauftragter und Sozialbehörden geht sie zu weit. Es stellt sich die Frage, warum das Problem – wenn es denn eines gab – nicht durch eine angemessene Änderung des § 73 SGB X, etwa durch Wegfall des Richtervorbehalts für die Datenübermittlung bei gleichzeitiger Beschränkung auf Personen, die zur Festnahme ausgeschrieben sind, gelöst wurde.

Die Einbeziehung des zukünftigen Aufenthalts birgt ein erhebliches Missbrauchspotential. Zwar haben die Sozialleistungsträger keine Befugnis, die Betroffenen zu täuschen und sie mit anderer Begründung zum Zwecke der Festnahme vorzubestellen. Aber: Wie behandelt die Praxis dieses Problem und vor allen Dingen, wer kann das nachprüfen?

Sicherlich wird das Sozialgeheimnis durch die Änderung des § 68 SGB X nicht zur Farce, wie eine Reihe von Datenschutzbeauftragten öffentlich erklärte. Aber es wird in seiner Wirksamkeit weiter herabgesetzt, denn dies ist nicht die einzige Änderung zum Nachteil des Sozialdatenschutzes. Die Verschärfung des Überwachungsdrucks für Sozialhilfeempfänger durch die kürzlich erfolgte Änderung des § 117 BSHG oder die ständigen Bemühungen um Kostendämpfung durch Herstellung von Datentransparenz in der Krankenversicherung sind andere Beispiele. Richtig ist wohl, dass sich die derzeitige politische Diskussion des Themas zu sehr auf die polizeiliche Effektivität konzentriert und andere, gleichermaßen bedeutsame Ziele staatlichen Handelns zurückstehen."

(Anmerkung: Vgl. im Einzelnen Schuber, Die Sozialbehörden als Informationsquellen der Polizei? Kommunal-Praxis, 1998, 342)

11.2 Sozialhilfe

11.2.1 Was lange währt, ...

Der LfD ist stets bemüht, auch Anfragen mit komplizierten Sachverhalten oder schwierigen Rechtsfragen zeitnah zu beantworten. Erfordert die Vorgangsbearbeitung jedoch die Beteiligung anderer Stellen, kommt es häufig zu Verzögerungen, die insbesondere für den Petenten kaum nachzuvollziehen sind. Auffallend ist, dass im Berichtszeitraum die sog. „Schubverfügungen" deutlich zugenommen haben. Wurde beispielsweise eine öffentliche Stelle vom LfD um eine Stellungnahme gebeten, veranlasste diese zunächst im eigenen Zuständigkeitsbereich oder auch über die Zuständigkeitsgrenzen hinaus eine Rundfrage zum Problem. Die Antwort bestand dann in der Darstellung von Auffassungen, die von irgendwelchen an der Sache nicht beteiligten Stellen vertreten werden. Die geforderte eigene Beurteilung von Rechtsfragen des Datenschutzes kommt bei diesem Verfahren zu kurz. Gelegentlich kommt es auch zu einer Form des Kreisverkehrs, wenn der LfD aufgrund örtlicher Feststellungen Abstimmungsbedarf mit der Aufsichtsbehörde sieht, diese die Meinung der betroffenen Verwaltung erfragt und sie inhaltlich unverändert an den LfD weitergibt. Dass durch eine solche Verfahrensweise eine zügige Bearbeitung von Anfragen nahezu ausgeschlossen ist, liegt auf der Hand.

Einen „Dauerbrenner" in diesem Sinne bildete das von einer Stadtverwaltung verwandte Formular „Anfrage über den Arbeitsverdienst" (vgl. 16.Tb.,Tz. 11.5.4). Hierin wurden dem Arbeitgeber vom Sozialhilfeträger weit mehr Informationen abverlangt als gesetzlich zugelassen (§ 116 Abs. 2 BSHG). So sollte dieser beispielsweise über Lohnpfändungen, Abtretungen und die Kran-

kenkasse seines Arbeitnehmers Auskunft geben. Tatsächlich besteht eine Auskunftspflicht des Arbeitgebers gegenüber dem Träger der Sozialhilfe lediglich in Bezug auf die Art und Dauer der Beschäftigung, die Arbeitsstätte und den Arbeitsverdienst. Nachdem die Stadtverwaltung zunächst davon überzeugt werden musste, dass weder der Kauf von Vordrucken bei einer Verlagsgesellschaft noch die Verwendung inhaltsgleicher Vordrucke in anderen Kommunen die rechtliche Zulässigkeit der Datenerhebung begründen, legte sie schließlich ein inhaltlich reduziertes, den gesetzlichen Anforderungen entsprechendes Formular vor. Dass es gleichwohl erst nach zwei Jahren zu einer landesweiten Übernahme des Musters kam, mag mit der eingangs erwähnten Praxis in Zusammenhang stehen.

11.2.2 Übermittlung von Sozialdaten an die Staatsanwaltschaft

Die Prüfung der sachlichen Voraussetzungen für die Gewährung von Hilfe zum Lebensunterhalt durch das Sozialamt einer Stadt ergab, dass ein Hilfeempfänger über einen längeren Zeitraum Mietzuschuss für eine Wohnung erhielt, die nur als Rohbau existierte, also gar nicht bewohnbar war.

Die Leistungsgewährung wurde eingestellt; sowohl der Hilfeempfänger als auch der Vermieter wurden wegen Betrugs angezeigt. Gegen den Einstellungsbescheid legte der Hilfeempfänger Widerspruch ein.

Der Sozialhilfeträger erbat eine Äußerung des LfD zu der Frage, ob er befugt ist, der Staatsanwaltschaft in dem Strafverfahren gegen den Vermieter den Widerspruchsbescheid, der die Einstellung der Sozialhilfe des Mieters betrifft, vorzulegen. Ein besonderes Problem sah das Sozialamt darin, dass die Staatsanwaltschaft die Vorlage einer richterlichen Anordnung nach § 73 SGB X ablehnte.

Der LfD bezweifelte in seiner Stellungnahme, ob § 73 SGB X im konkreten Falle überhaupt als Rechtsgrundlage für eine Datenübermittlung an die Staatsanwaltschaft herangezogen werden konnte, denn es ging nicht um die Durchführung eines Strafverfahrens wegen eines Verbrechens oder wegen einer sonstigen Straftat von erheblicher Bedeutung (Absatz 1). Auf Absatz 2 – Sozialdatenübermittlung zur Druchführung eines Strafverfahrens wegen einer anderen Straftat – kann die Weitergabe eines Widerspruchsbescheids ebenfalls nicht gestützt werden, denn die Vorschrift lässt nur die Übermittlung der in § 72 Abs. 1 Satz 2 genannten Angaben und die Angaben über erbrachte oder demnächst zu erbringende Geldleistungen zu. Im Übrigen stehen beide Übermittlungsalternativen unter dem Vorbehalt einer richterlichen Anordnung, deren Vorlage die Staatsanwaltschaft ausdrücklich ablehnte.

Auch § 68 SGB X schied als Übermittlungsgrundlage aus, denn diese Vorschrift lässt – auch in der jetzt erweiterten Fassung – ebenfalls nur die Weitergabe bestimmter, im Einzelnen aufgezählter Angaben zu.

Auch § 69 Abs. 1 Nr. 2 enthielt für den konkreten Fall keine Übermittlungsbefugnis, denn diese Vorschrift deckt nicht die Datenübermittlung im Rahmen von behördlichen Verfahren, auch wenn sie zur Vorbereitung, aus Anlass oder aufgrund eines gerichtlichen Verfahrens durchgeführt werden (Hase in GK-SGB X 2, § 69 Rz. 103). Auf staatsanwaltliche und polizeiliche Ermittlungsverfahren ist sie nicht anzuwenden, ebenso wenig auf Bußgeld- oder Disziplinarverfahren (Hauck/Haines-Walloth, SGB-Komm., § 69 RdNrn. 25, 27).

Als Rechtsgrundlage für eine Datenweitergabe an die Staatsanwaltschaft kommt aber grundsätzlich § 69 Abs. 1 Nr. 1 erste Alternative in Betracht, denn es gehört auch zu den Aufgaben eines Sozialleistungsträgers, Strafverfahren einzuleiten oder zu fördern, die einen Bezug zur Leistungsgewährung haben. Dabei kommt es keineswegs darauf an, dass Hilfeempfänger selbst Beschuldigte sind. Es kann auch Aufgabe des Leistungsträgers sein, staatsanwaltschaftliche Ermittlungen deshalb zu fördern, weil durch die generalpräventive Wirkung von Strafverfahren Vermieter davon abgehalten werden, an Betrugshandlungen von Leistungsempfängern mitzuwirken.

Von Bedeutung ist, dass Übermittlungsfälle nach § 69 Abs. 1 Nr. 1 – anders als Fälle nach § 69 Abs. 1 Nr. 2 – allein aus der Perspektive des Leistungsträgers zu beurteilen sind (vgl. Hase a. a. O., Rz. 96, 97). Wichtig ist auch, dass nur die zur Aufgabenerfüllung erforderlichen Daten übermittelt werden dürfen. Ob diese Voraussetzung bezüglich des gesamten Inhalts eines Widerspruchsbescheids vorliegt, ist im Einzelfall zu prüfen.

11.2.3 Fragebogen zum Vorliegen einer nichtehelichen Lebensgemeinschaft

Personen, die in eheähnlicher Gemeinschaft leben, dürfen hinsichtlich der Voraussetzungen sowie des Umfanges der Sozialhilfe nicht besser gestellt werden als Ehegatten (§ 122 BSHG). Um festzustellen, ob eine nichteheliche Lebensgemeinschaft vorliegt, setzen Sozialämter häufig Fragebogen ein, in denen die Betroffenen z. B. darüber Auskunft geben sollen, wie häufig sich der Partner in der Wohnung aufhält, ob er dort auch übernachtet, ob gemeinsam eingekauft wird und wer die Hausarbeiten ausführt. Obwohl solche Informationen größtenteils den Bereich privater Lebensführung von Sozialhilfeempfängern und deren Mitbewohnern betreffen, ist dies im Grundsatz nicht zu beanstanden. Wie anders als durch Befragung soll ein Sozialamt die Voraussetzungen des § 122 BSHG prüfen können? Gegenüber dem Einsatz von sog. Sozialhilfeermittlern (vgl. Tz. 11.2.6) stellt das Ausfüllen eines Fragebogens jedenfalls das mildere Mittel dar.

Ein Sozialamt verwandte ein Formular, in dem der Betroffene u. a. auch die Beziehung zu seinem Wohnungspartner wie folgt charakterisieren sollte:

– „freundschaftlich oder
– intensiv mit inneren Bindungen, gegenseitiger Verantwortlichkeit, gegenseitige Anteilnahme am persönlichen Leben und auf längere Dauer oder
– keine persönliche Beziehung, sondern reine Zweckgemeinschaft ...“

Die Frage nach der Einschätzung von persönlichen Gefühlen gegenüber dem Wohnungspartner ist nach Auffassung des LfD weder erforderlich noch verhältnismäßig. Sie betrifft einen den staatlichen Institutionen grundsätzlich nicht zugänglichen Intimbereich des Betroffenen. Darüber hinaus kommt es nach höchstrichterlicher Rechtsprechung auf innere Bindungen oder auf das Bestehen von Verpflichtungen zur Unterhaltsgewährung oder zur gemeinsamen Lebensführung ebenso wenig an wie darauf, ob die Partner durch geschlechtliche Beziehungen miteinander verbunden sind.

Das Formular wurde unter Verzicht auf diese Frage überarbeitet.

11.2.4 Arbeitsunfähigkeitsbescheinigung bei der Verrichtung gemeinnütziger Arbeit

In einer Eingabe ging es um die Frage, ob bei einem Sozialhilfeempfänger, der zur Verrichtung gemeinnütziger Arbeit herangezogen wird und angibt, arbeitsunfähig zu sein, die gleichen Grundsätze in Bezug auf Arbeitsunfähigkeitsbescheinigung und ärztliche Schweigepflicht zu gelten haben, wie dies bei einem Arbeitnehmer gegenüber seinem Arbeitgeber der Fall ist. Der LfD beurteilte den Sachverhalt wie folgt:

Die Übermittlung von Diagnosedaten an den Sozialleistungsträger stellt eine Durchbrechung der ärztlichen Schweigepflicht dar. Diese ist jedoch dann zulässig, wenn eine Rechtsvorschrift die Übermittlung von Patientendaten zulässt oder wenn der Patient seine Einwilligung zu der Datenübermittlung erklärt hat. Diese Einwilligungserklärung kann auch als Obliegenheit gegenüber dem Sozialleistungsträger erfolgen, denn die Verpflichtung, sich einer ärztlichen Untersuchung zu unterziehen und der Übermittlung des Untersuchungsergebnisses zuzustimmen, zählt zu den Mitwirkungspflichten des Sozialhilfeempfängers gegenüber dem Leistungsträger.

Ein Sozialhilfeempfänger hat nach § 18 BSHG auch seine Arbeitskraft zur Beschaffung des Lebensunterhaltes einzusetzen und kann daher zu gemeinnütziger Arbeit herangezogen werden (§ 19 Abs. 2 BSHG). Macht ein Sozialhilfeempfänger geltend, arbeitsunfähig zu sein, kann der Träger der Sozialhilfe verlangen, dass der Hilfe Suchende sich einer (amts-)ärztlichen Untersuchung unterzieht (vgl. § 62 SGB I) und das Ergebnis dem Sozialleistungsträger vorlegt oder dessen Übermittlung an den Sozialleistungsträger zustimmt. Voraussetzung ist jedoch, dass dies für die Aufgabenerfüllung, insbesondere zur Prüfung der Leistungsverpflichtung gegenüber dem Hilfe Suchenden, erforderlich und verhältnismäßig ist.

Die Angabe von Diagnosen ist in Fällen der vorliegenden Art erforderlich, da die ärztliche Bescheinigung nicht nur der Überprüfung der Arbeitsunfähigkeit dient, sondern auch Grundlage für die weitere Verwendung des Hilfeempfängers ist. Dem Sozialhilfeträger steht nämlich bei der Ausgestaltung des Arbeitseinsatzes ein Ermessensspielraum zu, den er unter Berücksichtigung der örtlichen Verhältnisse und der besonderen Situation des Hilfeempfängers auszufüllen hat. Dem Hilfe Suchenden darf daher beispielsweise keine Arbeit zugemutet werden, zu der er körperlich oder geistig nicht in der Lage ist (§ 18 Abs. 2 BSHG). Die Diagnoseangabe ist geeignet und erforderlich, um die Überzeugungsgewissheit des Sozialleistungsträgers zu begründen, dass der Sozialhilfeempfänger die ihm zugewiesene Arbeit tatsächlich nicht ausüben kann.

Aufgrund der besonderen Ausgestaltung des Verhältnisses Sozialhilfeempfänger – Leistungsträger ist dieser Fall mit dem eines Arbeitnehmers gegenüber seinem Arbeitgeber nicht vergleichbar.

Im Ergebnis ist daher die Angabe der Diagnose auf einer ärztlichen Bescheinigung bei der Heranziehung eines Sozialhilfeempfängers zu gemeinnütziger Arbeit zulässig.

11.2.5 Die Einholung von Bankauskünften im Sozialleistungsverfahren

Gegenstand der Berichterstattung über Vordrucke im Sozialleistungsbereich (13. Tb., Tz. 11.3.3, 14. Tb., Tz. 11.3.2, 16. Tb., Tz. 11.5.8) ist regelmäßig auch die Einwilligungserklärung in die Einholung von Bankauskünften. Der LfD hat stets vertreten, dass es nicht zulässig ist, bei der Beantragung von Sozialleistungen routinemäßig eine solche Einwilligungserklärung einzuholen. Voraussetzung sei vielmehr, dass im Einzelfall der Verdacht bestehe, die Einkommens- und Vermögensverhältnisse seien bei der Antragstellung nicht vollständig oder nicht zutreffend dargestellt worden.

Die Rechtsauffassung des LfD wird gestützt durch einen Beschluss des HessVGH vom 7. Februar 1995 – 9 TG 3113/94 – . Das Gericht stellte fest, dass das Verlangen, der Einholung von Bankauskünften zuzustimmen, ohne Vorliegen konkreter Anhaltspunkte eine überflüssige Ermittlungstätigkeit des Sozialhilfeträgers darstelle und somit nicht „erforderlich“ i. S. von § 60 Abs. 1 Nr. 1 SGB I sei. Es führte in der Entscheidung aus, dass auch die Befugnis des Sozialhilfeträgers, im Rahmen des ihm nach § 20 SGB X eingeräumten Ermessens, über das Ausmaß der Ermittlungen zu entscheiden, nicht bedeute, dass die Behörde auf der Grundlage einer nicht näher begründeten pauschalen Verdächtigung grundsätzlich davon ausgehen dürfe, die von dem Hilfe Suchenden abgegebene Erklärung über seine Einkommens- und Vermögensverhältnisse könnten unwahr sein.

11.2.6 Missbrauchskontrolle bei der Gewährung von Sozialhilfe

§ 117 Abs. 1 bis 2 a BSHG lässt nach seiner Neufassung durch Gesetz vom 23. Juli 1996 (BGBl. I S. 1088) zu, dass Sozialdaten im automatisierten Verfahren zwischen den Trägern der Sozialhilfe sowie mit den Trägern der gesetzlichen Unfall- und Rentenversicherung sowie der Bundesanstalt für Arbeit abgeglichen werden. Nach Absatz 3 sind die Sozialhilfeträger ferner befugt, zur Vermeidung rechtswidriger Inanspruchnahme von Sozialhilfe Daten von Leistungsempfängern bei anderen Stellen ihrer Verwaltung, bei ihren wirtschaftlichen Unternehmen und bei den Kreisen, Kreisverwaltungsbehörden und Gemeinden zu überprüfen, soweit diese für die Erfüllung dieser Aufgaben erforderlich sind. Auch diese Überprüfung darf regelmäßig im Wege des automatisierten Datenabgleichs durchgeführt werden.

11.2.6.1 Der Datenabgleich nach § 117 Abs. 1 bis 2 a BSHG

Der Datenabgleich nach diesen Vorschriften wird in der Weise durchgeführt, dass Sozialdaten von den am Abgleich beteiligten Sozialleistungsträgern auf maschinenlesbaren Datenträgern an eine zentrale Vermittlungsstelle weitergegeben werden, die dann die erforderlichen Rechenarbeiten durchführt und die Feststellungen an die Träger der Sozialhilfe zurückmeldet. Die Verfahrensdetails sind in der Sozialhilfedatenabgleichsverordnung vom 21. Januar 1998 (BGBl. S. 103) geregelt.

In ihrer Antwort (Drs. 13/3445) auf die Kleine Anfrage 1647 des Abgeordneten Franz Josef Bischel (CDU) berichtete die Landesregierung, in welchem Umfange kreisfreie Städte und Landkreise in der Zeit vom 1. Januar bis 30. Juni 1998 Sozialhilfedaten für den Abgleich übermittelten und in welchem Umfange „Feststellungen“ – dies ist beispielsweise der gleichzeitige Sozialhilfe- und Rentenbezug – zurückgemeldet wurden. Die Zahlen waren teilweise recht beeindruckend. Bei der Stadt Mainz beispielsweise führten im ersten Quartal 22 764 Abgleiche zu 5 353 Treffern, im zweiten Quartal erbrachten 18 791 Abgleiche 5 845 Treffer. Bei der Kreisverwaltung des Rhein-Lahn-Kreises führte fast jeder zweite Abgleich zu einem Treffer (637 von 1 375). Es sei, so wurde schon in der Antwort betont, in der ganz überwiegenden Mehrzahl der Fälle davon auszugehen, dass die übermittelten Daten zum Rentenbezug bzw. dem Bestehen eines Beschäftigungsverhältnisses bereits bekannt sind.

Die Fragen nach dem Umfang des mit Hilfe der Zentraldatei des VDR aufgedeckten unberechtigten oder unberechtigt hohen Sozialhilfebezugs und nach dem Umfang der Minderung von Sozialhilfezahlungen aufgrund der Abgleichsergebnisse konnten von der Landesregierung nicht beantwortet werden.

Gerade diese Ergebnisse sind aus der Sicht des Sozialdatenschutzes interessant, denn es geht auch darum, die Verhältnismäßigkeit der neu geschaffenen Eingriffsregelungen zu beurteilen. Der LfD bat deshalb die in der Antwort genannten Städte und Landkreise um ergänzende Informationen.

Eine Stadtverwaltung teilte mit, dass die Bearbeitung der Auswertungsergebnisse in den jeweiligen Einzelfällen sehr zeitaufwendig und arbeitsintensiv sei. „Aufgrund der Tatsache, dass die hierfür zuständigen Mitarbeiterinnen und Mitarbeiter auch ansonsten mehr als ausgelastet sind, können zum gegenwärtigen Zeitpunkt noch keine abschließenden Zahlen über die aus dem Datenabgleich resultierenden Reduzierungen bzw. Einstellungen von Sozialhilfeleistungen mitgeteilt werden.“ Auch in der Folgezeit war nichts Näheres zu erfahren. In zwei anderen kreisfreien Städten und in einem Landkreis waren die Feststellungen aus dem Datenabgleich (Stichtag 30. Juni 1998) zum Berichtszeitpunkt (Dezember 1998 oder Januar 1999) ebenfalls noch nicht ausgewertet. Eine kreisfreie Stadt berichtete, dass Sozialhilfeleistungen in 35 Fällen gekürzt und in zwölf Fällen eingestellt wurden. Eine andere Stadt berichtete über die Kürzung der Sozialhilfeleistungen in zwölf Fällen und die Einstellung in sechs Fällen. In einem Fall führten die aus dem Abgleich gewonnenen Informationen zu einer Strafanzeige wegen Sozialhilfebetrugs (Schadenshöhe ca. 80 000,– DM).

Aus der Stadt Frankfurt/M. wurde bekannt, dass 626 Fälle unberechtigten Sozialhilfebezugs aufgrund 8 495 positiver Antwortsätze ermittelt wurden. Der Schaden wird auf 1,45 Mio. DM beziffert; dies sind 0,2 v. H. der Gesamtsumme der gesamten Sozialhilfeleistungen bzw. 0,4 v. H. der reinen HLU-Jahresausgaben (27. Tb. des Hess. DSB, Tz. 14.1).

Es ist sicherlich noch zu früh, die Gesetzesänderung und ihre Folgen aufgrund dieser Ergebnisse unter dem Blickwinkel der Verhältnismäßigkeit zu beurteilen. Der LfD bleibt weiter bemüht, an verlässliche Informationen zu gelangen. Eindeutig unzulässig, weil zur Aufgabenerfüllung nicht erforderlich, ist es jedenfalls, Datenabgleiche durchzuführen, die dann nicht ausgewertet werden. Der Abgleich ist ein Informationseingriff, der auch dann, wenn er gesetzlich zugelassen ist, den Anforderungen an die Zweck-Mittel-Relation entsprechen muss.

11.2.6.2 Sozialhilfedatenabgleich nach § 117 Abs. 3 BSHG mit der Kfz-Zulassungsstelle

Zum Zwecke der Missbrauchsverhütung wurde auch zugelassen, dass regelmäßig im Wege des automatisierten Datenabgleichs zwischen den Sozialämtern und den Kraftfahrzeugzulassungsstellen überprüft wird, ob Kraftfahrzeuge auf Sozialhilfeempfänger zugelassen sind. Die Zulassungsstelle darf dem Sozialamt lediglich die „Eigenschaft als Kraftfahrzeughalter“ von Personen mitteilen, die in dem Abgleichdatenbestand enthalten sind; die Übermittlung weiterer Merkmale ist unzulässig.

Die Kenntnis der Haltereigenschaft ist für das Sozialamt deshalb wichtig, weil der Kraftfahrzeugbesitz grundsätzlich als Indiz für fehlende Hilfebedürftigkeit angesehen wird. Liegt die Information über den Kraftfahrzeugbesitz vor, sind nähere Feststellungen unter Mitwirkung des Hilfe Suchenden oder Hilfeempfängers zu treffen. Diese haben insoweit Mitwirkungspflichten, die sich aus §§ 60 ff. SGB I ergeben.

Eine Stadtverwaltung fragte beim LfD an, ob es zulässig sei, dass für die Sachbearbeiter des Sozialamtes auch ein Online-Zugriff auf die Kraftfahrzeughalterdatei eingerichtet wird. Dies wurde zunächst insbesondere deshalb verneint, weil sich dieser Online-Zugriff auf alle Halterdaten und nicht nur auf die „Eigenschaft als Kraftfahrzeughalter" erstrecken sollte. Diese Einschränkung folgt aus dem Gesetzeswortlaut, der völlig eindeutig ist und keine extensive Auslegung zulässt.

Die ablehnende Stellungnahme des LfD stieß auf Unverständnis. Es sei erforderlich, so wurde argumentiert, den Zugriff auf Angaben über den Kfz-Hersteller, den Typ und das Baujahr auszudehnen, weil nur aufgrund dieser Angaben beurteilt werden könne, ob Sozialhilfemittel unwirtschaftlich verwendet würden. Der Sozialdatenschutz, der einen solchen umfassenden Zugriff nicht zulasse, behindere in einer unvertretbaren Weise die Aufklärung von Betrugsfällen.

Interessant ist die Vorgeschichte des Falles. Das Sozialamt und die Zulassungsstelle hatten bereits einen Datenabgleich durchgeführt, der ein überraschendes Ergebnis zeitigte: Auf rund 4 000 Sozialhilfeempfänger waren nicht weniger als 1 500 Kraftfahrzeuge zugelassen – in einem Falle sechs Pkw –.

Bei vordergründiger Betrachtung lässt sich mit solchen Zahlen sicherlich belegen, wie wichtig der Datenabgleich nach § 117 Abs. 3 BSHG ist. Bei genauerem Hinsehen wird aber deutlich, dass die Unkenntnis des Sozialamtes über sozialhilferelevante Sachverhalte wohl zuvörderst andere Ursachen hat. Auch in der Vergangenheit – vor der Änderung des § 117 BSHG – war kein Sozialhilfesachbearbeiter gehindert, immer dann, wenn er dies in konkreten Fällen für angezeigt hielt, bei der Kraftfahrzeugzulassungsstelle nachzufragen, ob ein Antragsteller oder Leistungsempfänger ein Kraftfahrzeug besitzt. Die damit verbundene Übermittlung von Sozialdaten war im erforderlichen Umfang durch § 69 Abs. 1 Nr. 1 SGB X gedeckt und auch die Zulassungsstelle war auskunftsbefugt. Die Vermutung, dass die von der Stadtverwaltung selbst als erschreckend bezeichneten Ergebnisse des Abgleichs ihre Ursache wohl eher in einer mangelhaften Sachbearbeitung haben, ist nahe liegend. Vielleicht ist das Personal überlastet, vielleicht liegt es auch an der Qualität der Sachbearbeitung. Mit Behinderungen durch den Sozialdatenschutz hat dies jedenfalls nichts zu tun.

Im konkreten Falle war darauf hinzuweisen, dass der Untersuchungsgrundsatz (§ 20 SGB X) durch § 117 Abs. 3 BSHG unberührt bleibt. Beim Vorliegen der Voraussetzungen des § 67 a SGB X darf der Sozialleistungsträger Sozialdaten erheben. Der LfD hält es für datenschutzrechtlich zulässig, dass die Eigenschaft als Fahrzeughalter durch einen Direktzugriff (Online-Zugriff) auf die Fahrzeug-Bestandsdaten ermittelt wird. Weitere Halterdaten dürfen nicht abrufbar sein. Die Zugriffsmöglichkeit muss auf Sachbearbeiter beschränkt bleiben, die die Information regelmäßig benötigen und es ist geboten, dass die Zugriffe für das Sozialamt – und nur für dieses – protokolliert und durch den Leiter regelmäßig überprüft werden. Es muss ausgeschlossen sein, dass die Zulassungsstelle feststellen kann, in welchen Fällen auf die Halterdatei zugegriffen wurde. Für Abrechnungszwecke darf von dieser nur die Zahl der Zugriffe erfasst werden.

11.2.6.3 Sozialhilfeermittler

Nicht selten werden in den Medien Fälle des Sozialleistungsmissbrauchs in ihrem Spannungsverhältnis zum Sozialdatenschutz dargestellt. Es wird beklagt, dass den Sozialleistungsträgern nicht genügend Ermittlungsbefugnisse zur Verfügung stünden, um Betrügereien der Sozialleistungsempfänger aufzudecken. Schuld sei der Datenschutz, der die Ermittlungstätigkeit in unvertretbarer Weise behindere.

Die Datenschutzbeauftragten können in dieser Situation nichts weiter tun, als die Gesetzeslage erläutern und deutlich machen, wie Sozialhilfeermittler bei ihrer Arbeit vorgehen müssen, um nicht mit dem Datenschutz in Konflikt zu geraten.

Der LfD vertritt in enger Anlehnung an die vom Bayerischen Landesbeauftragten für den Datenschutz entwickelten Grundsätze für den Einsatz von Außendienstmitarbeitern der Sozialhilfeträger folgende Rechtsauffassung:

a) Der Einsatz von Sozialhilfeermittlern zur Prüfung, ob die gesetzlichen Voraussetzungen des Leistungsbezuges gegeben sind, ist zulässig, soweit diese Art der Datenerhebung erforderlich und verhältnismäßig ist.

   Gemäß § 37 Satz 3 SGB I geht das Zweite Kapitel des SGB X (Sozialdatenschutz) dessen Erstem Kapitel (Verwaltungsverfahren) vor, soweit sich die Ermittlung des Sachverhalts nach den §§ 20 und 21 SGB X auf Sozialdaten erstreckt. Die Grenzen der Datenerhebung bestimmen sich deshalb nach § 67 a SGB X.

b) Die Verhältnismäßigkeit dieses Einsatzes ist sowohl im Vergleich zu weniger beeinträchtigenden Ermittlungsmöglichkeiten als auch ggf. hinsichtlich des Gewichts vorliegender Verdachtsmomente auf Sozialhilfemissbrauch zu überprüfen.

c) Unter dem Gesichtspunkt der Verhältnismäßigkeit kommen als weniger eingreifend vorrangig andere Ermittlungsmöglichkeiten, wie z. B. die schriftliche Befragung des Betroffenen, dessen Einbestellung ins Amt oder die in § 117 BSHG vorgesehenen Datenabgleiche in Betracht.

   Sozialhilfeermittler sollten jedenfalls nur mit genau definiertem Auftrag und regelmäßig nur gegenüber Betroffenen eingesetzt werden. Voraussetzung für die Maßnahmen sind konkrete Erhebungsanlässe, insbesondere konkrete Anhaltspunkte für Sozialhilfemissbrauch; für einen Ermittlereinsatz zur Verdachtsfindung fehlt es am Kriterium der Erforderlichkeit gegenüber dem Betroffenen.

d) Bei der Befragung haben die Ermittler dem Betroffenen die erforderlichen Informationen zu geben über Name und Dienststelle des Ermittlers, den Zweck seines Besuches sowie die Angaben, inwieweit der Betroffene zu Auskünften verpflichtet ist (ggf. nach welcher Vorschrift) oder seine Angaben freiwillig sind; im Falle der Auskunftspflicht ist er auf die Folgen der Verweigerung hinzuweisen (vgl. § 67 Abs. 3 SGB X).

   Sozialhilfeermittler dürfen keinen Zutritt zur Wohnung des Betroffenen erzwingen oder mit falschen Angaben (Vorwänden) erreichen. Der Ermittler muss im Hinblick auf Art. 13 GG (Unverletzlichkeit der Wohnung) klarstellen, dass der Betroffene nicht verpflichtet ist, ihm Zutritt zur Wohnung zu gestatten. Leistungsversagung oder Leistungsentzug nach § 66 SGB I dürfen bei Zutrittsverweigerung allenfalls dann angedroht bzw. realisiert werden, wenn die erforderliche Sachverhaltsermittlung ohne Zutritt zur Wohnung nicht durchführbar ist. Dies bedarf sorgfältiger Überprüfung.

e) Bei dritten Personen oder Stellen dürfen die Sozialhilfeermittler Daten über den Betroffenen nur nach Maßgabe der in § 67 a Abs. 2 Satz 2 Nr. 2 SGB X genannten Voraussetzungen erheben. Dabei haben sie insbesondere die Verhältnismäßigkeit dieser Form der Datenerhebung, die ohne Mitwirkung des Betroffenen erfolgt, zu prüfen.

   Im Falle des § 67 a Abs. 2 Satz 2 Nr. 2 b SGB X dürfen auch keine Anhaltspunkte dafür bestehen, dass überwiegende schutzwürdige Interessen des Betroffenen beeinträchtigt werden; dies kann z. B. der Fall sein, wenn die Befragten durch Tatsache, Art und Inhalt der Ermittlungen über den Kontakt des Betroffenen zum Sozialamt bzw. über gegen ihn bestehende Verdachtsmomente unkorrekten Verhaltens Kenntnis erlangen.

   Dieser gesetzlichen Regelung liegt die Überlegung zu Grunde, dass Datenerhebungen in Sozialleistungs-/Sozialhilfeangelegenheiten bei Dritten ohne Kenntnis des Betroffenen erhebliche Eingriffe in das Recht auf informationelle Selbstbestimmung bewirken. Deswegen müssen die genannten Voraussetzungen dieser Ausnahmebestimmung genau geprüft werden. Datenerhebung bei Dritten darf nicht zum Regelfall werden.

   Eine Datenerhebung aus allgemein zugänglichen Quellen – wie z. B. durch Ablesen von Klingel-Schildern an der Haustüre, durch Adressbuch- oder Telefonbuch-Recherchen – stellt keine Datenerhebung bei „anderen Personen oder Stellen“ dar.

f) Gegen eine verdeckte Beobachtung („Beschattung“) durch Sozialhilfeermittler bestehen größte Bedenken. Das gilt lediglich nicht für Ausnahmefälle kurzfristiger Beobachtung – etwa ob der Betroffene zur Arbeit geht –, wenn ein konkreter, auf Tatsachen begründeter Verdacht besteht und alle anderen Erkenntnismittel nicht zum Ziel führen.

   Eine derartige, auf engste Ausnahmefälle beschränkte kurzfristige Beobachtung unter Berücksichtigung des konkreten Tatverdachts und der Schwere des zur Last gelegten Delikts sollte jedenfalls schriftlich und durch den Leiter des Sozialamtes selbst angeordnet werden, ebenso ihr zeitlicher Umfang und die enge Begrenzung des Erhebungsauftrages.

g) In allen Fällen des Einsatzes von Sozialhilfeermittlern ist eine Notiz über Anlass und Zweck des Einsatzes, über die Vorlage des Dienstausweises gegenüber Betroffenen und über ihnen erteilte Belehrungen sowie über Verlauf und Ergebnis des Einsatzes notwendig, die zur Sozialhilfe-Akte zu nehmen ist. Diese Verfahrensweise ermöglicht die Erteilung von Auskünften an die Betroffenen nach § 83 SGB X, die Aufsichtsführung durch die Sozialhilfeverwaltung sowie die Datenschutzkontrolle dieser Erhebungen.

11.2.7 Rechnungsprüfung und Begleichung ambulanter und stationärer Krankenhilfeaufwendungen

Ein Dienstleitungsunternehmen bot den kreisfreien Städten in Rheinland-Pfalz an, Aufgaben der Rechnungsprüfung nach §§ 37 ff. BSHG, § 3 AsylbLG, § 276 LAG sowie § 26b BVG für sie zu übernehmen und bei der Zahlbarmachung von Leistungen für sie tätig zu werden. Die Rechnungsprüfung könne sich auf die Leistungsabrechnung der gesamten Krankenhilfe erstrecken. Als Zusatzleistung wurde die Kontoführung sowie die Archivierung zahlungsbegründender Unterlagen angeboten.

Der LfD vertritt die Auffassung, dass eine solche Aufgabenübertragung nach den Vorschriften des Sozialgesetzbuchs nicht zulässig ist. Da die Dienstleistung nicht auf manuelle oder technische Hilfs- und Unterstützungsleistungen beschränkt ist, sind die Vorschriften über die Datenverarbeitung im Auftrag (§ 80 SGB X) nicht anwendbar. Die Prüfung der sachlichen Richtigkeit von Abrechnungen der Leistungserbringer und die Abrechnung unter Berücksichtigung von Rechnungskorrekturen sind als Funktionsübertragungen zu qualifizieren. Da es sich bei den Leistungserbringern im Gesundheitsbereich um Ärzte und andere in § 203 Abs. 1 und 3 StGB genannte Personen handelt, sind die besonderen Verarbeitungsrestriktionen des § 76 SGB X zu berücksichtigen. Es fehlt an einer Rechtsgrundlage für die Datenübermittlung an das Unternehmen zur Erbringung der angebotenen Leistungen.

Es sind freilich Modifikationen der Leistungserbringung denkbar, die es zulassen könnten, der datenschutzrechtlichen Beurteilung ein Auftragsverhältnis i. S. von § 80 SGB X zugrunde zu legen. Der LfD ist insoweit gesprächsbereit.

11.2.8 Datenübermittlung im Rahmen der Kostenerstattung bei Umzug (§ 107 BSHG)

Nach § 107 BSHG besteht eine auf die Zeitdauer von zwei Jahren begrenzte Kostenerstattungspflicht des Trägers der Sozialhilfe des bisherigen Aufenthaltsorts, wenn eine Person vom Ort ihres bisherigen gewöhnlichen Aufenthalts verzieht und innerhalb eines Monats nach dem Aufenthaltswechsel der Hilfe bedarf. Selbstverständlich hat dieser kostenerstattungspflichtige Sozial-

hilfeträger ein Interesse daran, dass der nunmehr zuständige örtliche Träger Leistungen nur im wirklich erforderlichen Umfange erbringt. Streit entsteht beispielsweise dann, wenn der zuständig gewordene Sozialhilfeträger auf Kosten des früher zuständigen ohne Rücksicht auf die Geeignetheit des Hilfeempfängers Arbeitsmarkt-Qualifizierungsmaßnahmen mit dem Ziel durchführt, Leistungsansprüche gegenüber der Bundesanstalt für Arbeit zu begründen. Es stellt sich die Frage, ob die Leistungsakten zum Zwecke der Prüfung von Anspruchsvoraussetzungen an den erstattungspflichtigen Sozialhilfeträger herauszugeben sind.

Der Hilfe gewährende Sozialhilfeträger hat die Pflicht, alle nach Lage des Einzelfalles zumutbaren und möglichen Maßnahmen und Vorkehrungen zu treffen, die erforderlich sind, um die erstattungsfähigen Kosten möglichst niedrig zu halten. Es besteht eine Sorgfaltspflicht des zur Leistung verpflichteten Sozialhilfeträgers, den aktuellen Fall in sozialhilferechtlich einwandfreier und ordnungsgemäßer Weise zu bearbeiten. Der erstattungspflichtige Sozialhilfeträger muss in die Lage versetzt werden, im Rahmen seiner schon aus den allgemeinen Verwaltungsgrundsätzen herzuleitenden materiell-rechtlichen und rechnerischen Überprüfungspflicht die Grundlagen und Gründe, die den erstattungsberechtigten Träger zu seiner Entscheidung über die Hilfegewährung veranlasst haben, nachvollziehen zu können. Die Zentrale Spruchstelle führte in einer Entscheidung vom 21. März 1996 – B 123/93 – aus, dass der erstattungsberechtigte Sozialhilfeträger auf Verlangen des erstattungspflichtigen Sozialhilfeträgers die Gründe und Grundlagen, auf denen seine Entscheidung über die Hilfegewährung beruht, darzulegen habe. Seiner Darlegungs- und Aufklärungspflicht könne der erstattungsberechtigte Träger in der Regel nur durch die Übersendung seiner entsprechenden Akten oder von auszugsweisen Kopien hiervon genügen. Die Übersendung einer Liste, in der lediglich die einzelnen Leistungen mit Summen aufgezählt sind, genüge nicht.

Der LfD stimmt mit dem Ministerium für Arbeit, Soziales und Gesundheit in der Beurteilung überein, dass die Übersendung von Akten in Fällen der beschriebenen Art nur unter den in § 69 Abs. 1 Nr. 1 SGB X genannten Voraussetzungen zulässig ist. Eingeschränkt ist die Befugnis zur Datenübermittlung damit durch den Erforderlichkeitsgrundsatz. Der zuständige Sozialhilfeträger kommt nicht umhin zu prüfen, ob wirklich der gesamte Akteninhalt für die Prüfung der Erstattungspflicht benötigt wird. Die von der Spruchstelle vorgenommenen Einschränkungen auf „entsprechende“ Akten oder „auszugsweise“ Kopien gehen in diese Richtung. Selbstverständlich dürfen dem Übermittlungsempfänger keine Informationen vorenthalten werden, die für seine Prüfung notwendig sein können. Aber auch eine routinemäßige Übersendung aller vorhandenen Akten ohne Prüfung der Erforderlichkeit kommt nicht in Betracht.

Aus der Befugnis zur Datenübermittlung folgt beim Vorliegen der Amtshilfevoraussetzungen eine Verpflichtung.

11.3 Jugendhilfe

11.3.1 Rechnungsprüfung im Jugendamt

Sozialdaten, die dem Mitarbeiter eines Jugendamtes zum Zweck persönlicher und erzieherischer Hilfe anvertraut worden sind, dürfen von diesem nur beim Vorliegen besonderer Voraussetzungen weitergegeben werden (§ 65 Abs. 1 Nr. 1 bis 3 SGB VIII). Zu diesen Voraussetzungen gehört die Einwilligung dessen, der die Daten anvertraut hat.

Unter Hinweis auf die zitierte Vorschrift verweigerten Mitarbeiter des Jugendamtes dem Rechnungsprüfungsamt den Zugang zu den geschützten Daten. Dieses wiederum verwies auf seinen gesetzlichen Prüfungsauftrag, der sich ausnahmslos auf alle Verwaltungsbereiche erstrecke.

Der LfD geht von einem uneingeschränkten Prüfungsrecht des Rechnungshofs und anderer Rechnungsprüfungsbehörden im Bereich der wirtschaftlichen Jugendhilfe aus. Das Prüfungsrecht erstreckt sich indessen nicht auf Sozialdaten, die dem besonderen Vertrauensschutz in der persönlichen und erzieherischen Hilfe nach § 65 SGB VIII unterliegen. Sofern im Sinne dieser Vorschrift „anvertraute“ Sozialdaten für sonstige Jugendhilfeleistungen anspruchsbegründend sind, dürfen sie – auch innerhalb des Jugendamtes – nur mit Zustimmung der Betroffenen weitergegeben werden. Wird die Zustimmung nicht erteilt, treten die Folgen fehlender Mitwirkung nach § 66 SGB I ein. Der besondere Vertrauensschutz nach § 65 SGB VIII erfordert die getrennte Speicherung der nach dieser Vorschrift anvertrauten Daten von sonstigen Sozialdaten des Jugendamtes (getrennte Aktenführung).

Die Rechtsauffassung des LfD wurde anerkannt; die Rechnungsprüfung wurde in dem für zulässig gehaltenen Rahmen durchgeführt.

11.3.2 Einkommensabhängige Erhebung von Elternbeiträgen für Kindertagesstätten

§ 13 Abs. 2 Kindertagesstättengesetz lässt zu, dass bei der Festsetzung des Elternbeitrages für Kindertagesstätten sowie der Ermäßigung für Mehrkindfamilien das Einkommen berücksichtigt wird. Das Bundesverfassungsgericht hat die entsprechende gesetzliche Ausgestaltung der einkommensabhängigen Erhebung der Elternbeiträge im Grundsatz zwischenzeitlich für zulässig erachtet (Az.: BvR 178/97). Gleichwohl erreichten den LfD zahlreiche Anfragen zur datenschutzrechtlichen Ausgestaltung der Erhebung der Beiträge. Denn nach den Richtlinien des Kreistages eines Landkreises war für die Berechnung der Beiträge die Summe der positiven Einkünfte im Sinne des § 2 Abs. 1 und 2 des EStG maßgeblich. Der Nachweis sollte durch die Vorlage des Steuerbescheides geführt werden.

Der LfD konnte im Wesentlichen auf ein unter seiner Beteiligung zustande gekommenes Rundschreiben des Ministeriums für Kultur, Jugend, Familie und Frauen aus dem Jahre 1995 verweisen, welches Richtlinien für die Erhebung und Festsetzung von Elternbeiträgen nach dem Kindertagesstättengesetz enthält (vgl. 15. Tb, Tz. 11.4). Die von der Kreisverwaltung verwandten Fragebögen und Informationsblätter entsprachen diesen Anforderungen nur bedingt. Beispielsweise wurde nicht auf die Möglichkeit hingewiesen, dass die für die Sachbearbeitung nicht relevanten Daten des Steuerbescheides geschwärzt werden können. Auf Veranlassung des LfD wurden die Fragebögen dem o. g. Rundschreiben entsprechend überarbeitet.

11.4 Wohngeld

11.4.1 Unaufgeforderte Datenübermittlung der Wohngeldstelle an das Sozialamt

Gegenstand einer Eingabe war die Zulässigkeit der Datenübermittlung der Wohngeldstelle einer Kreisverwaltung an das Sozialamt einer Verbandsgemeinde. Nachdem sich die Höhe des Wohngeldes geändert hatte, teilte dies die Wohngeldstelle, ohne dass hierfür eine allgemeine oder konkrete Anfrage des Sozialamtes vorgelegen hätte, diesem „zur Vermeidung von Überzahlungen und unnötigen Neuberechnungen, Rückforderungen und Geltendmachung von Erstattungsansprüchen“ mit.

Nach Auffassung des LfD war die Mitteilung über die zu erwartende Wohngeldneufestsetzung nicht erforderlich i. S. d. § 69 Abs. 1 Nr. 1 SGB X und damit unzulässig, weil zum einen das Sozialamt der Verbandsgemeinde vorliegend selbst in der Lage war, die Daten beim Betroffenen unmittelbar zu erheben (Vorrang der Ersterhebung beim Betroffenen) und der Betroffene zum anderen über seine Mitwirkungspflichten gem. § 60 Abs. 1 Nr. 2 SGB I seinerseits zu Änderungsmitteilungen verpflichtet war (vgl. VGH Baden-Württemberg, Urteil vom 1. April 1992, RDV 1993, S. 185 ff.). Anlassunabhängige Kontrollmitteilungen an andere Behörden bedürfen einer ausdrücklichen gesetzlichen Regelung, wie sie beispielsweise in § 117 BSHG enthalten ist. Diese Voraussetzungen lagen jedoch hier nicht vor.

Das Finanzministerium hat diese Rechtsauffassung bestätigt und darauf hingewiesen, dass das Sozialamt für jeden Bewilligungszeitraum die Anspruchsvoraussetzungen erneut zu prüfen habe und zu diesem Zweck Erkundigungen auch bei der Wohngeldstelle einholen könne. Dem Sozialamt diese Amtspflicht abzunehmen oder ihre Erfüllung zu erleichtern, bestehe für die Wohngeldstelle kein Anlass und vor allem keine rechtliche Befugnis.

Die Wohngeldstelle der Kreisverwaltung wird künftig entsprechend verfahren.

11.4.2 Landesweiter Datenabgleich im Wohngeldverfahren

Die Wohngeldberechnung und -zahlbarmachung erfolgt in einem landeseinheitlichen Verfahren durch das Statistische Landesamt. Dieses Verfahren soll auf eine neue technische Grundlage gestellt werden. In diesem Zusammenhang war beabsichtigt, den Wohngeldsachbearbeitern eine automatisierte Prüfung zu ermöglichen, ob ein Fall des Doppelbezugs vorliegen könnte. Vor der Vergabe einer neuen Fallnummer sollte ein Suchvorgang aktiviert werden, der sich auf alle Wohngeldzahlfälle des Landes erstreckt. Als Suchkriterien sollten der Name und das Geburtsdatum des Antragstellers dienen. Das Ergebnis der Suche sollte dem Sachbearbeiter nur die Information geben, ob und ggf. bei welcher Wohngeldstelle der Antragsteller bereits geführt wird. Die weitere Sachverhaltsaufklärung sollte dann im direkten Kontakt zwischen den Wohngeldstellen erfolgen.

Der LfD äußerte Zweifel, ob sich der geplante Abgleich von Antragsdaten mit einem zentralen Bestand aller Zahlfälle im Lande unter § 79 SGB X – Einrichtung automatisierter Abrufverfahren – subsumieren lässt. Das Problem besteht darin, dass das Verfahren die Bildung eines Datenpools voraussetzt, in dem Grunddaten über alle Leistungsfälle des Landes zusammengefasst sind. Die Recherche erfolgt unter Nutzung aller Pooldaten; dem Übermittlungsempfänger wird erst im Trefferfalle bekannt, welche Stelle Wohngeld zahlt. Ein automatisiertes Abrufverfahren i. S. von § 79 setzt indessen voraus, dass Sozialdaten im automatisierten Verfahren zwischen zwei „bestimmten“ Stellen übermittelt werden. Das Charakteristikum des automatisierten Abrufverfahrens besteht darin, dass die Datenübermittlung ohne Mitwirkung der übermittelnden Stelle erfolgt; nur diese besondere Qualität des Informationseingriffs veranlasste den Gesetzgeber, gegenüber dem Normalfall der Datenübermittlung weiter gehende inhaltliche und verfahrensmäßige Festlegungen zu treffen. Der Abruf bei einer dem Übermittlungsempfänger unbekannten speichernden Stelle bzw. gleichzeitig bei mehreren Stellen ist nicht umfasst.

Auch die Anforderung des § 79 Abs. 1 SGB X, dass das Verfahren unter Berücksichtigung der Vielzahl der Übermittlungen angemessen sein muss, bildet ein Hindernis für den Abgleich, denn auch hier können nur bestimmte verfahrensbeteiligte Stellen gemeint sein. Die „Vielzahl“ kann sich nicht auf Datenübermittlungen aus einem zentralen Datenbestand beziehen, sondern nur auf Abrufverfahren, die zwischen bestimmten Sozialleistungsträgern unter Beachtung der Anforderungen des § 79 eingerichtet wurden.

Mit dem Statistischen Landesamt wurde weiter erörtert, ob der Abgleich innerhalb des Zuständigkeitsbereichs einer Tabellenwohngeldstelle zulässig ist. Das oben beschriebene Verfahren würde danach nicht landesweit, sondern reduziert auf den Zuständigkeitsbereich eines Landkreises oder einer Stadt durchgeführt.

Obwohl der LfD nach Prüfung zu dem Ergebnis kam, dass das letztere Verfahren von den geltenden datenschutzrechtlichen Vorschriften gedeckt wäre, verzichtete das Statistische Landesamt schließlich vollständig auf einen maschinellen Datenabgleich.

11.5 Krankenkassen, Kassenärztliche Vereinigungen

11.5.1 Eingeschränkter Zugriff auf Versichertendaten bei landesweiten oder überregionalen gesetzlichen Krankenkassen

Im 15. Tb., Tz. 11.1.2, berichtete der LfD über Probleme, die durch den Zusammenschluss von zuvor selbständigen gesetzlichen Krankenkassen entstanden. Die Kassen bieten ihren Mitgliedern nach dem Zusammenschluss die Möglichkeit, Versichertenangelegenheiten bei jeder Geschäftsstelle (Regionaldirektion) bearbeiten zu lassen. Zu diesem Zweck wurden die technischen Voraussetzungen geschaffen, dass jede dieser Stellen auf die zentral gespeicherten oder im Datenverbund verfügbaren Versichertendaten zugreifen kann.

Die Thematik war wegen ihrer grundsätzlichen Bedeutung Beratungsgegenstand in der 49. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 9. und 10. März 1995. Die bei dieser Sitzung gefasste Entschließung enthielt folgende Forderungen:

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

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

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

Soweit bekannt, hat keine gesetzliche Kasse mit überregionalen Zuständigkeiten diese Forderungen umgesetzt.

Der LfD erkennt das Bestreben der Kassen nach Kundennähe und umfassender Versichertenbetreuung grundsätzlich an. Gegen uneingeschränkte Zugriffsmöglichkeiten auf Versichertendaten bei landesweiten oder überregionalen Krankenkassen im Rahmen der in einer Geschäftsstelle üblichen Zugriffsbeschränkungen nach Sachaufgaben bestehen keine Bedenken, wenn dies dem Willen des Versicherten entspricht. Es dürfen aber gegen den Willen des Versicherten landesweite bzw. überregionale Datenzugriffe durch „fremde" Geschäftsstellen nicht realisierbar sein. Es reicht nicht aus, vom Willen des Versicherten nicht getragene Zugriffsmöglichkeiten etwa durch Dienstanweisungen zu untersagen, vielmehr müssen unzulässige Datenzugriffe technisch unterbunden werden.

Die Thematik wird nun bereits seit fünf Jahren ergebnislos erörtert. Dabei zeigen die landesweit tätigen Kassen durchaus Verständnis für das Anliegen der Datenschutzbeauftragten. Zugleich wird aber auf die jeweiligen Bundesverbände verwiesen, die den Kassen technische Unterstützung leisten und die eine im Sinne der Datenschutzbeauftragten abgestufte Zugriffsberechtigung für schwer umsetzbar halten.

Der LfD bemüht sich weiterhin um eine datenschutzverträgliche Lösung.

11.5.2 Anforderung von Behandlungsunterlagen durch Krankenkassen

Im Berichtszeitraum ging es wiederholt um Rechtsfragen bei der Anforderung medizinischer Unterlagen gegenüber Leistungserbringern durch Krankenkassen.

In einem Fall vertrat eine KV die Ansicht, dass die Krankenkasse nicht berechtigt sei, bei einem ihrer Mitglieder sämtliche Behandlungsunterlagen im Zusammenhang mit der Geltendmachung eines Schadensersatzanspruchs des Versicherten anzufordern.

Der LfD vertrat hingegen die Auffassung, dass bei Schadensersatzansprüchen, die gem. § 116 SGB V auf die Krankenkasse übergegangen sind, § 284 Abs. 1 Nr. 4 SGB V einschlägig ist. Die Krankenkasse kann hiernach Sozialdaten erheben, soweit diese für die Gewährung von Leistungen an Versicherte erforderlich sind. Unter den in diesem Zusammenhang weit auszulegenden Begriff der Leistungsgewährung fällt als Annex auch die Geltendmachung von Regressansprüchen (Hauck/Haines, Kommentar zum SGB V, K § 284, RdNr. 9).

Soweit Schadensersatzansprüche, die bei der Inanspruchnahme von Versicherungsleistungen entstanden sind, nicht gem. § 116 SGB X auf die Krankenkasse übergehen, ergibt sich die Datenerhebungsbefugnis der Krankenkasse unmittelbar aus § 284 Abs. 1 Nr. 5 SGB V, wonach die Krankenkasse Sozialdaten erheben darf, soweit diese für die Unterstützung der Versicherten bei Behandlungsfehlern (§ 66 SGB V) erforderlich sind.

Da der Versicherte schriftlich in die Weitergabe seiner Unterlagen eingewilligt hatte, bestanden auch im Hinblick auf die ärztliche Schweigepflicht gegen die Weiterleitung der Unterlagen an die Krankenkasse keine datenschutzrechtlichen Bedenken (vgl. § 100 SGB X).

Anders verhält es sich jedoch, wenn die Krankenkasse im Zusammenhang mit der Einschaltung des MDK bei Ärzten oder Krankenhäusern Behandlungsunterlagen anfordert.

Zur diesbezüglichen Datenerhebungsbefugnis der Krankenkassen hat der LfD im 15. Tb. (Tz. 11.1.1) bereits darauf hingewiesen, dass § 276 Abs. 2 SGB V, wonach Sozialdaten auf Anforderung des MDK unmittelbar an diesen zu übermitteln sind, selbst bei Vorliegen einer Einwilligungserklärung des Versicherten grundsätzlich keinen Raum für die Übermittlung von Behandlungsunterlagen an die Krankenkasse lässt.

Die Krankenkasse darf nur insoweit medizinische Daten bei den Leistungserbringern erheben, als dies für die Prüfung der Erforderlichkeit einer Begutachtung durch den MDK wegen der Art, Schwere, Dauer oder Häufigkeit der Erkrankung oder wegen des Krankheitsverlaufs erforderlich ist (§§ 284 Abs. 1 Nr. 7 i. V. m. 275 Abs. 1 S. 1 SGB V). Hiervon nicht erfasst ist beispielsweise die Erhebung von Arztbriefen, Facharzt- und Krankenhausberichten, Befundberichten, ärztlichen Gutachten etc.

Das Landessozialgericht Mainz vertritt in diesem Zusammenhang die Auffassung, dass die Krankenkasse bereits für diese Vorprüfung den MDK einzuschalten habe (Beschluss vom 11. September 1995, Az.: L 5 EA-K-21/95). Die Anforderung von Behandlungsunterlagen bei den Leistungserbringern komme erst dann in Betracht, wenn die Untersuchungen des MDK die vorhandenen Zweifel haben fortbestehen lassen.

Die Krankenkassen sehen ihre Rechtsauffassung indes in einem Urteil des LSG Baden-Württemberg (MedR 1997, S. 331) bestätigt, wonach § 276 Abs. 2 SGB V den eigenen direkten Datenherausgabeanspruch der Krankenkassen nicht beschränke.

Nach der Auffassung des LfD verkennt diese Rechtsprechung, dass es auf Seiten der Leistungserbringer grundsätzlich an einer gesetzlichen Offenbarungsbefugnis im Sinne des § 203 Abs. 1 StGB zur Übermittlung medizinischer Daten fehlt. Der LfD sieht sich daher nicht veranlasst, seinen bisher vertretenen Standpunkt zu revidieren.

11.5.3 Auskünfte an Versicherte

§ 305 Abs. 2 SGB V bestimmt, dass die an der vertragsärztlichen Versorgung teilnehmenden Ärzte und ärztlich geleitete Einrichtungen die Versicherten schriftlich über die zu Lasten der Krankenkassen zu zahlenden Entgelte innerhalb von vier Wochen nach Ablauf des Quartals, in dem die Leistungen in Anspruch genommen worden sind, unterrichten. Das Nähere, so der Gesetzestext, regeln die Vertragspartner nach § 82 SGB V in den Bundesmantelverträgen.

Weil es bislang nicht zum Abschluss von Verträgen gekommen ist, konnte diese datenschutzfreundliche Regelung noch nicht umgesetzt werden. Die Kassenärztlichen Vereinigungen im Zuständigkeitsbereich des LfD haben erklärt, dass eine Unterrichtung der Versicherten ohne die Vereinbarung fester Punktwerte im Sinne des § 85 SGB V nicht möglich und im Übrigen mit zu hohen Kosten verbunden sei. Die Krankenkassen haben einen Zusammenhang mit § 85 bestritten und darauf hingewiesen, dass eine Information der Patienten auch anhand des letzten bekannten Abrechnungspunktwertes möglich sei.

Der Versicherte kann sich zwar über die in Anspruch genommenen Leistungen bei seiner Krankenkasse gem. § 305 Abs. 1 SGB V informieren, dies setzt jedoch ein aktives Handeln des Versicherten voraus, die durch die Regelung in Absatz 2 gerade ausgeschlossen sein sollte.

Der LfD wird sich zusammen mit den Datenschutzbeauftragten des Bundes und der Länder mit Nachdruck für eine Umsetzung der gesetzlichen Unterrichtungspflicht einsetzen.

11.5.4 Briefzustellung durch Privatunternehmen

Eine der Kontrollzuständigkeit des LfD unterliegende Krankenkasse fragte an, ob es zulässig sei, einen privaten Dienstleister für die Zustellung von Briefen und anderen Sendungen in einem bestimmten Postleitzahlenbereich in Anspruch zu nehmen. Aufgrund des von dem Unternehmen vorgelegten Angebots konnte davon ausgegangen werden, dass erhebliche Einsparungen zu erzielen sind.

Unter datenschutzrechtlichen Gesichtspunkten ist die Zustellung von Dokumenten- und Warensendungen durch ein Privatunternehmen als eine Datennutzung im Rahmen eines Auftragsverhältnisses durch eine nichtöffentliche Stelle anzusehen, die beim Vorliegen der Voraussetzungen des § 80 SGB X grundsätzlich zulässig ist. Es gehört freilich zu den Pflichten der Kasse als Auftraggeber, sich Gewissheit darüber zu verschaffen, dass es sich beim Auftragnehmer um ein zuverlässiges Unternehmen handelt, das den Auftrag mit der gebotenen Sorgfalt und unter Beachtung der Anforderungen an den technisch-organisatorischen Datenschutz ausführt. Für die Beurteilung der Zuverlässigkeit ist es z. B. von Bedeutung, ob die Vorschriften des Postgesetzes bezüglich der Lizenzierung beachtet werden.

Der LfD bot seine weitere Beratung für den Fall an, dass die Kasse in Verhandlungen über die Durchführung des Auftrags eintritt. Soweit bekannt, kam die Zusammenarbeit zwischen der Kasse und dem Unternehmen aber aus Gründen, die mit dem Datenschutz nichts zu tun haben, nicht zustande.

11.5.5 Datenschutzprobleme bei der Umsetzung des Psychotherapeutengesetzes

Am 1. Januar 1998 ist das Psychotherapeutengesetz in Kraft getreten. In den Übergangsbestimmungen wird u. a. geregelt, unter welchen Voraussetzungen die Approbation bzw. die Kassenzulassung zu erteilen ist. Erforderlich sind insoweit Nachweise insbesondere über die bisherige Berufstätigkeit (Bsp.: 4 000 Stunden umfassende psychotherapeutische Berufstätigkeit, Durchführung bestimmter Therapieverfahren) sowie die Vorlage der Approbationsurkunde bei den Kassenärztlichen Vereinigungen bis zum 31. März 1999.

Somit konnte nicht ausgeschlossen werden, dass im Rahmen des Nachweisverfahrens sensible Patientendaten gegenüber der Approbationsbehörde bzw. den Zulassungsausschüssen offenbart werden. Da die Regelungen des Psychotherapeutengesetzes nach Auffassung der Landesbeauftragten für den Datenschutz jedoch keine gesetzlichen Offenbarungsbefugnisse im Sinne des § 203 StGB darstellen, hat die 56. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 5./6. Oktober 1998 folgenden Beschluss gefasst:

> „Die Ministerien werden aufgefordert, ein datenschutzgerechtes Verfahren zu entwickeln, das die Nachweise unter Wahrung der Schweigepflicht ermöglicht. So hat das BMG mit Schreiben vom 10. August 1998 an den Bundesbeauftragten für den Datenschutz ausgeführt, dass die Nachweise möglichst mit Fremdbelegen zu führen sind. Dies sind z. B. Bestätigungen, die von den gesetzlichen Krankenkassen, den privaten Krankenversicherungen und den Beihilfestellen ausgestellt werden. Wo dies nicht möglich ist, dürfen nur Nachweise mit anonymisierten Daten verlangt werden. Die Nachweispflichtigen können verpflichtet werden, die personenbezogenen Unterlagen für einen bestimmten Zeitraum vorzuhalten."

Das Ministerium für Arbeit, Soziales und Gesundheit stimmte in der Beurteilung der Rechtslage hiermit weitgehend überein und hat die Entwicklung eines einfachen Verschlüsselungsverfahrens für solche Fälle empfohlen, in denen die Bewerber auf den Nachweis selbstzahlender Patienten angewiesen sind. Darüber hinaus konnte durch die Verwendung eines speziell entwickelten Vordrucksatzes eine personenbezogene Übermittlung an die zuständigen Stellen vermieden werden.

Der LfD hat sich sowohl beim Landesamt für Soziales, Jugend und Versorgung als zuständige Approbationsbehörde als auch bei den für das Zulassungsverfahren zuständigen Kassenärztlichen Vereinigungen durch örtliche Feststellungen von der weitgehend datenschutzgerechten Ausgestaltung des Nachweisverfahrens überzeugt.

11.6 Dialogverfahren der Rentenversicherungsträger

Im 16. Tb. (Tz. 11.3) wurde über das Verfahren einschließlich der nach Auffassung des LfD erforderlichen technischen und organisatorischen Sicherungsmaßnahmen bereits berichtet. Das Verfahren ermöglicht eine Versichertenberatung auch durch unzuständige Rentenversicherungsträger, da von der kontoführenden Versicherungsanstalt die Daten bundesweit zum Abruf durch andere Rentenversicherungsträger zur Verfügung stehen. Aus datenschutzrechtlicher Sicht ist die Einrichtung solcher Verfahren nicht unproblematisch:

Die Mitarbeiter der Rentenversicherungsträger, die in den Auskunfts- und Beratungsstellen tätig sind, erhalten einen bundesweiten Zugriff auf die ca. 50 Millionen Versichertenkonten und damit eine Abfrageberechtigung für solche sensible Sozialdaten, wie z. B. Krankheits- und Arbeitslosigkeitszeiten, Rentenpfändungen, Zeiten verminderter Erwerbstätigkeit, Freiheitsentziehungszeiten. Mit der steigenden Zahl zugriffsberechtigter Personen steigt jedoch zwangsläufig auch die Gefahr einer missbräuchlichen Verwendung. So ist nach Auskunft der LVA Rheinland-Pfalz die Zahl der telefonischen Ausspähversuche, bei denen sich Anrufer als Mitarbeiter eines Sozialamtes oder einer Krankenversicherung ausgeben, um an geschützte Sozialdaten zu gelangen, in letzter Zeit deutlich angestiegen.

Zweifellos konnten bei der Umsetzung des Verfahrens auch bei der LVA Rheinland-Pfalz zahlreiche datenschutzrechtlichen Verbesserungen erreicht werden. So ist beispielsweise ein Zugriff ausschließlich für Beratungszwecke bei persönlicher Vorsprache des Versicherten zulässig; die Identität des Antragstellers ist anhand eines Lichtbildes zu überprüfen; jeder Online-Zugriff wird lückenlos protokolliert.

Gleichwohl wurde eine zentrale Datenschutzforderung, nämlich die Teilnahme am Verfahren vom Willen des Versicherten abhängig zu machen, nur halbherzig umgesetzt: Die Versicherten haben zwar das Recht, der Teilnahme zu widersprechen, werden hierüber jedoch nicht unterrichtet. Leider hat die LVA Rheinland-Pfalz in Übereinstimmung mit anderen Rentenversicherungsträgern den Aufwand und die Kosten gescheut, die Versicherten über diese Widerspruchsmöglichkeit zu informieren. Somit dürften nahezu sämtliche bei der LVA Rheinland-Pfalz Versicherten – ohne dies zu wissen – an dem Verfahren teilnehmen, einschließlich solcher, die diesen Service niemals in Anspruch nehmen oder auf eine Teilnahme gar keinen Wert legen. Der Nutzen des Verfahrens für die Versicherten steht, aus der Sicht des Datenschutzes betrachtet, in keinem angemessenen Verhältnis zu den Risiken einer unzulässigen Verwendung der Sozialdaten. Wenn schon die technische Möglichkeit besteht, die Online-Übermittlung der Daten in Widerspruchsfällen zu berücksichtigen, sollten die Versicherten auch hierauf hingewiesen werden. Der LfD wird sich im Rahmen seiner Möglichkeiten weiter um eine Unterrichtung der Versicherten bemühen.

11.7 Datenerhebung und -verwendung bei der Kontrolle von Heimen

Aus konkretem Anlass hatte der LfD die Frage zu beurteilen, ob die Vorlage der aktuellen, vollständigen Pflegedokumentation an die Verbände der Pflegekassen – evtl. unter weiterer Beteiligung des Medizinischen Dienstes der Krankenkassen und der Heimaufsicht – sowie eine gemeinsame Heimbegehung und Einsicht in Akten und Unterlagen zulässig ist.

Die Spitzenverbände der Pflegekassen haben nach § 35 SGB I das Sozialgeheimnis und damit die Vorschriften des SGB X zum Sozialdatenschutz zu beachten. Bei der Datenerhebung sind sie nach § 67 a SGB X an den Erforderlichkeitsgrundsatz gebunden. Die Aufgabe, zu deren Erfüllung die Verbände der Pflegekassen im konkreten Falle Daten erheben wollen, hat ihre Rechtsgrundlage in § 80 SGB XI. Danach sind Maßnahmen der Qualitätssicherung durchzuführen.

Die zugelassenen Pflegeeinrichtungen sind verpflichtet, sich an Maßnahmen der Qualitätssicherung zu beteiligen. Sie haben auf Verlangen der Landesverbände der Pflegekassen dem Medizinischen Dienst der Krankenversicherung oder den von den Landesverbänden bestellten Sachverständigen die Prüfung der Qualität ihrer Leistungen durch Einzelprüfungen, Stichproben und vergleichende Prüfungen zu ermöglichen. Die Prüfungen sind auf die Qualität der Pflege, der Versorgungsabläufe und der Pflegeergebnisse zu erstrecken (§ 80 Abs. 2 SGB XI). Nach Auffassung des LfD ist es nicht unverhältnismäßig, eine vorhandene Pflegedokumentation in Qualitätssicherungsmaßnahmen nach § 80 einzubeziehen. Bestellte Sachverständige und der Medizinische Dienst dürfen also insoweit personenbezogene Daten erheben.

Es gehört zu den Aufgaben von Pflegeeinrichtungen, Pflegeleistungen ordnungsmäßig zu dokumentieren. Dem Arztgeheimnis würden die Pflegedokumentationen nur dann unterliegen, wenn diese fremde Geheimnisse enthielten, die einem Arzt, dem Angehörigen eines anderen Heilberufs oder einem berufsmäßig tätigen Gehilfen anvertraut worden oder sonst bekannt geworden sind (§ 203 Abs. 1 und Abs. 3 StGB). Die Mitarbeiterinnen und Mitarbeiter im Pflegedienst eines Heimes gehören nicht zu diesem Personenkreis; eine ausdrückliche, das Berufsgeheimnis nach § 203 StGB durchbrechende Befugnis ist also nicht Voraussetzung für die Datenübermittlung an die o. a. Einrichtungen. Je nach der Trägerschaft der Pflegeeinrichtung kann die Zulässigkeit der Datenübermittlung aber vom Vorliegen anderer gesetzlicher Voraussetzungen abhängen. Bei Einrichtungen in kirchlicher Trägerschaft ist kirchliches Datenschutzrecht zu beachten; bei Einrichtungen in freigemeinnütziger oder privater Trägerschaft ist das BDSG einschlägig, bei Einrichtungen in öffentlicher Trägerschaft gilt grundsätzlich das Landesdatenschutzgesetz, das aber für öffentliche Stellen, die als Unternehmen mit eigener Rechtspersönlichkeit am Wettbewerb teilnehmen – also auch für entsprechende Pflegeeinrichtungen – auf das materielle Datenschutzrecht des BDSG verweist (§ 2 Abs. 3 LDSG).

Kirchliches Datenschutzrecht lässt die Übermittlung von Daten an öffentliche Stellen zu, wenn diese zur rechtmäßigen Erfüllung öffentlicher Aufgaben erforderlich ist. Nach dem BDSG ist die Datenübermittlung u. a. zulässig, soweit sie zur Wahrung öffentlicher Interessen erforderlich ist und kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat (§ 28 Abs. 2 Nr. 1 BDSG). Danach kann davon ausgegangen werden, dass die Datenübermittlung nach beiden Rechtsgrundlagen zulässig ist.

Es stellt sich noch die Anschlussfrage, ob die Datenübermittlung auch dann zulässig ist, wenn die übermittelten Daten zur Grundlage einer Besprechung gemacht werden sollen, an der sowohl die Verbände der Pflegekassen wie auch der Medizinische Dienst und die Heimaufsicht teilnehmen. Der LfD vertrat die Auffassung, dass die Datenübermittlung zum Zwecke der gemeinsamen Besprechung mit den Verbänden und dem Medizinischen Dienst zulässig ist. Die gleichzeitige Anwesenheit von Vertretern der Heimaufsicht müsste aber als ein Problem angesehen werden:

Die Tätigkeit der Heimaufsicht ist nicht im SGB XI, sondern im Heimgesetz geregelt. Nach § 9 Abs. 1 werden die Heime durch wiederkehrende Prüfungen der zuständigen Behörden überwacht. Absatz 2 gibt den von der zuständigen Behörde mit der Überwachung des Heims beauftragten Personen die Befugnis, die für das Heim benutzten Grundstücke und Räume, soweit diese nicht einem Hausrecht der Bewohner unterliegen, während der üblichen Geschäftszeit zu betreten, dort Prüfungen und Besichtigungen vorzunehmen, in die geschäftlichen Unterlagen des Auskunftspflichtigen Einsicht zu nehmen, sich mit den Bewohnern in Verbindung zu setzen und die Beschäftigten zu befragen. Diese Vorschrift deckt ihrem Wortlaut nach nur die Datenerhebung durch Einsicht „vor Ort“, gilt insoweit aber nur vor dem Hintergrund einer zwischen der Heimaufsicht und dem Heimträger streitigen Wahrnehmung von Prüfungsaufgaben und schließt jedenfalls nicht aus, dass ein Heimträger, wenn er die Heimaufsicht in dieser Weise unterstützen will, prüfungsrelevante Materialien an die Behörde übersendet oder in einer gemeinsamen Besprechung mit der Heimaufsicht verwendet. Im Übrigen sind die Zielsetzungen der Heimaufsicht und der Prüfungen zum Zwecke der Qualitätssicherung nicht vollkommen identisch. Es ist davon auszugehen, dass letztere einen stärker fachlich-medizinischen Bezug hat.

Sofern die Heimaufsicht ihre Prüfungsaufgaben gemeinsam mit den Verbänden der Pflegekassen und dem Medizinischen Dienst wahrnehmen will, sei es, dass sie an einer gemeinsamen Besprechung und Beurteilung von Pflegedokumentationen teilnimmt, sei es, dass gemeinschaftliche Begehungen stattfinden, stellt sich freilich ein datenschutzrechtliches Problem, wenn hierbei nicht nur personenbezogene Daten erhoben, sondern auch weitergegeben werden. Die Weitergabe solcher Informationen durch die Verbände und den Medizinischen Dienst einerseits, wie auch durch die Heimaufsicht andererseits ist als Datenübermittlung zu

qualifizieren. Eine Datenweitergabe findet in aller Regel auch statt, wenn Vorgänge von Angehörigen unterschiedlicher Behörden besprochen werden. Denn die Erörterung beschränkt sich in aller Regel nicht auf die Wiedergabe der zur Kenntnis genommenen Informationen, sondern sie umfasst Beurteilungen und Reflexionen, die als selbständige Informationsvorgänge i. S. der datenschutzrechtlichen Übermittlungsbestimmungen anzusehen sind. Die Verbände und der Medizinische Dienst haben hierbei die Vorschriften des Sozialgesetzbuchs, die Heimaufsicht die Vorschriften des LDSG zu beachten. Besonders das Sozialgesetzbuch setzt einer Datenübermittlung an Behörden, die, wie die Heimaufsicht, nicht Sozialleistungsträger sind, enge Schranken. Nach § 69 Abs. 1 Nr. 1 SGB X ist sie zulässig, wenn sie zur Erfüllung einer gesetzlichen Aufgabe der übermittelnden Stelle erforderlich ist. Aus § 35 SGB I ergibt sich für die Verbände und den Medizinischen Dienst unmittelbar die Verpflichtung, auch innerhalb dieser Organisationen sicherzustellen, dass die Sozialdaten nur Befugten zugänglich sind oder nur an diese weitergegeben werden. Jeder Datenübermittlung hat jedenfalls eine Prüfung der rechtlichen Zulässigkeit vorauszugehen.

Zusammenfassend äußerte der LfD die Besorgnis, dass die Beachtung der datenschutzrechtlichen Übermittlungsbestimmungen in einer nicht hinnehmbaren Weise gefährdet ist, wenn Einzelvorgänge aus der Pflegedokumentation durch die o. a. Stellen gemeinsam zur Kenntnis genommen und erörtert werden. Er empfahl, von einer gemeinsamen Wahrnehmung von Aufgaben nach § 80 SGB XI und § 9 Heimgesetz abzusehen.

12. Datenschutz im Ausländerwesen

12.1 Einführung von Asyl-Cards

Im letzten Tätigkeitsbericht wurde über eine sog. „Machbarkeitsstudie für Asyl-Card“ berichtet (16. Tb., Tz. 12.6). Das Ergebnis dieser Studie liegt zwischenzeitlich vor. Danach kann aus Sicht der Verfasser eine Chipkarte mit Identitätsdaten, aber auch mit Verwaltungsdaten über den Karteninhaber wesentlich zur Vereinfachung des Verfahrens beitragen. Aus datenschutzrechtlicher Sicht hat der LfD demgegenüber auf die damit einhergehenden Risiken für die Persönlichkeitsrechte der Asylbewerber hingewiesen. Nunmehr zeichnet sich ab, dass seitens des zuständigen Bundesministeriums eine sog. „Basisdatenlösung“ bevorzugt wird. Dies würde darauf hinauslaufen, dass eine Asyl-Card zwar als Chipkarte ausgestaltet wird, diese Chipkarte aber im Wesentlichen nur Identitätsdaten des betroffenen Asylbewerbers, sozusagen als qualifiziertes Ausweisdokument enthalten soll. Das Ministerium des Innern und für Sport hat vorbehaltlich der Klärung der Kostenfrage der Weiterentwicklung grundsätzlich zugestimmt. Offen ist derzeit noch, ob Rheinland-Pfalz an einem entsprechenden Pilotprojekt teilnehmen wird.

Aus datenschutzrechtlicher Sicht ist dem geplanten Verfahren im Grundsatz nicht zu widersprechen. Allerdings ist auch in diesem Zusammenhang das Gebot der Transparenz zu beachten, mit anderen Worten: Der Asylbewerber muss die Möglichkeit haben, den Inhalt der auf der Chipkarte gespeicherten Daten zur Kenntnis nehmen zu können. Dies bedeutet, dass zumindest die Ausländerbehörden mit Lesegeräten auszustatten sind, die den Karteninhabern die Möglichkeit geben, sich selbst über die gespeicherten Daten zu informieren.

Soweit beabsichtigt ist, unveränderliche Identifikationsmerkmale (wie Fingerabdrücke oder ähnliche biometrische Daten) auf der Chipkarte digitalisiert zu speichern, so sieht der LfD auch dagegen aus datenschutzrechtlicher Sicht keine durchgreifenden Bedenken. Die Fälschungssicherheit und die Eindeutigkeit der Zuordnung eines Ausweisdokuments zum jeweiligen Inhaber verhindert Missbrauchsmöglichkeiten; die „Freiheit, sich rechtswidrig zu verhalten“, wird eingeschränkt. Diese Freiheit ist aber auch aus datenschutzrechtlicher Sicht nicht schutzwürdig. Die Einzelheiten der Nutzung eines solchen besonderen maschinenlesbaren Ausweises für Asylbewerber, insbesondere auch über die Nutzung der Daten, die beim Einsatz dieses Ausweises bei den kartenlesenden Stellen entstehen, sollten allerdings in Anlehnung an die Regelungen des Personalausweisgesetzes verbindlich festgelegt werden.

12.2 Ausschreibungen zur Einreiseverweigerung im Schengener Informationssystem

Wenn Drittstaatler, also Nicht-EG-Ausländer, von deutschen Ausländerbehörden ausgewiesen werden, so können sie von diesen gem. Artikel 96 des Schengener Durchführungsübereinkommens zur Einreiseverweigerung im Schengener Informationssystem ausgeschrieben werden. Damit soll erreicht werden, dass bereits an den Außengrenzen der Europäischen Union festgestellt werden kann, ob ein einreisewilliger Drittstaatler in das Schengengebiet einreisen darf.

In letzter Zeit erreichen den LfD auf folgendem Weg in zunehmendem Maße Auskunfts- und Löschungsersuchen von betroffenen Personen:

Die Betroffenen wenden sich zur Wahrnehmung ihrer Auskunfts- und Löschungsansprüche an die Kontrollinstanzen des Staates, an dessen Grenze sie zurückgewiesen wurden. Insbesondere die französische Kontrollbehörde, die Commission Nationale de l’Informatique et des Libertés (CNIL) übermittelt derzeit durchschnittlich etwa zwei bis drei Ersuchen pro Woche an den Bundesbeauftragten für den Datenschutz mit der Bitte, die Rechtmäßigkeit der Ausschreibung des betreffenden Petenten durch deutsche Stellen zu überprüfen. Die datenschutzrechtliche Prüfung fällt im Einzelfall dann in den Aufgabenbereich des jeweils zuständigen Landesdatenschutzbeauftragten, der vom BfD über die Anfrage unterrichtet und gebeten wird, ihm das Ergebnis der Überprüfung mitzuteilen.

Auch Ausschreibungen durch rheinland-pfälzische Ausländerbehörden sind von derartigen Anfragen betroffen worden. Die Überprüfungen durch den LfD haben bislang nicht ergeben, dass die Ausländerbehörden die maßgeblichen rechtlichen Grundlagen (neben Art. 96 SDÜ insbesondere die „Allgemeinen Anwendungshinweise zum Schengener Durchführungsübereinkommen" vom 28. Januar 1998) missachtet hätten. Zu prüfen war, ob eine Ausschreibung als datenschutzrechtlich unbedenklich zu bewerten ist und ob die Ausschreibungsfristen eingehalten worden sind. Die Ausschreibung zur Einreiseverweigerung soll regelmäßig zunächst für drei Jahre erfolgen; danach ist eine Verlängerung zu prüfen. Eine einmalige Verlängerung um weitere drei Jahre ist grundsätzlich nicht zu beanstanden. Die darüber hinausgehende Verlängerung allerdings bedarf einer besonderen Begründung. Die vom LfD zu überprüfenden Fälle betrafen sämtlich straffällig gewordene Ausländer, deren Taten so gewichtig waren, dass die angeordneten Fristen auch aus datenschutzrechtlicher Sicht zu akzeptieren waren.

12.3 Verpflichtungserklärung vor Visum an ausländischen Gast

Welche datenschutzrechtlichen Fragen bestehen, wenn jemand, der Ausländer aus bestimmten Staaten einlädt, sich verpflichtet, die Kosten des Lebensunterhalts des Ausländers zu tragen, ist bereits im 16. Tb. (Tz. 12.5) geschildert worden.

Die Ausländerbehörden sollen hier grundsätzlich bundeseinheitlich verfahren. Dies soll durch eine allgemeine Verwaltungsvorschrift der Bundesregierung zum Ausländergesetz sichergestellt werden. Die entsprechende Verwaltungsvorschrift ist bislang noch nicht in Kraft gesetzt. Sie ist dem Bundesrat mit Datum vom 9. Juli 1998 zur Zustimmung zugeleitet worden (BR-Drs. 972/98). Der Bundesrat hat eine Reihe von Änderungen vorgeschlagen, die zum Teil nicht nur der Verwaltungsvereinfachung, sondern auch dem Datenschutz dienen (BR-Drs. 350/99). Der Text des vorliegenden Entwurfes und die dazu vorliegenden Änderungsvorschläge des Bundesrates sind aus Sicht des LfD nicht zu beanstanden.

13. Finanzverwaltung

13.1 Outsourcing in der Steuerverwaltung – Versand von Steuervordrucken durch Private

Einem Ende 1998 erschienenen Zeitungsartikel war zu entnehmen, dass die OFD Koblenz beabsichtigte, aus Kostengründen die Steuerformulare für 1998 durch eine private Firma in Bamberg verschicken zu lassen. Darauf angesprochen informierte die OFD den LfD über ihr Vorhaben: Die Firma in Bamberg sollte einen Datenträger mit Angaben von Namen, Anschriften und Steuernummern der Bürger sowie über die Art der jeweils zu verschickenden Formulare erhalten. Sie sollte dann das Anschreiben aufgrund dieser Angaben ausdrucken und mit den entsprechenden Formularen versenden. Dadurch sollte sich eine Einsparung von rund 180 000,– DM ergeben.

Eine hier vorliegende Auftragsdatenverarbeitung durch nichtöffentliche Stellen soll gem. § 4 Abs. 4 Satz 2 LDSG nur dann erfolgen, wenn überwiegende schutzwürdige Interessen einer solchen Vergabe nicht entgegenstehen. Steuerdaten unterliegen als besonders sensible Daten dem Steuergeheimnis und stehen unter dem besonderen Schutz der Rechtsordnung. Damit dürfen Datenverarbeitungsvorgänge solch sensibler Art nur ausnahmsweise an Private übertragen werden. Ökonomische Gründe können eine solche Ausnahme rechtfertigen, wenn der Datenschutz beim Auftragnehmer im Übrigen gemäß den Anforderungen des § 4 LDSG gewährleistet ist. Diese Voraussetzungen waren hier erfüllt. Allerdings hatte sich der Auftragnehmer im mit der OFD abgeschlossenen Datenschutzvertrag der Kontrolle des LfD gem. § 4 Abs. 1 Satz 3 LDSG nicht unterworfen. Eine solche Regelung wurde nach einem Hinweis des LfD in den Datenschutzvertrag mit dem Auftragnehmer aufgenommen.

Weiterhin war davon auszugehen, dass es sich bei der Nutzung der Steuerpflichtigendaten zum Zwecke der Verschickung der Steuerformulare durch eine Fremdfirma um eine wesentliche Änderung der von der OFD angemeldeten automatisierten Verfahren handelt. Solche Änderungen sind gem. § 27 Abs. 1 Satz 3 LDSG fortlaufend von Amts wegen mitzuteilen, was auf Anfrage des LfD hin auch geschehen ist.

Der Datenträger wurde nach Versand der Vordrucke an das DIZ zurückgeschickt und dort gelöscht.

Obwohl das Verfahren letztlich datenschutzrechtlich nicht zu beanstanden war, wäre eine Einbeziehung des LfD durch die OFD bereits vor der Auftragsvergabe wünschenswert gewesen.

13.2 Arzt und Fahrtenbuch oder der Patient als Geschäftspartner

Seit dem 1. Januar 1998 sind Ärzte bei der Führung eines steuerlichen Fahrtenbuches verpflichtet, neben Datum, Kilometerstand und Ort den aufgesuchten Patienten – sozusagen als Geschäftspartner – mit Name und Anschrift zu verzeichnen. Sind diese Angaben im Fahrtenbuch nicht enthalten, wird die Nutzung des betrieblichen Kfz nach einer Pauschalregelung bewertet. Vor diesem Zeitpunkt war es ausreichend, statt Name und Anschrift lediglich „Patientenbesuch" zu vermerken.

Diese Regelung stößt auf erhebliche datenschutzrechtliche Bedenken, da hierin vom LfD ein Verstoß gegen das auch abgabenrechtlich geschützte Arztgeheimnis (§ 102 Abs. 1 Nr. 3 lit. c AO) gesehen wird. Danach steht Ärzten ein Auskunftsverweigerungsrecht über das zu, was ihnen in ihrer Eigenschaft als Arzt anvertraut oder bekannt geworden ist. Diese Vorschrift dient der Wahrung der ärztlichen Schweigepflicht. Dabei bezieht sich die Vorschrift auf alles, was dem Arzt im Rahmen seiner Tätigkeit

als solchem bekannt geworden ist. Dies beinhaltet nicht allein Inhalte des Arzt-Patienten-Verhältnisses, sondern schützt bereits die Information über die Tatsache, dass der Patient einen Arzt aufgesucht hat, vor Preisgabe. Zudem könnte sich der Arzt nach § 203 Abs. 1 Nr. StGB strafbar machen, wenn er die Patientennamen und -adressen angibt.

Nunmehr konnte auf Betreiben des BfD eine Kompromisslösung mit dem Bundesfinanzministerium erzielt werden: Danach sollen in einem vom eigentlichen Fahrtenbuch getrennten Verzeichnis Name und Adresse der aufgesuchten Patienten vermerkt werden. Die Finanzbehörden sollen dieses Verzeichnis nur dann einsehen, wenn Zweifel an der Richtigkeit der Eintragungen im Fahrtenbuch bestehen und alle anderen rechtlichen Mittel zum Ausräumen dieser Zweifel ausgeschöpft sind.

Dies ist nach Ansicht des LfD ein weiterer Schritt, um den bereichsspezifischen Datenschutz in der Abgabenordnung voranzubringen.

13.3 Bekämpfung der Korruption in der öffentlichen Verwaltung

Mit der Verwaltungsvorschrift zur „Bekämpfung der Korruption in der öffentlichen Verwaltung“ hat sich der LfD bereits 1997 auseinander gesetzt (vgl. 16. Tb., Tz. 14.5).

War man vor zwei Jahren im Ministerium der Finanzen noch der Auffassung, bei der dort eingerichteten Melde- und Informationsstelle würde die Notwendigkeit zur Speicherung personenbezogener Daten nicht bestehen, geht man nun davon aus, zukünftig auch solche Daten zu speichern. Denn mittlerweile schicken die Staatsanwaltschaften des Landes Kopien einschlägiger Strafurteile – die zwangsläufig personenbezogen sind – an das Finanzministerium, das daraus Angaben für die Melde- und Informationsstelle übernehmen soll.

Der LfD ist davon ausgegangen, dass auch das Speichern personenbezogener Daten nicht zu beanstanden ist, da dies für die Aufgabenerfüllung des Finanzministeriums als oberstem Wächter über die öffentlichen Haushaltsmittel erforderlich ist. Zudem bedeutet das Speichern bei der Melde- und Informationsstelle nicht den automatischen Ausschluss vom Vergabeverfahren, so dass der Eingriff nicht so schwer wiegend ist, dass er eine eigene spezialgesetzliche Rechtsgrundlage erfordert. Voraussetzung ist allerdings, dass die Betroffenen über die Speicherung informiert werden und so die Möglichkeit haben, ihre inhaltliche Richtigkeit zu prüfen und ggf. gegen eine solche vorzugehen.

14. Wirtschaft und Verkehr

14.1 Grundsätzliches zur Auskunftserteilung über Gewerbeanzeigen

Die von den Gewerbetreibenden vorgenommenen Anzeigen werden immer seltener in einer Gewerbekartei geführt. Die Verarbeitung der erstatteten Gewerbeanzeigen auf elektronischen Datenträgern hat sich durchgesetzt.

Die den Gewerbebehörden zu erstattenden Gewerbeanzeigen sind für andere Behörden, aber auch für Privatpersonen und Gewerbetreibende von Bedeutung. Es stellt sich daher häufig die Frage, ob und in welchem Umfang Gewerbeanzeigen Dritten bekannt gegeben werden dürfen. Hinsichtlich der Einordnung der abrufbaren Datensammlungen weist der LfD regelmäßig darauf hin, dass das Gewerberegister kein öffentliches Register wie etwa das Handels- oder das Vereinsregister ist.

In § 14 Abs. 5 GewO werden die öffentlichen Stellen benannt, die regelmäßig Daten aus den Gewerbeanzeigen erhalten können. Die jeweils zur Übermittlung in Betracht kommenden Daten aus den Gewerbeanzeigen sind in den Nummern 1 bis 8 im Einzelnen bestimmt und durch die Feldnummern der nach dem Absatz 4 und der Anlage 1 bis 3 vorgeschriebenen Gewerbeanzeigeformulare festgelegt. Damit ist eine – nach den Erfahrungen des LfD bei örtlichen Feststellungen – streng zweckorientierte Datenauswahl, die den jeweiligen öffentlichen Stellen zugeht, gewährleistet.

Die Rechtslage bei der Auskunftserteilung an Private aus dem Gewerberegister hat der LfD im 15. Tb, Tz. 14.2 dargestellt.

Hinzuweisen ist schließlich auf eine Gesetzesänderung im Bereich der Gewerbeabmeldung. So konnte nach der früheren Rechtslage die Abmeldung des Gewerbes nicht von Amts wegen erfolgen, sondern musste oft mit Zwangsmitteln, die regelmäßig zeitraubend waren, durchgesetzt werden. Hier konnte es dazu kommen – dies belegt eine Eingabe aus dem Berichtszeitraum –, dass bei einer Auskunft aus der Gewerbeanzeige nach § 14 Abs. 8 GewO wegen der fehlenden Anzeige der Gewerbeabmeldung ein ordnungsgemäß angemeldetes Gewerbe vorgetäuscht wurde. Zwischenzeitlich hat der Gesetzgeber mit dem Zweiten Gesetz zur Änderung der Gewerbeordnung vom 16. Juni 1998 (BGBl I, 1291 ff.) diesen Missstand behoben. Nunmehr kann die Behörde nach § 14 Abs. 1 GewO eine Gewerbeabmeldung von Amts wegen vornehmen, wenn die Aufgabe des Gewerbes eindeutig feststeht und die Abmeldung nicht innerhalb eines angemessenen Zeitraums erfolgt.

14.2 Zugriffe auf den Datenbestand des Gewerbeamtes

Anlässlich örtlicher Feststellungen bei einer Stadtverwaltung war unter anderem der geplante automatisierte Zugriff des Steueramtes auf die Daten des neu eingeführten Gewerbeinformationssystems Gegenstand der Erörterung. Die nähere Prüfung hat ergeben, dass die Erläuterungen im Rahmen der Anmeldung zu Missverständnissen geführt haben. So wurde seitens des Gewerbeamtes in der Verfahrensanmeldung darauf hingewiesen, dass eine Selektion der weiterzuleitenden Daten nicht möglich sei, so dass dem Steueramt ein Zugriff auf den gesamten Datenbestand ermöglicht werden müsse.

Es hat sich jedoch herausgestellt, dass entgegen den Angaben in der Anmeldung die Zugriffe des Steueramtes sich nicht auf alle in dem Verfahren anfallenden personenbezogenen Daten bezogen haben, sondern aus der gesamten Palette der Datensätze lediglich einige Felder für das Steueramt von Bedeutung gewesen sind. Da die Feldstruktur des Gewerbeinformationssystems programmseitig die freie Steuerung zugelassen hat, ist eine Verfahrensweise vereinbart worden, die das Steueramt in die Lage versetzt, die gewerbesteuerlichen Aspekte zu beurteilen, ohne einen Zugriff auf sämtliche Datenfelder zu eröffnen.

Dem Steueramt werden auf der Grundlage von § 14 Abs. 6 GewO folgende Datenfelder per Maske angeboten:
- Name,
- Geburtsdatum,
- betriebliche Anschrift,
- angezeigte Tätigkeit,
- Anmeldedatum,
- Vorgangsnummer.

Problematisch war indessen, dass aufgrund technischer Gegebenheiten in dem Gewerbeinformationssystem keine Möglichkeit bestanden hat, die (nicht ändernden) Zugriffe seitens des Steueramtes zu protokollieren. Lediglich dann, wenn (feldbezogen) der Dateninhalt geändert wurde, führte das System Protokoll. Die datenschutzrechtlichen Anforderungen waren im Hinblick auf die Protokollierungsregelung in § 14 Abs. 7 GewO also nicht erfüllbar.

Der LfD hält allerdings eine vom Anwender nicht beeinflussbare Protokollierung als angemessene Maßnahme des technisch-organisatorischen Datenschutzes für unverzichtbar und hat darum gebeten, das Erforderliche zu veranlassen.

14.3 Weitergabe von Gewerbedaten an den Ausländerbeirat

Der LfD hatte sich mit der Frage der Zulässigkeit der Übermittlung von Anschriften ausländischer Gewerbebetriebe zu befassen, wobei eine Datenweitergabe durch ein Gewerbeamt an den Ausländerbeirat in Rede stand.

Für eine inhaltliche Stellungnahme ist der LfD hier zuständig, soweit personenbezogene Daten natürlicher Personen betroffen sind. Er hat die Zulässigkeit der Datenübermittlung verneint:

Durch § 14 Abs. 5 GewO werden die öffentlichen Stellen benannt, die regelmäßig Daten aus den Gewerbeanzeigen erhalten können. Der Ausländerbeirat ist dort nicht erwähnt. Gemäß der Regelung in § 14 Abs. 6 GewO dürfen an weitere öffentliche Stellen fallweise bestimmte Daten übermittelt werden, soweit dies zur Erfüllung der in ihre Zuständigkeit fallenden Aufgaben erforderlich ist. Die ersuchte Behörde hat also zu prüfen, ob die Voraussetzungen für eine Datenübermittlung gegeben sind. Die Erforderlichkeit der Übersendung der Daten liegt dann vor, wenn die Empfängerseite ohne die zu übermittelnden Daten ihre Aufgaben nicht oder nicht sachgerecht erfüllen kann. Eine gesetzlich dem Ausländerbeirat zugewiesene Aufgabe, woraus sich eine Datenerhebungsbefugnis im vorliegenden Zusammenhang hätte ergeben können, war nicht ersichtlich; ebenso oblag ihm keine Aufgabe, zu deren Erfüllung die begehrte Datenübermittlung erforderlich war.

14.4 Weitergabe aller Firmendaten an einen Online-Dienst

Aufgrund der Anfrage einer Industrie- und Handelskammer hatte sich der LfD mit dem Problem zu befassen, ob die dort vorhandenen Handelsregisterdaten und die Daten der Kleingewerbetreibenden des Kammerbezirks einem kammerzugehörigen Unternehmen zwecks Einspeisung in das Internet übermittelt werden dürfen.

Er hat der datenschutzrechtlichen Beurteilung folgende Überlegungen zugrunde gelegt:

Für die Daten der Kammerzugehörigen enthält § 9 IHK-Gesetz eine bereichsspezifische Datenschutzregelung. Nach § 9 Abs. 4 dürfen die Industrie- und Handelskammern Name, Firma, Anschrift und Wirtschaftszweig ihrer Kammerzugehörigen zur Förderung von Geschäftsabschlüssen und zu anderen dem Wirtschaftsverkehr dienenden Zwecken an nichtöffentliche Stellen übermitteln. Bei der Einspeisung in das Internet kann jedoch jedermann weltweit ohne Nachweis irgendeines Interesses die Daten abrufen. Bei diesem Verfahren ist nicht gewährleistet, dass die Daten nur zur Förderung von Geschäftsabschlüssen und zu anderen dem Wirtschaftsverkehr dienenden Zwecken übermittelt werden.

Bei der Bereitstellung im Internet ergäben sich auch vielfältige Auswertungsmöglichkeiten nach vielen verschiedenen Suchkriterien. Die über Stichwörter gesuchten Angaben könnten auf dem Bildschirm angezeigt und ausgedruckt werden. So wäre es z. B. möglich, mit dem Suchkriterium eines bestimmten Namens die gesamten Geschäftsbeteiligungen dieser Person (u. U. bundesweit) festzustellen und auszudrucken.

Wenn die IHK sämtliche Handelsregisterdaten und sämtliche Daten der Kleingewerbetreibenden des Kammerbezirks einem kammerzugehörigen Unternehmen überlassen würde (um ihm den Aufbau eines sog. Internet-Marktes zu ermöglichen), könnte dies insoweit neben dem Registergericht ein zweites (Teil-)Handelsregister darstellen. Nach § 8 HGB i. V. m. § 125 FGG werden die Handelsregister aber ausschließlich von den Amtsgerichten geführt. Werden die bestehenden Handelsregister in das Internet eingestellt, könnte auf diese Art und Weise bald ein bundesweites Handelsregister entstehen.

Derartige frühere Bemühungen sind bereits durch den BGH im Jahre 1989 gestoppt worden. Seinerzeit wurde von privater Seite angestrebt, bundesweit die Daten sämtlicher Handelsregister auf Mikrofilm zu übertragen. Der BGH verneinte hier die Zulässigkeit einer solchen Totalaufnahme aller Handelsregistereintragungen mit der Begründung, die einzig in Betracht kommende Vorschrift, § 9 HGB, gestatte nur die Einsichtnahme im Einzelfall, nicht aber eine Gesamteinsichtnahme des Registers. Darüber hinaus widerspricht es dem Zweck des Handelsregisters, die Daten zu einem Serviceangebot aufzubereiten und über Internet anzubieten.

Der 1993 eingefügte § 9 a HGB regelt den automatischen Abruf aus dem Handelsregister und lässt diesen nur unter engen Voraussetzungen zu. Mit der Regelung wollte der Gesetzgeber „hinreichende Vorkehrungen gegen einen Missbrauch, insbesondere gegen eine zweckwidrige Benutzung derartiger Anschlüsse“ schaffen und den „Schutz personenbezogener Daten“ gewährleisten (Gesetzentwurf der Bundesregierung vom 12. August 1993, BT-Drs. 12/5553, Begründung zu § 9 a HGB). Zwar richtet sich § 9 a HGB nicht unmittelbar an die Industrie- und Handelskammern, sondern an die für die Führung der Handelsregister zuständigen Gerichte. Aus der Sicht des Betroffenen macht es jedoch keinen Unterschied, ob das Registergericht oder eine andere Stelle den automatisierten Abruf seiner personenbezogenen Daten ermöglicht. Seine Schutzbedürftigkeit ist in beiden Fällen die gleiche. Die Schutzwirkung des § 9 a HGB erstreckt sich deshalb auch auf alle Fälle, in denen andere Stellen als die Registergerichte Handelsregisterdaten in automatisierten Abrufverfahren anbieten. Eine Beachtung der Voraussetzung des § 9 a HGB wäre bei einer Einstellung von Handelsregisterdaten in das Internet nicht möglich.

Nach Auffassung des LfD wären gegen die Einstellung von Handelsregisterdaten in das Internet nur dann keine Einwände zu erheben, wenn die Betroffenen vor einer Veröffentlichung ihrer personenbezogenen Daten im Internet ihre (informierte) Einwilligung erteilt hätten.

14.5 Datenerhebung bei Stundungen

Der LfD hatte sich mit Eingaben zu befassen, in denen die Beschwerdeführer den Inhalt eines auf kommunaler Ebene entwickelten Fragebogens zum Stundungsantrag hinsichtlich fälliger Gebühren rügten. Es würden unverhältnismäßig viele Informationen über ihre wirtschaftliche Situation verlangt: nämlich Angaben zu den Familienverhältnissen, zum Einkommen und Vermögen sowie zu Krediten und sonstigen laufenden Zahlungsverpflichtungen.

Rechtsgrundlage für die Erhebung der diesbezüglichen personenbezogenen Daten ist § 3 Abs. 1 KAG i. V. m. § 222 AO. Danach besteht die Möglichkeit, die Forderung zu stunden oder zu erlassen. Der Gesetzgeber macht dies jedoch von ganz strengen Voraussetzungen abhängig. Einerseits muss die Einziehung der Forderung bei Fälligkeit für den Betroffenen eine erhebliche Härte bedeuten und andererseits darf der Anspruch durch die Stundung nicht gefährdet erscheinen. Diese Regelung macht es erforderlich, den Antrag auf Stundung hinreichend zu begründen. Der Begriff „erhebliche Härte“ ist ein unbestimmter Rechtsbegriff, der mit einer Ermessensentscheidung gekoppelt ist. Um zu dieser Ermessensentscheidung zu kommen, muss eine Überprüfung der wirtschaftlichen Verhältnisse der antragstellenden Person durchgeführt werden. Die öffentliche Stelle ist daher verpflichtet zu prüfen, ob beim Betroffenen aufgrund der persönlichen und wirtschaftlichen Verhältnisse ein Härtefall vorliegt, der es ermöglicht, Ratenzahlung zu gewähren. Der Nachweis der Stundungsgründe ist hinsichtlich des möglichen Missbrauchs der Vorschrift des § 222 AO unerlässlich. Dies gilt insbesondere auch für die Wahrung des Gleichheitsgrundsatzes.

Die in dem Vordruck gestellten Fragen waren aus Sicht des LfD nicht offensichtlich unvertretbar, so dass er keinen Verstoß gegen datenschutzrechtliche Vorschriften erkennen konnte.

Allerdings wurde die den Fragebogen nutzende Stelle um eine Ergänzung des Vordrucks insoweit gebeten, dass dort die Betroffenen auf die Rechtsvorschriften für die Datenerhebung bzw. die Freiwilligkeit ihrer Angaben ausdrücklich hingewiesen werden sollten.

14.6 Privatisierung von Tätigkeitsbereichen

Die Datenschutzbeauftragten des Bundes und der Länder haben auf ihrer 55. Konferenz im März 1998 beschlossen – unter Federführung des LfD Rheinland-Pfalz – eine Arbeitsgruppe „Outsourcing“ einzusetzen, die sich mit den datenschutzrechtlichen Rahmenbedingungen einer Auslagerung von Datenverarbeitungsaufgaben näher befassen sollte.

Gegenwärtig wird in allen Zweigen der Verwaltung nach Entlastungsmöglichkeiten gesucht. Immer häufiger wird die Frage gestellt: „Make or Buy?“ Ist Eigenherstellung erforderlich oder kann fremdgefertigt werden? Argumentiert wird häufig mit Kostensenkung. Die Zauberformel Outsourcing ist jedoch nichts völlig Neues. Die Nutzung externer Leistungen und Hilfsmittel gibt es in mancherlei Organisationsformen seit langem. Outsourcing wird oft skeptisch gesehen. Für diese Verarbeitungsform können aber auch gute Gründe sprechen, so z. B. hohe Qualität der Verarbeitung durch Spezialisierung und die Interessenferne der Auftragnehmer gegenüber den Daten der Betroffenen.

Die Arbeitsgruppe hat den Versuch unternommen, eine gemeinsame Sichtweise zu entwickeln, Gefahren zu erkennen und neue Entwicklungen in datenschutzgerechte Bahnen zu lenken. Es wurde ein – von der Konferenz zustimmend zur Kenntnis genommenes – Tendenzpapier erarbeitet, das nachfolgend wiedergegeben ist:

„I. Problembeschreibung

Unter Outsourcing (Outside Resource Using) versteht man die Auslagerung von Unternehmensfunktionen auf ein anderes Unternehmen zur selbständigen Aufgabenerledigung. Zunehmend übertragen auch öffentliche Stellen ihre Aufgaben an Privatunternehmen in der Form des Outsourcing. Diese Entwicklung hat erhebliche Bedeutung auch für die Datenverarbeitung und erfordert eine Überprüfung der datenschutzrechtlichen Behandlung.

Es ist nicht zwingend, dass der Datenschutz von Outsourcing-Unternehmen schlechter gewahrt wird als von öffentlichen Stellen selbst. Das Outsourcing kann vielmehr zu einer Spezialisierung und zu einer höheren Professionalisierung führen (z. B. durch den Einsatz höher entwickelter Sicherheitstechniken).

Outsourcing geschieht in Form von Datenverarbeitung im Auftrag oder Funktionsübertragung.

1. Auftragsdatenverarbeitung

   Outsourcing in der Form der Auftragsdatenverarbeitung ist dadurch gekennzeichnet, dass die einzelnen Schritte der Datenverarbeitung vom Auftraggeber präzise vorgegeben werden. Der Auftragnehmer hat keinerlei Ermessensspielraum (vgl. § 11 BDSG).

2. Funktionsübertragung

   Beim Outsourcing als Funktionsübertragung bestimmt der Funktionsnehmer selbständig die Art und Weise der Datenverarbeitung. Im Unterschied zur Auftragsdatenverarbeitung kennen die allgemeinen Datenschutzgesetze für die Funktionsübertragung keine besonderen Regelungen. Für die Weitergabe der Daten an den Funktionsnehmer gelten vielmehr die Regelungen für die Datenübermittlung. Insbesondere fehlt eine gesetzliche Regelung dahin gehend, dass auch bei der Funktionsübertragung der Funktionsgeber dem Funktionsnehmer bestimmte Verpflichtungen auferlegen muss (z. B. Kontrolle durch den Funktionsgeber, Eignungsprüfung).

II. Möglichkeiten einer Problemlösung

Das Outsourcing wirft Probleme auf, für die das bestehende Datenschutzrecht keine geeigneten Lösungen anbietet:

Bei der bestehenden Rechtslage sollten für die Funktionsübertragung die einschlägigen Vorschriften zur Auftragsdatenverarbeitung (z. B. Zuverlässigkeit des Auftrag- bzw. Funktionsnehmers) ergänzend angewandt werden. Insbesondere ist die Nutzung der Daten für eigene Zwecke des Funktionsnehmers auszuschließen (Grundsatz der Zweckbindung). Eine Subdelegation ist nur zulässig, wenn dies im Auftrag ausdrücklich zugelassen wird.

Häufig wird die bei der Funktionsübertragung stattfindende Datenübermittlung an den Funktionsnehmer auf die Einwilligung der Betroffenen gestützt. Die Entscheidung über die Zulässigkeit des Outsourcing sollte aber nicht ohne weiteres in die Hände der Betroffenen gelegt werden, da die Vorgänge regelmäßig so kompliziert sind, dass sie den Betroffenen nicht transparent gemacht werden können. Daher sind zumindest die strengen Anforderungen an eine Einwilligung nach der EG-Datenschutzrichtlinie einzuhalten.

Außerdem sollte für die häufigen Fälle, in denen keine rechtswirksame Einwilligung in Betracht kommt, eine gesetzliche Regelung geschaffen werden, die einerseits präzise Bedingungen für die Zulässigkeit der Funktionsübertragung und andererseits hinreichende Betroffenenrechte, wie z. B. Aufklärung, Auskunfts- und Widerspruchsrecht (vgl. Art. 14 EG-Datenschutzrichtlinie), enthält.

Soweit für die Datenschutzkontrolle unterschiedliche Stellen zuständig sind, sollten die rechtlichen und praktischen Möglichkeiten der Zusammenarbeit ausgeschöpft werden (Optimierung der Kooperation), um ein Kontrolldefizit zu vermeiden.

Es gibt Formen der Datenverarbeitung, die ohne Kenntnis der personenbezogenen Daten auskommen (privacy enhancing technologies). Diese Entwicklung sollte sowohl für die Auftragsdatenverarbeitung als auch für die Funktionsübertragung unterstützt werden. Auch dann, wenn keine personenbezogenen Daten mehr anfallen oder durch organisatorische oder sonstige Maßnahmen eine Kenntnisnahme ausgeschlossen ist, sollten Vorschriften für das Outsourcing jedenfalls insoweit geschaffen werden, dass die Kontrollierbarkeit gewährleistet wird (z. B. Meldepflichten, Kontrollbefugnisse des Datenschutzbeauftragten). Dies gilt z. B. für Versuche, die Vorschriften zur Auftragsdatenverarbeitung dadurch zu „unterfliegen“, dass das Outsourcing-Unternehmen zwar Verarbeitungsaufgaben übernimmt, hierbei durch organisatorische oder sonstige Maßnahmen jedoch die Kenntnisnahme personenbezogener Daten weitestgehend ausgeschlossen wird.

III. Grenzen des Outsourcing

Hoheitliche Befugnisse dürfen auf ein Outsourcing-Unternehmen nur durch formelle Beleihung aufgrund einer gesetzlichen Regelung übertragen werden (z. B. bei Übertragung von Prüfaufgaben für Kraftfahrzeuge an amtlich anerkannte Sachverständige nach § 29 StVZO). Selbst hierbei ist der Funktionsvorbehalt (vgl. Art. 33 Abs. 4 GG) zu berücksichtigen, wonach die Ausübung hoheitlicher Befugnisse in der Regel Angehörigen des öffentlichen Dienstes zu übertragen ist. Das Auslagern von Datenverarbeitungsaufgaben kommt überhaupt nicht in Betracht, wenn die Aufgaben den Kernbereich hoheitlicher Tätigkeit

betreffen. Dies schließt Outsourcing z. B. im hoheitlichen Bereich der Finanzverwaltung und der Polizei aus. Unter der Voraussetzung effektiver Weisungs- und Kontrollrechte ist eine Übertragung einzelner Aufgaben, z. B. Problemlösungen im EDV-Bereich, möglich.

In den Fällen, in denen zwar öffentliche, aber nicht hoheitliche Aufgaben übertragen werden, sollte in Anlehnung an die Bestimmungen zu automatisierten Übermittlungsverfahren (§ 10 BDSG) oder zur Organisationskontrolle (Anhang zu § 9 BDSG) eine Angemessenheitsprüfung stattfinden. So gelangt man zu einer Abschätzung, welche Risiken mit der Aufgabenübertragung verbunden sind. Dabei kann es Sachverhaltskonstellationen geben, bei denen man zum Ergebnis gelangt, dass auch im nichthoheitlichen Bereich derartige datenschutzrechtliche Risiken bestehen, dass ein Outsourcing nicht in Betracht kommt.

Der Staat darf nicht dadurch seine Handlungsfähigkeit einschränken, dass er wesentliche Funktionen der Datenverarbeitung einem Dritten überträgt und auf diese Art und Weise die Freiheit verliert, Datenverarbeitungsverfahren zu regeln. Es muss sichergestellt werden, dass unter bestimmten Umständen (z. B. Unzuverlässigkeit des Auftrag- bzw. Funktionsnehmers) das Outsourcing rückgängig gemacht werden kann (Rückholbarkeit). Nicht umkehrbare Aufgabenübertragung ist unzulässig.

Der Staat hat aufgrund seiner – aus den Grundrechten abzuleitenden – Beobachtungs- und ggf. Nachbesserungspflicht die Auswirkungen des Outsourcing kontinuierlich zu verfolgen. Dabei kommt auch eine nachträgliche Einschränkung des übertragenen Aufgabenbereichs oder eine Verschärfung datenschutzrechtlicher Auflagen in Betracht."

Ein benachbartes Problemfeld ist die datenschutzrechtliche Behandlung von Teleheimarbeit. Hier sollte beachtet werden, dass sie kein Minus gegenüber der Auftragsdatenverarbeitung darstellt, sondern als eine Arbeitsform anzusehen ist, die gleich hohe oder sogar höhere Risiken birgt. Hinsichtlich der Erledigung von Aufgaben durch Bedienstete einer öffentlichen Stelle in Heimarbeit ist es angezeigt, Restriktionen, wie sie z. B. für die Auftragsdatenverarbeitung durch Private existieren, auch für die Heimarbeit zu definieren (vgl. dazu Tz. 17.3).

14.7 Datenschutzrechtliche Aspekte bei der Beteiligung Privater an der kommunalen Geschwindigkeitsüberwachung

Immer häufiger überwachen die Gemeinden selbst, ob Verkehrsteilnehmer die zulässige Geschwindigkeit einhalten. Da sie die Aufgabe der innerörtlichen Geschwindigkeitsüberwachung nicht ausschließlich unter Inanspruchnahme eigener Verwaltungsressourcen durchführen können, bieten zunehmend Privatfirmen Leistungen auf diesem Gebiet an. Datenschutzrechtliche Aspekte bei der Beteiligung Privater an der kommunalen Geschwindigkeitsüberwachung wurden mit dem Ministerium des Innern und für Sport unter Beteiligung eines Vertreters einer auf diesem Gebiet tätigen Privatfirma erörtert.

Anzusprechen waren verschiedene Tätigkeitsfelder, u. a. das Aufstellen und Justieren der Überwachungsgeräte sowie die Entwicklung und die Auswertung von Filmen. Der Meinungsaustausch hat zu folgenden grundsätzlichen Feststellungen geführt:

Die Geschwindigkeitsüberwachung und die Verfolgung und Ahndung daraus resultierender Verstöße ist als funktionell originäre Staatsaufgabe nicht auf Private übertragbar. Auch Hilfstätigkeiten sind in jenen Bereichen, in denen die einzelnen Verarbeitungsphasen selbständige Beurteilungen und Verfahrensentscheidungen durch die privaten Firmen voraussetzen würden, nicht zulässig. Die Verfolgungsbehörde hat vielmehr sämtliche Verfahrensschritte – dazu gehört insbesondere das Anlegen von Akten sowie die diesbezüglich erforderliche Erfassung von Daten – selbst durchzuführen.

Eine Behörde, die in eigener Regie Verkehrsüberwachungsgeräte betreiben möchte, hat allerdings jederzeit das Recht, diese Geräte bei Privaten anzumieten und zwecks Durchführung der Aufgaben auf deren technische Hilfeleistung, etwa beim Aufstellen und Justieren eines Überwachungsgeräts, zurückzugreifen.

Soweit die zuständige Behörde den Privatanbieter mit der Entwicklung von Filmen beauftragt, die im Rahmen von Geschwindigkeitsmessungen angefertigt worden sind, handelt es sich nicht um die Übertragung einer hoheitlichen Aufgabe. Mit der Filmentwicklung ist auch keine Entscheidung zur Einleitung eines Ordnungswidrigkeitenverfahrens verbunden. Hier kommt eine Datenverarbeitung im Auftrag gem. § 4 LDSG in Betracht. Soweit die entsprechenden gesetzlichen Vorgaben berücksichtigt werden, besteht gegen eine Filmentwicklung durch Private aus der Sicht des Datenschutzes kein Einwand. Denn die Hilfstätigkeit des Filmentwickelns hat nur den rein technischen Teil der Datenverarbeitung zum Gegenstand und erstreckt sich nicht auf das Verwaltungshandeln, dem die Daten dienen.

Wenn private Unternehmen in die Geschwindigkeitskontrollen und deren Auswertung als Auftragnehmer eingebunden werden, ist vertraglich sicherzustellen, dass diese keinerlei Daten aus dem Verfahren speichern bzw. Unterlagen oder Duplikate behalten. In diesem Zusammenhang darf der Private keine Möglichkeit erhalten, eine Ordnungswidrigkeit „unter den Tisch fallen zu lassen". Der entwickelte Film muss vollständig erhalten der auftraggebenden Behörde ausgehändigt werden, um gegebenenfalls später auch vor Gericht jederzeit in voller Länge eingesehen werden zu können.

Werden personenbezogene Daten im Auftrag einer öffentlichen Stelle durch andere (nichtöffentliche) Stellen verarbeitet, ist die auftraggebende Stelle weiterhin für die Einhaltung datenschutzrechtlicher Vorschriften verantwortlich (§ 4 LDSG). Dies gilt insbesondere für die Zulässigkeit der Verarbeitung personenbezogener Daten, die Wahrung der Rechte der Betroffenen sowie die Einhaltung der nach § 9 LDSG erforderlichen Datensicherungsmaßnahmen.

Der Auftragnehmer muss sorgfältig ausgewählt werden. Wichtiges Auswahlkriterium ist das Datensicherungskonzept des Auftragnehmers. Ein solches schriftlich festgelegtes Datensicherungskonzept erleichtert dem Auftraggeber auch den Vergleich und die Entscheidung zwischen mehreren Anbietern. Hierbei kann auch überprüft werden, ob der Auftragnehmer seiner Meldepflicht bei der Aufsichtsbehörde nach § 32 Abs. 1 Nr. 3 BDSG nachgekommen ist. Dies kann durch Einsicht in die Unterlagen des meldepflichtigen Dienstleistungsunternehmens oder durch Anfrage bei der zuständigen Aufsichtsbehörde geschehen. Die Gemeinde hat auch ihre Verantwortung für die Durchführung von Kontrollen beim Auftragnehmer sorgfältig wahrzunehmen. Sie muss als Auftraggeberin die Einhaltung der an den Auftragnehmer erteilten Weisungen überprüfen, um zu gewährleisten, dass die Verarbeitung der Daten durch den Auftragnehmer nur entsprechend ihren Weisungen erfolgt. Kein Auftraggeber darf sich mit der bloßen Erklärung des Auftragnehmers zufrieden geben, dass dieser die einschlägigen Datenschutzvorschriften beachten werde. Um diese Überprüfung durchführen zu können, bedarf es der Einräumung einer Kontrollbefugnis in den Geschäftsräumen des Auftragnehmers. Wenn der Auftragnehmer eine nichtöffentliche Stelle ist und somit die Vorschriften des LDSG für ihn nicht gelten, muss die datenschutzrechtliche Kontrolle dadurch sichergestellt werden, dass sich der Auftragnehmer gem. § 4 Abs. 1 LDSG der Überwachung durch den LfD unterwirft. Schließlich sollten folgende Festlegungen getroffen werden:

- Beschreibung der organisatorischen Maßnahmen zur Abgrenzung der Auftragsdatenverarbeitung zu anderen Unternehmensbereichen;
- Verpflichtung der Mitarbeiter des Auftragnehmers zur Wahrung des Datengeheimnisses gem. § 5 BDSG;
- falls die Beauftragung von Subunternehmen gestattet wird, Verpflichtung des Auftragnehmers, die Verfügungsberechtigungen und das Kontrollrecht des Auftraggebers auch gegenüber dem Subunternehmen vertraglich abzusichern;
- Vereinbarung wirksamer Sanktionen für den Fall datenschutzrelevanter Vertragsverletzungen durch den Auftragnehmer/Subunternehmer (z. B. außerordentliches Kündigungsrecht, Vertragsstrafenregelung).

Insgesamt hat die Erörterung des Themas aus Sicht des LfD einmal mehr vor Augen geführt, dass die Sorge um die Funktionsfähigkeit der Verwaltung regelmäßig mit den datenschutzrechtlichen Erfordernissen in Einklang steht.

14.8 Künftig Kraftfahrzeugzulassung über das Internet?

Die Frage der Zulässigkeit und Ausgestaltung des Verfahrens der Kfz-Zulassung über das Internet hat ein Repräsentant des Bundesverbandes der Kennzeichenhersteller an den LfD herangetragen. In Rheinland-Pfalz sind diesbezüglich bislang keine konkreten Überlegungen angestellt worden. Im Hinblick auf geplante Modellversuche in anderen Bundesländern hat eine Kontaktaufnahme mit dem Ministerium für Wirtschaft, Verkehr, Landwirtschaft und Weinbau stattgefunden. Es wurde eine datenschutzrechtliche Bewertung denkbarer Verfahrensgestaltungen vorgenommen.

In der Diskussion stehen zwei Varianten, wobei nach der ersten (lediglich) geplant ist, dass z. B. Autohäuser unter Benutzung eines Passwortes die Zulassungsdaten in das EDV-System der Behörde eingeben können. Nach dortiger Datenaufbereitung könnten dann die Unterlagen für die Zulassung zu einem vereinbarten Zeitpunkt bei der Behörde abgeholt werden.

Im Vergleich hierzu gehen die Planungen im Bereich der zweiten Variante wesentlich weiter, indem der gesamte Zulassungsvorgang letztlich auf Autohändler verlagert und der Zulassungsstelle nur noch eine Art Registrierfunktion belassen werden soll. In diesem Zusammenhang würden die Autohäuser als beliehene Unternehmer handeln, die im Rahmen des Zulassungsvorgangs für die Aufnahme des Antrags und die Kontrolle der Halterpersonalien, das Bedrucken, die Bestempelung und Aushändigung der Fahrzeugpapiere, die Beschaffung und Plakettierung der Kennzeichen und die Kontrolle der Versicherungsbestätigungen zuständig wären. Dazu wäre erforderlich, jedem beliehenen Autohaus Blanko-Fahrzeugschein-Vordrucke, Dienststempel und Prüfplaketten zu überlassen. Nach entsprechender Bearbeitung würde dann der Händler die Bestätigung des Halters über die Aushändigung der Fahrzeugpapiere und die Versicherungsbestätigung an die Zulassungsstelle übersenden, die diese Unterlagen lediglich noch verwaltet. Selbst die Zulassungsgebühr würde der Händler direkt beim Kunden erheben.

Die Vorgehensweise bei der ersten Variante – also die Datenspeicherung durch Autohäuser direkt im EDV-Bereich der Behörde – wirft in rechtlicher Hinsicht kaum Probleme auf. § 23 StVZO steht einer Zulassung über Internet nach überwiegender Auffassung der Landesbeauftragten für den Datenschutz nicht entgegen, wenn eine entsprechende technisch-organisatorische Konzeption Missbrauchsmöglichkeiten verhindert. So ist es nach allgemeiner Lebenserfahrung durchaus üblich, dass der Halter eines Kraftfahrzeugs das Autohaus, bei dem er das Fahrzeug erworben hat, beauftragt, die Zulassungsformalitäten für ihn zu erledigen. Ein Unterschied zur gegenwärtigen Praxis liegt nur darin, dass die Mitarbeiter der Autohäuser nicht mehr persönlich bei der Zulassungsstelle erscheinen müssen, um dort die für den Verwaltungsvorgang notwendigen Angaben zu machen, sondern sie übermitteln diese Daten per Internet. Allerdings muss für die Halter auch weiterhin die Möglichkeit bestehen, das Fahrzeug selbst bei der Zulassungsstelle anzumelden.

Aus technisch-organisatorischer Sicht sollten folgende Anforderungen gestellt werden:

- Das Eintragen von Antragsdaten in den Echtdatenbestand der Zulassungsbehörden sollte nicht zugelassen werden. Stattdessen sollten diese Daten durch die Autohäuser ausschließlich in jeweils unabhängig und abgeschottet vom Zulassungsbestand geführte Speicher eingegeben werden, die auch von den Daten anderer Autohäuser getrennt sind. Auch dürfen Dritte keine schreibenden oder lesenden Zugriffe auf andere Bereiche oder vorhandene Datensätze erhalten. Dieses müsste durch entsprechende Sicherungsmaßnahmen wie Zugangs- und Zugriffskontrolle sowie Protokollierungsverpflichtungen sichergestellt sein. Die so übermittelten Daten sollten erst im Rahmen der Bearbeitung durch die Zulassungsbehörden in den Gesamtbestand übernommen werden.

– Eine zweifelsfreie Identifizierung der Zugangsberechtigten ist sicherzustellen.

– Die Antragsdaten sind für die Übertragung auf den Verbindungswegen durch Verschlüsselung vor unbefugter Kenntnisnahme zu schützen.

– Durch die am Verfahren beteiligten Stellen sind geeignete Maßnahmen zu treffen, um die auf ihren EDV-Systemen gespeicherten personenbezogenen Daten vor unbefugtem Zugriff zu schützen. Alle sicherheitsrelevanten Ereignisse, insbesondere fehlerhafte Anmeldeversuche an die Behörden-EDV, sind zu protokollieren.

– Vor Aufnahme des Verfahrens haben die Zulassungsbehörden festzulegen, welche Bedingungen für die Teilnahme am Verfahren zu fordern sind, welche Stellen am Verfahren teilnehmen dürfen und auf welche Weise die Einhaltung der geforderten Sicherungsmaßnahmen zu prüfen ist.

Die in der zweiten Variante angedachte Übertragung von hoheitlichen Aufgaben auf Autohäuser – als beliehene Unternehmer zwecks Zulassung von Kraftfahrzeugen über das Internet – ist gegenwärtig mangels Rechtsgrundlage unzulässig. Unabhängig davon wäre eine solche Vorgehensweise auch datenschutzrechtlich höchst problematisch. Denn die Autohäuser müssten die Daten der Fahrzeughalter nicht nur weitergeben, sondern auch vor Ort speichern. Es würde damit eine Vielzahl von privaten speichernden Stellen entstehen, die kaum zu überblicken und zu kontrollieren wären. Die Zulassungsstellen haben Zugriff auf die Daten des KBA. Es stellt sich daher die Frage, ob dieser Zugriff auch den Autohäusern gewährt werden müsste mit der Folge, dass sie einen Zugriff auf sämtliche in der Bundesrepublik zugelassenen Kraftfahrzeuge und ihre Halter hätten. Um einen Datenmissbrauch möglichst auszuschließen, müsste eine Art Zuverlässigkeitsprüfung der Inhaber von Autohäusern und ihrer Angestellten durchgeführt werden (wie z. B. bei der Erteilung von Erlaubnissen im Gewerbe- oder Waffenrecht). Das Beispiel der Beleihung von Autohäusern könnte auch in anderen Bereichen, die ein Massengeschäft darstellen (beispielsweise Einwohnermeldewesen, Gewerbeanmeldung) „Schule machen“. Dies würde bedeuten, dass mit der Zeit ein unübersehbares Netz privater speichender Stellen entstehen würde. Abgesehen vom Problem der Kontrolle dieser Stellen, wäre es für den Betroffenen kaum noch zu überschauen, wer über ihn wann wo welche Daten gespeichert hat und was mit diesen Daten geschieht.

Der LfD wird die weitere Entwicklung in diesem Bereich aufmerksam beobachten.

14.9 Halteranfragen von Privaten

Häufig beklagen Bürgerinnen und Bürger die Übermittlung ihrer personenbezogenen Daten an Private im Rahmen von Halteranfragen. Der LfD weist insoweit auf Folgendes hin:

Durch Gesetz zur Änderung des Straßenverkehrsgesetzes vom 28. Januar 1987 wurden die Vorschriften der §§ 30 a bis 47 StVG eingefügt. Während § 30 a den Abruf von Daten aus dem Verkehrszentralregister im automatisierten Verfahren regelt, enthalten die §§ 31 bis 47 Vorschriften über die Fahrzeugregister, die Erhebung von Fahrzeug- und Halterdaten sowie deren Übermittlung. Zur Entlastung des Gesetzes blieben bestimmte Gegenstände einer Regelung durch Rechtsverordnung vorbehalten, für deren Erlass § 47 Abs. 1 StVG die notwendige Ermächtigungsgrundlage enthält. Darauf beruht die Fahrzeugregisterverordnung, die detaillierte Regelungen über Erhebung und Speicherung von Fahrzeug- und Halterdaten im zentralen und örtlichen Fahrzeugregister sowie über deren Übermittlungen enthält.

Nach der Regelung in § 39 StVG dürfen Auskünfte aus dem Halterregister der Kfz-Zulassungsstelle auch an Private erteilt werden, wenn der Anfragende einen Rechtsanspruch geltend macht, der im Zusammenhang mit der Teilnahme am Straßenverkehr steht. Auch der ruhende Verkehr ist Teil des Begriffs „Straßenverkehr.“ Ob der Anspruch letztlich durchsetzbar sein wird, ist für die Auskunftserteilung unerheblich.

14.10 Erteilung der Betriebserlaubnis und Ausstellung eines neuen Fahrzeugscheins durch den TÜV bei Änderungen an Fahrzeugen – Modellversuch in ausgewählten Zulassungsbezirken

Bei technischen Änderungen an Kraftfahrzeugen, durch die die Betriebserlaubnis erlischt, muss der Halter das Fahrzeug nach den Vorschriften der StVZO zunächst dem TÜV zur Begutachtung vorstellen und anschließend bei der Zulassungsstelle eine neue Betriebserlaubnis beantragen. Um dem Bürger den Weg zur Zulassungsstelle zu ersparen, wird auf Initiative des Ministeriums für Wirtschaft, Verkehr, Landwirtschaft und Weinbau in einem Modellversuch ein anderes bürgerfreundlicheres Verfahren erprobt. Der TÜV führt hier nicht nur die Begutachtung durch, sondern trägt gleichzeitig – sofern der Halter dies wünscht – die Änderungen in den Fahrzeugbrief ein, stellt einen neuen Fahrzeugschein aus und erteilt die erforderliche Betriebserlaubnis. Zu diesem Zweck hat der TÜV über eine EDV-Standleitung zu den betreffenden Zulassungsstellen die Möglichkeit, auf die dort gespeicherten Daten zuzugreifen, soweit sie auch im Fahrzeugschein, der ohnehin bei der Begutachtung des Fahrzeugs dem TÜV-Sachverständigen vorzulegen ist, enthalten sind. Auf weitere personenbezogene Daten hat der TÜV keine Zugriffsmöglichkeiten. Ist z. B. eine Auskunftssperre zu dem Fahrzeug angeordnet oder liegt eine Anzeige über eine Adressänderung, eine Mängel- oder Veräußerungsanzeige oder eine Meldung über das Erlöschen der Versicherung oder die Nichtentrichtung der Kfz-Steuer bei der Zulassungsstelle vor, so kann der TÜV-Sachverständige nicht auf deren Daten zugreifen und muss den Halter wegen der Änderung der Fahrzeugpapiere und der Erteilung der Betriebserlaubnis an die Zulassungsstelle verweisen.

Aus datenschutzrechtlicher Sicht bestehen nach dem derzeitigen Informationsstand gegen die genannte Datenverarbeitung keine grundsätzlichen Bedenken, da der Zugriff auf die personenbezogenen Daten im örtlichen Fahrzeugregister nur mit Einwilligung der Betroffenen erfolgt und die technische Prüfstelle lediglich auf jene personenbezogenen Daten Zugriff erhält, die zur Erfüllung der Aufgabe erforderlich sind. Des Weiteren sind insbesondere im Hinblick auf die in § 7 Abs. 2 Nr. 4 LDSG erwähnten technischen und organisatorischen Maßnahmen Vorkehrungen zum Schutz der Abfragestationen und -wege (Schutz der Leitungen, Identifikationsmaßnahmen) zu treffen sowie die Protokollierung der Datenzugriffe und der festgestellten Zugriffsverfehlungen vorzusehen. In diesem Zusammenhang ist auch § 36 Abs. 6 StVG zu beachten.

14.11 Tilgung von Datenspeicherungen in Führerscheinakten

Den LfD erreichen immer wieder Anfragen von Betroffenen, die wissen möchten, welche früheren Straftaten im Zusammenhang mit der Neuerteilung einer entzogenen Fahrerlaubnis verwertet werden dürfen.

Während des Berichtszeitraums hat sich die Rechtslage geändert. Bis zum 31. Dezember 1998 bestand folgende Rechtslage: Nach § 52 Abs. 2 BZRG galt das Verwertungsverbot des § 51 Abs. 1 BZRG nicht in Verfahren zur Erteilung oder Entziehung einer Fahrerlaubnis. Vom Verwertungsverbot waren alle strafgerichtlichen Verurteilungen ausgenommen, die in das Verkehrszentralregister einzutragen waren. In das Verkehrszentralregister waren rechtskräftige Entscheidungen der Strafgerichte, soweit sie wegen einer im Zusammenhang mit der Teilnahme am Straßenverkehr begangenen rechtswidrigen Tat auf Strafe oder andere Maßnahmen erkannten oder einen Schuldspruch enthielten, einzutragen. Nach der gesetzlichen Regelung bestand keine feste zeitliche Grenze für eine Verwertbarkeit länger zurückliegender Verkehrsstraftaten. Inwieweit aber auch nach § 52 Abs. 2 BZRG der Verwertung getilgter Verkehrsstraftaten Grenzen gesetzt waren, hatte die Rechtsprechung ausdrücklich offen gelassen, also keinen Anlass gesehen, in grundsätzlicher Weise etwa bestehende zeitliche Grenzen für eine Verwertbarkeit lange zurückliegender Zuwiderhandlungen aufzuzeigen. So konnten ggf. auch weit in der Vergangenheit liegende, bereits getilgte Straftaten berücksichtigt werden. Aus der Praxis der Verwaltungsbehörden war bekannt, dass im Bundeszentralregister getilgte Eintragungen in Fahrerlaubnisverfahren in der Regel berücksichtigt wurden, wenn eine Tat nicht länger als zehn Jahre zurücklag. In Einzelfällen wurden aber auch noch weitaus länger zurückliegende Taten einbezogen, um ein Gesamtbild der charakterlichen Haltung im Straßenverkehr zu gewinnen. In diesem Zusammenhang waren auch die Verfahrenshinweise des Ministeriums für Wirtschaft, Verkehr, Landwirtschaft und Weinbau vom 10. Mai 1995 (Az.: 8088-125/01/01) von Bedeutung. Für die Fahrerlaubnisbehörden bedeutete dies, dass Verurteilungen, die in das Verkehrszentralregister einzutragen waren, weiterhin in den Führerscheinakten verblieben und auch über einen Zeitraum von mehr als zehn Jahren aufzubewahren und in die Würdigung der Gesamtpersönlichkeit mit einzubeziehen waren. Dies schloss die Übersendung jener Vorgänge an die Untersuchungsstellen ein.

Seit dem 1. Januar 1999 gelten neue Regelungen: Nunmehr unterliegen Entscheidungen (z. B. Urteile) nach Ablauf der für das Verkehrszentralregister geltenden Tilgungsfrist einem gesetzlichen Verwertungsverbot; die bisher unbefristete Verwertungsmöglichkeit nach § 52 BZRG wurde abgeschafft. Damit dürfen die Tat und die Entscheidung dem Betroffenen nach der Tilgung im Verkehrszentralregister im Verfahren über die Erteilung oder Entziehung einer Fahrerlaubnis nicht mehr vorgehalten werden (zu den Einzelheiten der Neuregelung vgl. Tz. 14.12).

14.12 Gesetz zur Änderung des Straßenverkehrsgesetzes und anderer Gesetze

Über den Stand des Gesetzgebungsverfahrens hat der LfD im 16. Tb. unter Tz. 14.6 berichtet. Nunmehr ist das Gesetz zur Änderung des Straßenverkehrsgesetzes und anderer Gesetze vom 24. April 1998 (BGBl. I, 747) zum 1. Januar 1999 in Kraft getreten. Die Richtlinie des Rates der Europäischen Union vom 29. Juli 1991 über den Führerschein (2. EG-Führerscheinrichtlinie 91/439/EWG; ABl. EG-Nr. L 237, 1) ist damit – wenn auch verspätet – umgesetzt worden. Der Gesetzgeber hat sich jedoch nicht auf die Harmonisierung des deutschen mit dem europäischen Fahrerlaubnisrecht beschränkt, sondern hat die Anpassungspflicht zum Anlass genommen, das bisherige deutsche Verkehrszulassungsrecht grundlegend zu überarbeiten.

Unter datenschutzrechtlichen Gesichtspunkten sind folgende Änderungen bedeutsam:

– Ab dem 1. Januar 1999 wird neben den örtlichen Fahrerlaubnisregistern auch ein Zentrales Fahrerlaubnisregister beim KBA geführt. Örtliche Fahrerlaubnisregister dürfen nur noch bis zum 31. Dezember 2005 geführt werden. Da alle Fahrerlaubnisinhaber gespeichert werden, handelt es sich um ein Register mit etwa 50 Millionen Datensätzen. Nur die unveränderbaren Personalien und Führerscheindaten der Betroffenen werden erfasst, die Anschriften also nicht gespeichert. Befürchtungen, die Einführung des Zentralen Fahrerlaubnisregisters führe zu einem bundesweiten Melderegister von Personen mit Führerschein, sind damit ausgeräumt.

– Die Online-Abrufmöglichkeiten wurden ausgeweitet. Bislang durften die Abrufprotokolle aus dem Verkehrszentralregister und dem Zentralen Fahrzeugregister nur für Zwecke der Datenschutzkontrolle genutzt werden. Nunmehr wird die Nutzung der Protokolldaten über Abrufe aus dem Verkehrszentralregister, dem Zentralen Fahrzeugregister und dem Zentralen Fahrerlaubnisregister auch zur Aufklärung oder Verhütung von schwer wiegenden Straftaten gegen Leib, Leben und Freiheit einer Person zugelassen. Die Aufbewahrungsfrist der Protokolldaten wurde von drei auf sechs Monate verlängert (§§ 30 a Abs. 3, 36 Abs. 6, 53 Abs. 3 StVG).

– Es ist eine unentgeltliche Auskunft über die eigenen Daten aus dem Verkehrszentralregister (§ 30 Abs. 8 StVG) und dem Fahrerlaubnisregister (§ 58 StVG) vorgesehen.

– Für den Umgang mit Führerscheinakten sind nunmehr gesetzliche Festlegungen getroffen worden. Gutachten, Gesundheitszeugnisse, Registerauskünfte und Führungszeugnisse sind nunmehr nach spätestens zehn Jahren zu vernichten, es sei denn, die Unterlagen stehen im Zusammenhang mit einer Eintragung im Verkehrszentralregister oder im Zentralen Fahrerlaubnisregister (§ 2 Abs. 9 StVG). Unterlagen in „Altakten“ müssen erst dann vernichtet werden, wenn die Fahrerlaubnisbehörde aus anderem Anlass mit dem Vorgang befasst ist. Gemäß der Regelung in § 65 Abs. 1 StVG muss die Überprüfung aller Führerscheinakten 15 Jahre nach In-Kraft-Treten des Gesetzes – zum 1. Januar 2014 – erfolgt sein.

– In § 52 Abs. 2 BZRG wurde eine Harmonisierung der Verwertungsregelungen unter Beachtung der Verwertungsfristen der §§ 28 bis 30 b StVG vorgenommen. In Verfahren, die die Erteilung oder die Entziehung einer Fahrerlaubnis zum Gegenstand hatten, galt bisher eine unbefristete Verwertungsmöglichkeit (s. o., Tz. 14.11), selbst wenn die Eintragungen sowohl im Bundeszentralregister als auch im Verkehrszentralregister getilgt waren. Die bislang mögliche lebenslange Verwendung von Informationen über Entscheidungen in diesen beiden Registern ist damit entfallen. Nunmehr dürfen die Tat und die Entscheidung den Betroffenen nach der Tilgung in den Registern im Verfahren über die Erteilung oder Entziehung der Fahrerlaubnis nicht mehr vorgehalten werden.

14.13 Die Fahrerlaubnis-Verordnung und das Problem mit den Führerscheinakten

Nach dem Ergebnis örtlicher Feststellungen bei mehreren Führerscheinstellen hat sich die Führung von Führerscheinakten als ein besonderes datenschutzrechtliches Problem erwiesen. Aus der Sicht des Datenschutzes war die bisherige Praxis im Bereich der Beibringung von Gutachten amtlich anerkannter medizinisch-psychologischer Untersuchungsstellen unzureichend. Häufig wurde die komplette Akte an den Gutachter weitergeleitet, auch wenn sich in der Akte teilweise jahrzehntealte Unterlagen befanden, die für die antragstellende Person nachteilige Auswirkungen haben konnten.

Die Fahrerlaubnis-Verordnung vom 18. August 1998 ist am 1. Januar 1999 in Kraft getreten (BGBl. I, 2214). Sie regelt das Verfahren über die Erteilung und Entziehung einer Fahrerlaubnis aufgrund der §§ 6 und 6 a StVG. Für einige Bereiche hat sich mit dieser Verordnung aus datenschutzrechtlicher Sicht eine Verbesserung im Verhältnis zur früheren Rechtslage ergeben. Denn bislang waren wichtige Rechtsbereiche lediglich in Form von Verwaltungsvorschriften geregelt (z. B. die Eignungsrichtlinien vom 1. Dezember 1982 zu § 12 StVZO a. F.). Es sind allerdings unter datenschutzrechtlichen Gesichtspunkten auch problematische Regelungen getroffen worden.

Aufgrund eines Beschlusses des Bundesrates wurden in der Verordnung nämlich Änderungen vorgenommen, die bedenklich sind. So ist nicht mehr die im Regierungsentwurf vorgesehene Regelung enthalten, dass der Betroffene die Fahrerlaubnisunterlagen vor Übersendung an eine Gutachterstelle einsehen kann. Dadurch sollte deutlich gemacht werden, dass die Fahrerlaubnisbehörde als Herrin des Verfahrens zwar bestimmt, welche Unterlagen für die Begutachtung zur Ausräumung von Zweifeln übersandt werden müssen, der Betroffene hierüber aber unterrichtet wird, damit er über die Verwendung seiner Daten informiert ist.

Weiterhin enthält die Fahrerlaubnisverordnung nunmehr in § 11 Abs. 6 Satz 4 die Regelung, dass die Fahrerlaubnisbehörde der untersuchenden Stelle die vollständigen Unterlagen übersendet. Der Regierungsentwurf hielt stattdessen eine Übermittlung der erforderlichen Unterlagen für ausreichend. In diesem Zusammenhang ist darauf aufmerksam zu machen, dass der Verordnungsgeber den Umfang der zu übermittelnden Daten nicht erweitern kann, wenn der Gesetzgeber in § 2 Abs. 14 Satz 1 StVG die Übersendung auf die für die Aufgabenerfüllung benötigten Daten beschränkt. So hat die Fahrerlaubnisbehörde als Herrin des Verfahrens zu entscheiden, welche Zweifel an der Eignung auszuräumen sind, und kann bei dieser Ermessensentscheidung auch beurteilen, welche aktenkundigen Unterlagen für die Begutachtung erforderlich sind.

Hier sind nach Auffassung des LfD klare gesetzliche Vorgaben nur unzureichend umgesetzt worden. Anlässlich dieser Entwicklung wurde mit dem Ministerium für Wirtschaft, Verkehr, Landwirtschaft und Weinbau Kontakt aufgenommen und für die Sichtweise des Datenschutzes geworben. Das Ergebnis der Erörterung ist erfreulich. Es wurde u. a. vereinbart, dass die Betroffenen regelmäßig auf ihre Akteneinsichtsrechte vor Übersendung der Fahrerlaubnisunterlagen an eine Untersuchungsstelle oder einen Gutachter hingewiesen werden. Außerdem besteht Übereinstimmung dahin gehend, dass lediglich die erforderlichen Unterlagen übersendet werden sollen. Entsprechende Verfahrenshinweise sind vorgesehen.

15. Landwirtschaft, Weinbau und Forsten

15.1 Datei der Rindfleischerzeuger zur Bekämpfung von BSE

Eine der Maßnahmen zur Bekämpfung von BSE und zur Marktberuhigung ist, die Herkunft von Rindern eindeutig zu dokumentieren. Zu diesem Zweck wird in Bayern im Auftrag aller Länder eine zentrale Datenbank geführt. Neben den tierbezogenen Daten werden auch Namen und Anschriften der bisherigen Tierhalter bis zum Zeitpunkt der Übernahme des Tieres durch den Schlachthof festgehalten. Es ist angestrebt, etikettiertes Fleisch von der Ladentheke bis zum Mast- und Geburtsbetrieb des Rindes zurückverfolgen zu können.

In diesem Zusammenhang ist von datenschutzrechtlicher Bedeutung, ob der Endverbraucher Auskunft darüber verlangen kann, von welchen Tierhaltern das von ihm erworbene Fleisch stammt, ob der Schlachthof darüber Auskunft verlangen darf, woher das zu schlachtende Tier stammt und ob der Erwerber eines Rindes Auskunft über die Abstammung verlangen kann.

Rechtsgrundlage zur Führung der oben angesprochenen Datei und zur Beantwortung dieser Fragen ist die EG-Verordnung Nr. 520/97, wonach die zuständigen Behörden der Mitgliedstaaten eine elektronische Datenbank gem. den Artikeln 14 und 18 der Richtlinie 97/12 EG im Rahmen eines Überwachungsnetzes erstellen müssen. Dort ist auch geregelt, welche Daten die Datenbank mindestens enthalten und welche Angaben diese Datenbank liefern muss. Als Hauptziele des Systems von Überwachungsnetzen sind genannt:

- die amtliche Qualifikation der Betriebe,
- die Beibehaltung der Qualifikation durch Inspektion,
- die Sammlung epidemiologischer Daten und
- die Überwachung von Krankheiten.

Die zuständige nationale Behörde legt die Verpflichtungen und Rechte jedes an dem System Beteiligten fest.

Eine Antwort auf die oben gestellten Fragen ergibt sich aus den EG-Regelungen allerdings unmittelbar nicht. Aus nationalem Recht (dem Rindfleischetikettierungsgesetz) folgt, dass die Inhaber von Etikettiersystemen und daran beteiligte Unternehmen die Tier- und Tierhalterdaten erheben, speichern und nutzen können, wenn dies zur Rückverfolgung der Herkunft eines Tieres erforderlich ist. Sie erteilen den an diesem System beteiligten Unternehmen Auskunft über die Tier- und Tierhalterdaten, soweit dies für die Feststellung der Herkunft eines Rindes oder zum Schutz des Verbrauchers vor Täuschung erforderlich ist. Soweit es dieser Zweck erfordert, erteilen sie auch einem Verbraucher oder einer Verbraucherorganisation Auskünfte über diese Daten. Um den Zweck dieser gesamten Regelwerke zu erreichen, nämlich das Vertrauen der Verbraucher in die Unbedenklichkeit des Fleischverzehrs zu stärken, ist es auch nötig, dass der Verbraucher ohne größeren Aufwand die Herkunft des erworbenen Fleisches in Erfahrung bringen kann. Diesem Zweck entspricht es, wenn dem Verbraucher entsprechende Auskünfte auch unter Nutzung der Daten aus der zentralen Datei erteilt werden.

Aus der Sicht des LfD ergibt sich unter ergänzender Zugrundelegung der Regelung des § 16 LDSG, dass eine entsprechende Auskunftserteilung durch die zuständigen Behörden zulässig ist.

15.2 Datenverarbeitung zum Zweck der Bodenkunde und des Bodenschutzes

Besonders im Bereich der grundstücksbezogenen Informationen hat die automatisierte Datenverarbeitung erhebliche Fortschritte gemacht. Auch die staatlichen Lehr- und Versuchsanstalten für Landwirtschaft, Weinbau und Gartenbau sind in diesem Bereich engagiert. Eine dieser Lehr- und Versuchsanstalten hat im Zusammenhang mit der örtlich zuständigen städtischen Stadtentwässerung, der Verbandsgemeindeverwaltung, der Bezirksregierung und dem Maschinen- und Betriebshilfsring der Region ein Datennetz eingerichtet. Auf der Basis der Einwilligung der betroffenen Landwirte werden einmal erfasste grundstücksbezogene Informationen zu den unterschiedlichsten Zwecken zwischen diesen Stellen übermittelt.

Aus datenschutzrechtlicher Sicht war besonders auf eine umfassende Aufklärung der beteiligten Landwirte vor Erteilung der Einwilligung zu achten. Das Verfahren selbst wird derzeit noch vom LfD überprüft.

15.3 Behördliche Auskünfte und Akteneinsichtsrechte im Zusammenhang mit der Einräumung eines Wasserrechts

Im Zusammenhang mit einem Streit über das Bestehen eines Wasserrechts hat der Eigentümer eines Grundstücks Akteneinsicht in die wasserrechtlichen Akten bei der Bezirksregierung begehrt. Dabei kam es ihm insbesondere auch darauf an, Einsicht in einen Kaufvertrag zu nehmen, durch den verschiedene Nachbargrundstücke, die von dem Wasserrecht mitbetroffen waren, von einem Nachbarn an eine dritte Person veräußert worden sind. Die Bezirksregierung hat grundsätzlich das Interesse des Petenten an einer Akteneinsicht anerkannt und hat ihm auch Einsicht in den Kaufvertrag der Grundstücke gegeben. Sie hat allerdings sieben Seiten dieses Kaufvertrages entfernt. Diese Seiten haben allein den Kaufpreis und die Abwicklungsmodalitäten betroffen und waren aus der Sicht der Bezirksregierung für die wasserrechtlichen Fragen völlig unerheblich. Der Petent wollte Einsicht in den vollständigen Kaufvertrag haben.

Nach seiner Einschaltung wurden dem LfD durch die Bezirksregierung die vollständigen Unterlagen des Grundstückskaufs zur Verfügung gestellt. Er konnte sich davon überzeugen, dass die Bezirksregierung mit ihrer Wertung völlig zutreffend geurteilt hatte. Damit konnte dem Beschwerdeführer nicht zugestimmt werden. Er musste weiterhin auf die Einsicht in den vollständigen Kaufvertrag verzichten. Aus datenschutzrechtlicher Sicht war es geboten, nur die Informationen auch im Wege der Akteneinsicht offen zu legen, die zur Rechtsverfolgung des Beschwerdeführers sachdienlich waren. Die Informationen, die ihm vorenthalten worden sind, haben mit seinem Anliegen in keinem Zusammenhang gestanden.

Der LfD hat dementsprechend die Entscheidung der Bezirksregierung unterstützt und gegenüber dem Beschwerdeführer vertreten.

16. Statistik

16.1 Alle Jahre wieder – Fragen zur „Kleinen Volkszählung“ (Mikrozensus)

Den LfD erreichten wiederum zahlreiche Anfragen von Bürgerinnen und Bürgern, die beunruhigt waren und vielfältige Fragen zu dieser statistischen Erhebung hatten. Nachfolgend sind die am häufigsten hinterfragten Grundlagen und Zusammenhänge des Mikrozensus kurz dargestellt:

Etwa alle zehn Jahre wurde bisher eine Volks-, Berufs-, Gebäude-, Wohnungs- und Arbeitsstättenzählung durchgeführt, wobei von allen Bürgern Daten zur Person, Familie, Haushalt, Wohnung, Beruf und Arbeitsstätte erhoben wurden. Zur laufenden Fortschreibung und sachlichen Vertiefung der daraus gewonnenen Übersicht wird jährlich bei 1 % der Bevölkerung eine ergänzende Umfrage, der sog. Mikrozensus, durchgeführt. Die Antworten der nach einem mathematischen Zufallsverfahren ausgewählten Haushalte ermöglichen ein repräsentatives statistisches Gesamtbild der wirtschaftlichen und sozialen Lage aller Bevölkerungsgruppen. Die „Kleine Volkszählung“ wird seit 1957 auf gesetzlicher Grundlage durchgeführt. Seit 1996 ist die Befragung durch ein neues Mikrozensusgesetz geregelt, wobei das Fragenprogramm um einige aktuelle, gesellschaftspolitisch interessante Merkmale (z. B. Pflegeversicherung) erweitert wurde. Im Wesentlichen stellen die Interviewerinnen und Interviewer Fragen zu den Themen

- persönliche Merkmale (Alter, Staatsangehörigkeit, Schulbesuch);
- Erwerbstätigkeit, Beruf, Arbeitszeit;
- Arbeitssuche, Nichterwerbstätigkeit, berufliche Aus- und Fortbildung;
- Altersvorsorge, Unterhalt und Einkommen.

Hinsichtlich dieser Fragen sind die Betroffenen zur Auskunft verpflichtet.

Auf freiwilliger Basis werden außerdem Antworten, insbesondere zum Jahr der Eheschließung und zu den Themen „Wohn- und Lebensgemeinschaft“, „Pflegebedürftigkeit“ und „Gesundheit“ (z. B. Grippeimpfung, Rauchgewohnheiten) erbeten.

Die Erhebung statistischer Daten bei der Bevölkerung erfolgt zwar in der Regel mit Hilfe von Interviewern, um auch komplizierte Sachverhalte ermitteln zu können. Die Betroffenen haben jedoch das Recht, den Erhebungsbogen selbst auszufüllen und an das Statistische Landesamt zu senden. Eine Pflicht, den Interviewer in die Wohnung zu lassen und ihm zu antworten, besteht nicht.

Die Geheimhaltung der erhobenen Daten ist gesetzlich sichergestellt. Die Verletzung des Statistikgeheimnisses steht unter Strafe. Die Vorschriften zur Geheimhaltung bewirken, dass Einzelangaben über die persönlichen und sachlichen Verhältnisse des Betroffenen grundsätzlich nur für statistische Zwecke und nicht etwa für die Regelung von Einzelfällen in der Verwaltung verwendet werden dürfen. Nur ausnahmsweise dürfen Einzelangaben an andere Stellen weitergeleitet werden, wobei dies jedoch in der die Statistik anordnenden Rechtsvorschrift ausdrücklich zugelassen und in den Erhebungsvordrucken bekannt gegeben werden muss. Nicht der Geheimhaltung unterliegen die Angaben, wenn sie zusammengefasst und so aufbereitet sind, dass sie Rückschlüsse auf die einzelnen Auskunftgebenden nicht mehr zulassen.

16.2 Volkszählung light?

Für das Jahr 2001 ist eine erneute Volkszählung geplant. Dieses Großprojekt soll unionsweit durchgeführt werden. Nachdem die Europäische Union von einer verbindlichen EU-Verordnung abgerückt ist, stützen sich die Überlegungen zu einem Zensus im Jahre 2001 bislang auf eine unverbindliche EU-Leitlinie aus dem Jahr 1997 und den Wunsch der Innenminister, preiswerte Modelle für einen registergestützten Zensus unter Berücksichtigung des Informationsbedarfs der Länder und Gemeinden zu entwickeln. Hier ist festzustellen, dass für die Bundesrepublik Deutschland ein Methodenwechsel weg von den als Primärerhebungen durchgeführten bisherigen Zensen hin zur registergestützten Zählung vor der Tür steht. Es handelt sich also um ein Verfahren, das vornehmlich vorhandene Datenbestände auswertet. Für diesen Methodenwechsel sind insbesondere finanzielle Gründe verantwortlich; denn die Kosten einer Primärerhebung würden nach Schätzungen mehr als 2 Milliarden DM betragen.

Gegenwärtig werden zwei Modelle diskutiert: das sog. Bundesmodell und das Ländermodell. Das vom Bund vorgeschlagene Modell stützt sich im Wesentlichen auf drei Quellen, nämlich die Einwohnermelderegister, die Erwerbstätigkeitsstatistiken (z. B. Beschäftigtendatei und Arbeitslosendatei der Bundesanstalt für Arbeit) und auf detaillierte Angaben des Mikrozensus, der regelmäßig bei 1 % der Bevölkerung durchgeführt wird und ausführliche Informationen über Haushalte, Wohnungen und Gebäude sowie den Bildungsstand abfragt. Das Bundesmodell befriedigt zwar die Wünsche der Europäischen Union, liefert aber nur bedingt Angaben auf Kreis- oder Gemeindeebene.

Das von den Amtsleitern der statistischen Ämter favorisierte Ländermodell sieht als zusätzlichen Bestandteil gegenüber dem Bundesmodell eine primärstatistische Gebäude- und Wohnungszählung vor. Darüber hinaus ist eine Ergänzungsstichprobe im Erwerbsbereich geplant. Die Kosten des Ländermodells liegen nach ersten Schätzungen zwar deutlich unter denen einer herkömmlichen Volkszählung, sie wären aber wesentlich höher als bei einer Erhebung nach dem Bundesmodell.

Der LfD hat bislang keine rechtliche Wertung vorgenommen, da die Planungen gegenwärtig noch nicht abgeschlossen sind und sich vieles noch in der Diskussion befindet.

Datenschutzrechtlich bedenklich wäre die in beiden Modellen geplante Zusammenführung der für notwendig gehaltenen Daten aus allen Einwohnermelderegistern der Bundesrepublik im Statistischen Bundesamt. Bisher wurden im Rahmen der Statistik noch nie die personenbezogenen Daten aller Bürger der Bundesrepublik im Statistischen Bundesamt gleichzeitig in einem Verfahren verarbeitet. Bei der Volkszählung 1987 und der Gebäude- und Wohnungszählung 1995 gelangten die personenbezogenen Daten lediglich bis zum jeweils zuständigen Statistischen Landesamt. Insoweit würde mit dem neuen Verfahren auch ein Präzedenzfall geschaffen. Ob ein derartiger immenser Datentransfer durch das damit verfolgte Ziel gerechtfertigt, ob er also verhältnismäßig wäre, erscheint fraglich. Es bedarf aus der Sicht des Datenschutzes noch vertiefter Prüfung, ob nicht eine Bereinigung der Mehrfachmeldungen auf anderem, weniger einschneidendem Wege erreicht werden kann oder ob auf sie nicht ganz verzichtet und die dann entstehende Unschärfe hingenommen werden sollte.

Anlässlich einer Sitzung des Statistischen Landesausschusses wies der LfD auf die Probleme in diesem Bereich hin.

16.3 Die Volkszählung und das Melderegister

Im Zusammenhang mit der geplanten Volkszählung wurde auf verschiedenen Ebenen die Frage erörtert, wie die Qualität der Melderegister, die die Datenbasis bilden sollen, verbessert werden kann. Im Vordergrund stand dabei die Zulässigkeit der Datenübermittlung an die Meldebehörden durch Behörden, die erkennen, dass Adressdaten falsch sind.

Der LfD vertrat hierzu die Auffassung, dass rheinland-pfälzische Behörden die Datenübermittlung an die Meldebehörden auf § 14 Abs. 1 i. V. m. § 12 Abs. 4 Nr. 3 LDSG stützen können, es sei denn, dass vorrangige bereichsspezifische Rechtsvorschriften entgegenstehen. Hierzu zählen z. B. Rechtsvorschriften aus dem Bereich der Statistik, des Sozialdatenschutzes und des Abgabenrechts.

Als weitere Maßnahme zur Verbesserung der Qualität der Melderegister wurde erwogen, Städten und Gemeinden zu empfehlen, den Inhabern von Nebenwohnungen mitzuteilen, dass sie nicht in das Wählerverzeichnis aufgenommen werden, es sei denn, dass sie die Nebenwohnung inzwischen als Hauptwohnung nutzen und das Melderegister auf ihren Antrag entsprechend berichtigt wird (negative Wahlbenachrichtigung). Diese Vorgehensweise ist datenschutzrechtlich problematisch, denn eine solche negative Wahlbenachrichtigung würde in erster Linie dazu dienen, Daten zur Berichtigung des Melderegisters zu erheben. Beim Betroffenen würde indessen der Eindruck erweckt, dass die negative Wahlbenachrichtigung wahlrechtliche Gründe hat. Die Bezeichnung „negative Wahlbenachrichtigung“ und die Verknüpfung der Überprüfung von Nebenwohnungen mit dem Wahlrecht wären irreführend. Die Betroffenen müssten über den eigentlichen Zweck der „negativen Wahlbenachrichtigung“ in geeigneter Weise informiert werden (§ 12 Abs. 2 LDSG).

17. Personaldatenverarbeitung

17.1 Mitteilung von Gehaltspfändungen durch die Zentrale Besoldungs- und Versorgungsstelle an die personalverwaltende Stelle

Die in Rheinland-Pfalz bestehende Praxis, Gehaltspfändungen uneingeschränkt der personalverwaltenden Stelle mitzuteilen, wurde wiederholt zwischen dem LfD einerseits sowie dem Ministerium der Finanzen und der ZBV andererseits erörtert. Die Datenschutzkommission – und nach dem Übergang der Kontrollzuständigkeit im Jahre 1991 – auch der LfD traten für eine Regelung ein, die Bagatellfälle von der Mitteilungspflicht ausnimmt. Das Ministerium und die ZBV vertreten die Auffassung, dass es Bagatellfälle, die von der Mitteilungspflicht ausgenommen werden könnten, nicht gebe (vgl. 10. Tb. der DSK, Tz. 14.5).

Im Rahmen der Erörterung dieser Thematik mit den Datenschutzkontrollbehörden anderer Länder wurde bekannt, dass Verfahrensweisen eingeführt sind, die den Interessen der Bediensteten unter Wahrung der Interessen der personalverwaltenden Stellen besser Rechnung tragen, als dies in Rheinland-Pfalz zurzeit der Fall ist. So hat das Finanzministerium Baden-Württemberg verfügt, dass die personalverwaltende Stelle nur dann zu unterrichten ist, wenn die einem Pfändungs- und Überweisungsbeschluss zugrunde liegende Forderung die regelmäßigen monatlichen Bruttobezüge (ohne Kindergeld) eines vollen Kalendermonats, mindestens jedoch 750,– DM überschreitet. Eine weitere Einschränkung betrifft Pfändungen wegen Unterhalt. Die Beschränkungen gelten nicht, wenn Pfändungsverfügungen oder Abtretungen innerhalb bestimmter Zeiträume häufiger vorgelegt werden. Andere, aber gleichfalls beschränkende Regelungen hat das Finanzministerium Mecklenburg-Vorpommern getroffen. Der LfD informierte das Finanzministerium und bat, die früher vertretene Auffassung vor dem Hintergrund dieser Entwicklung zu überprüfen.

Das Ministerium teilte mit, dass aus seiner Sicht keine Veranlassung bestehe, die bisherige Verfahrensweise zu ändern. Die ZBV solle weiterhin jede Gehaltspfändung der personalverwaltenden Stelle mitteilen, ohne zuvor Betragsgrenzen oder Eingänge innerhalb bestimmter Zeiträume prüfen zu müssen. Im Rahmen des pflichtgemäßen Ermessens obliege der personalverwaltenden Stelle nach Würdigung des Einzelfalls die Entscheidung, ob und ggf. welche dienstrechtlichen Schritte bei Gehaltspfändungen zu ergreifen sind. Zur Gewährleistung eines reibungslosen Dienstablaufs und aus Fürsorgegründen könne der Dienstherr nicht früh genug auf eine geordnete Regelung der finanziellen Verhältnisse hinwirken. Insbesondere stelle sich gerade in der Finanzverwal-

tung in jedem Einzelfall die Frage, ob ein in finanziellen Schwierigkeiten befindlicher Bediensteter seinen konkreten Dienstposten weiterhin ausfüllen könne oder ob er nicht zur Vermeidung möglicher Unregelmäßigkeiten umzusetzen sei. Deshalb gebe es bei Pfändungsmaßnahmen keine Bagatellfälle. In gravierenden Fällen müssten auch disziplinarrechtliche Maßnahmen eingeleitet werden.

Der LfD sieht derzeit keine Möglichkeit, eine aus seiner Sicht angemessene Problemlösung durchzusetzen.

17.2 Gewinnung von Wahlhelfern

Die Gewinnung von Wahlhelfern bereitet in einzelnen Städten und Gemeinden wohl immer noch Schwierigkeiten. Im zeitlichen Umfeld von Wahlen häufen sich jedenfalls Eingaben und Anfragen beim LfD, die dieses Thema betreffen. Öffentlich Bedienstete beklagen sich, dass sie von ihrer Dienstbehörde als potentielle Wahlhelfer an die Wahlämter gemeldet werden, soweit dies nicht geschieht, beklagen die für die Durchführung von Wahlen zuständigen Behörden, dass die Erfüllung ihrer Aufgabe, die Wahlvorstände zu bestellen, über Gebühr erschwert werde.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat sich in einer Entschließung schon im Jahre 1995 wie folgt zu dem Thema geäußert (vgl. 15. Tb., Anlage 23): „Beschäftigtendaten dürfen nur auf freiwilliger Basis übermittelt werden, sofern nicht eine besondere Rechtsvorschrift die Übermittlung zulässt. Im Falle der Freiwilligkeit muss es den Beschäftigten möglich sein, selbst die Meldung unmittelbar gegenüber der Wahlbehörde abzugeben."

Eine Stadtverwaltung vertrat die Auffassung, dass die Vorschriften des Landesbeamtengesetzes über die Personalaktenführung und § 31 LDSG über die Datenverarbeitung bei Dienst- und Arbeitsverhältnissen als „besondere Rechtsvorschriften" i. S. der obigen Entschließung anzusehen seien.

Dem war Folgendes entgegenzuhalten:

Personalaktendaten von Beamten dürfen gem. § 102 Abs. 1 Satz 3 LBG 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 LBG sind gegeben.

Wenn weder eine Einwilligung der Beamten noch eine gesetzliche Übermittlungsbefugnis vorliegt, kommt eine Übermittlung der Personaldaten nur in Betracht, wenn dies zur Abwehr einer erheblichen Beeinträchtigung des Gemeinwohls oder der Schutz höherrangiger Interessen des Dritten die Auskunftserteilung erfordert (§ 102 d Abs. 2 LBG).

Für Personalaktendaten von Angestellten im öffentlichen Dienst enthält § 31 Abs. 1 LDSG eine ähnlich enge Zweckbindung.

Es ist allerdings zu berücksichtigen, dass § 31 Abs. 2 LDSG Datenübermittlungen an nichtöffentliche Stellen unter weiteren Bedingungen zulässt; für Datenübermittlungen an öffentliche Stellen gelten die dort genannten Voraussetzungen entsprechend, weil öffentliche Stellen in diesem Zusammenhang nicht schlechter als private Personen bzw. Stellen gestellt sein können. Als Rechtsgrundlage der Datenverarbeitung käme vorliegend § 31 Abs. 2 Nr. 5 LDSG analog in Betracht, wonach eine Übermittlung zulässig ist, soweit die empfangende Stelle ein rechtliches Interesse darlegt und überwiegende schutzwürdige Interessen der Betroffenen nicht entgegenstehen.

Auch unter Berücksichtigung dieser Regelung ist indessen eine Datenübermittlung zum Zwecke der Gewinnung von Wahlhelfern nicht zulässig, weil schutzwürdige Belange der Betroffenen entgegenstehen: Diese sind darin zu sehen, dass die Betroffenen aufgrund eines für die Auswahl rechtlich nicht maßgeblichen Kriteriums (der Eigenschaft als öffentlich Bediensteter) in die Personengruppe gelangen, aus der die Wahlhelfer ausgewählt werden sollen. Die Zugehörigkeit zum öffentlichen Dienst ist kein für die Bestellung zum Wahlhelfer maßgebliches Kriterium: Jeder Bürger, bei dem die formalen Voraussetzungen vorliegen und der keine Gründe der Unzumutbarkeit geltend machen kann, müsste für dieses Amt ebenso herangezogen werden können. Außerdem läge – wenn man auf das Kriterium der Verwaltungserfahrung abstellen würde, das in diesem Zusammenhang aber nicht maßgeblich sein kann – in diesem Vorgehen gegenüber den Bediensteten anderer Verwaltungen eine nicht gerechtfertigte Ungleichbehandlung.

Die Grundsätze der „Amtsträgertheorie" führen zu keinem anderen Ergebnis. Sie bezieht sich nur auf das Tätigwerden eines öffentlich Bediensteten in Ausübung einer amtlichen Tätigkeit gegenüber dem Bürger (vgl. 13. Tb., Tz. 17.3).

17.3 Telearbeit

Im 16. Tb., Tz. 21.7, wird das Thema Telearbeit unter dem Gesichtspunkt des technisch-organisatorischen Datenschutzes behandelt. Das Fazit: „Datenschutzrechtliche Gesichtspunkte stehen der Telearbeit im Verwaltungsbereich grundsätzlich nicht entgegen." Bei Berücksichtigung der im Einzelnen dargelegten Anforderungen ist dies nach wie vor richtig.

Ausgeklammert blieben bei dieser Einschätzung indessen inhaltliche Aspekte und die Frage, wie der Umstand zu bewerten ist, dass die Kontrollmöglichkeiten der Telearbeit gegenüber der „Normalarbeit" erheblich eingeschränkt sind.

Telearbeit kann nicht isoliert betrachtet werden. Sie ist eine Unterform der Heimarbeit – technikgestützte Heimarbeit – und ähnelt anderen datenschutzrelevanten Arbeitsformen, wie Auftragsdatenverarbeitung oder Outsourcing. Diese Arbeitsformen sind im Folgenden unter dem Begriff Auftragsverarbeitung zusammengefasst.

Die rechtlichen Unterschiede zwischen Heimarbeit und Auftragsdatenverarbeitung sind gering. Beide Formen beruhen auf vertraglichen Vereinbarungen – mögliche Ausnahme: Heimarbeit durch Beamte – und für beide Formen bestehen strafrechtliche Sanktionsmöglichkeiten (Heimarbeit: § 203 Abs. 2 StGB; Auftragsdatenverarbeitung: Verpflichtungsgesetz, Strafgesetzbuch). Die Strafbestimmungen des LDSG gelten für beide Verarbeitungsformen.

Beim technisch-organisatorischen Datenschutz bestehen indessen deutlichere Unterschiede. Während die Auftragsdatenverarbeitung beim Auftragnehmer in aller Regel in einem professionellen Umfeld durchgeführt wird, lässt sich dies bei der Heimarbeit nur schwer realisieren. Solche Unterschiede werden jedenfalls deutlich, wenn man die Transportrisiken oder die Abschottungsproblematik bei einem gleichzeitig für private und dienstliche Zwecke in der Wohnung genutzten PC betrachtet. Technische Verfahren, die bei der Auftragsverarbeitung angewandt werden – wie z. B. eine Verschlüsselung, die es dem Auftragnehmer unmöglich macht, Inhalte der Verarbeitung zur Kenntnis zu nehmen –, sind nur schwer auf die Heimarbeit zu übertragen. Die Kontrollmöglichkeiten sind bei der Heimarbeit gegenüber der Auftragsdatenverarbeitung eher eingeschränkt (Beispiel: nicht angemeldete Kontrollen).

Hieraus folgt, dass Heimarbeit – datenschutzrechtlich betrachtet – kein Minus gegenüber der Auftragsdatenverarbeitung darstellt, sondern als eine Arbeitsform anzusehen ist, die gleich hohe oder sogar höhere Risiken birgt. Es ist deshalb unumgänglich, Restriktionen, wie sie z. B. für die Auftragsverarbeitung durch Private existieren, auch für die Heimarbeit zu definieren. So sollte Heimarbeit nicht zugelassen werden, wenn überwiegende schutzwürdige Interessen, insbesondere Berufs- oder besondere Amtsgeheimnisse, entgegenstehen. Auch die Errichtung formaler Hürden, wie sie z. B. im SGB X für die Auftragsdatenverarbeitung existieren, sollte in Betracht gezogen werden.

Der LfD lehnt jedenfalls Heimarbeit bei der Verarbeitung von Sozial-, Statistik- oder Personaldaten grundsätzlich ab. Dies gilt insbesondere auch für die Verarbeitung medizinischer Daten. Eine große Fachklinik hat daher das Schreiben von Patientengutachten, welche Ärzte im Rahmen genehmigter Nebentätigkeit im Auftrag u. a. von Gerichten oder Kostenträgern erstellen, durch Mitarbeiter der Klinik in Heimarbeit untersagt (zur Arztbriefschreibung durch externe Schreibbüros vgl. 14. Tb., Tz. 10.4.2).

18. Datenschutz im kommunalen Bereich

18.1 Bürgerbüros und informationelle Gewaltenteilung

Zur rationellen Wahrnehmung von Verwaltungsaufgaben und mit der Zielvorgabe „Bürgerfreundlichkeit“ werden in den Kreisen, Städten und Gemeinden Bürgerbüros, Bürgerämter oder „Kundenzentren“ eingerichtet. Gemeinsam ist diesen Einrichtungen, dass Verwaltungsleistungen, die überwiegend den direkten Kontakt mit dem Bürger erfordern, in einer Organisationseinheit zusammengefasst werden. Der Bürger hat auf Seiten der Verwaltung nur einen Ansprechpartner („one face to the customer“); die zeitaufwendige Vorsprache in mehreren Ämtern (die sog. Ämterrallye) wird ihm erspart.

Diese Ziele haben auch vor dem Hintergrund datenschutzrechtlicher Überlegungen ein eigenständiges Gewicht. Der LfD hat stets die Auffassung vertreten, dass gegen Bürgerbüros und ähnliche Einrichtungen, deren Befugnisse darin bestehen, Rat suchende Bürger an die zuständigen Ämter innerhalb der Verwaltung oder an andere zuständige Behörden zu verweisen, Vorsprachetermine zu vermitteln und andere Serviceleistungen mit geringer Datenschutzrelevanz (z. B. Erteilung von Einwohnerparkberechtigungen, Beglaubigungen, Wahrnehmung der Funktion eines Konzert- und Theaterbüros) zu erbringen, keine Bedenken bestehen. Für unbedenklich hält er es auch, dass ein Bürgerbüro Vordrucke aushändigt oder Anträge entgegennimmt und diese an die zuständige Stelle innerhalb der Verwaltung zur Bearbeitung weiterleitet. Als Datenbasis für die Arbeit der Bürgerbüros sieht der LfD im Wesentlichen die Kataloge des § 3 Abs. 1 und 2 MG an. Grundsätzlich muss es aber den Bürgern freigestellt bleiben, ob sie die Dienste des Bürgerbüros in Anspruch zu nehmen oder sich unmittelbar an die in der Sache zuständigen Ämter der Stadtverwaltung wenden.

Die Bündelung von Funktionen in den Bürgerbüros hat freilich auch Grenzen. Das geltende Datenschutzrecht geht davon aus, dass funktional unterschiedliche Verwaltungsbereiche voneinander zu trennen sind und eine Weitergabe personenbezogener Daten von einem an den anderen Bereich sowie die Zweckänderung von Daten nur dann erfolgen, wenn dies gesetzlich zugelassen ist. Im Volkszählungsurteil hat das Bundesverfassungsgericht gefordert, dass organisatorische und verfahrensrechtliche Vorkehrungen getroffen werden, die der Gefahr einer Verletzung des Persönlichkeitsrechts entgegenwirken (BVerfGE 65, 1). In einer anderen Entscheidung hat es darauf hingewiesen, dass aus der Einheit der Gemeindeverwaltung keine informationelle Einheit folgt; der „Grundsatz der informationellen Gewaltenteilung gilt auch innerhalb der Gemeindeverwaltung“ (BVerfG 1. BVR 962/87, NJW 88, 959).

In der Erörterung mit den Befürwortern von Bürgerbüros wird deutlich, dass die datenschutzrechtlichen Grenzen von organisatorischen Veränderungen bisweilen nicht hinreichend gewürdigt werden. Man möchte möglichst die ganze Verwaltung zum Bürgerbüro machen und sieht sich daran eigentlich nur durch bauliche Gegebenheiten oder die Qualifikation von Sachbearbeitern gehindert.

Verschärft werden die Datenschutzprobleme durch die räumliche Situation, wenn mehrere Sachbearbeiter in „Großraumbüros“ gleichzeitig mehrere Bürger „bedienen“. Sind die Abstände gering und fehlt es an Sichtblenden und Schallschutzeinrichtungen, so ist nicht gewährleistet, dass gleichzeitig anwesende Bürger keine Kenntnis von Verwaltungsvorgängen erhalten, die andere betreffen, oder dass Bürger nicht Gespräche und Telefonate mithören.

Insbesondere diese für den Bürger unmittelbar erkennbaren Datenschutzmängel haben zur Folge, dass den LfD Eingaben erreichen, die diese Thematik betreffen.

Aber auch von Landkreisen, Städten und Gemeinden erhält er immer wieder Anfragen zu den datenschutzmäßigen Anforderungen an Bürgerbüros usw. Solche Anfragen wurden in der Vergangenheit jeweils einzelfallbezogen beantwortet.

Die kommunalen Spitzenverbände haben ihre Mitgliedsverwaltungen in einem Rundschreiben vom 24. November 1998 über die Rechtsauffassung des LfD informiert und gebeten, bei der Einrichtung von Bürgerbüros verstärkt auch auf die Gesichtspunkte des Datenschutzes Rücksicht zu nehmen. Ferner wurde auf die Beratungsaufgaben des LfD hingewiesen.

Örtliche Feststellungen in mehreren Verbandsgemeinden ergaben, dass die jeweils realisierte Aufgabenbündelung im Bürgerbüro die informationelle Trennung der verschiedenen Organisationseinheiten – noch – nicht in einem unvertretbaren Maße tangiert. Unter Datenschutzgesichtspunkten nicht vollständig zufrieden stellend war indessen die Raumsituation und hier speziell die Verbindung des Wartebereichs mit dem Bearbeitungsbereich. Es war darauf hinzuweisen, dass angesichts der geringen Distanz zwischen Wartenden und den nächstgelegenen Arbeitsplätzen Gespräche mitgehört werden können oder Informationen in anderer Weise Unbefugten zur Kenntnis gelangen. Es wurde empfohlen, dass entweder Wartebereiche aus den Großraumbüros ausgegliedert oder durch Schallschutz- und Sichtwände so abgeschottet werden, dass die unerwünschten Wirkungen nicht eintreten.

Häufig sind auch die räumlichen Entfernungen zwischen den Arbeitsplätzen gering. Es muss hier freilich berücksichtigt werden, dass ein bewusstes und zielgerichtetes Mithören Unbefugter, die sich selbst in der Interaktion mit Behördenbediensteten befinden, kaum möglich ist. In einzelnen Verwaltungen konnten durch das Aufstellen hochwachsender Pflanzen als Sichtschutz und durch teiltransparente Stellwände Verbesserungen erzielt werden.

Bürgerfreundlichkeit bedeutet auch, dass die Datenschutzinteressen ernst genommen werden. Bei der Einrichtung von Bürgerbüros wird der Stellenwert deutlich, den die Kommunen diesen Interessen beimessen.

18.2 Wahrung des Wahlgeheimnisses bei der Briefwahl

In den Tagen vor der Kommunalwahl häuften sich Eingaben, in denen Bürgerinnen und Bürger als Wahlberechtigte ihre Besorgnis zum Ausdruck brachten, dass das Wahlgeheimnis bei der Briefwahl gefährdet sei. Diese Besorgnis gründete sich darauf, dass aufgrund der Hinweise für die Behandlung der Wahlunterlagen der Stimmzettel nach dem Ausfüllen in einen unverschlossenen amtlichen Wahlumschlag gesteckt werden musste, der dann – zusammen mit dem Wahlschein – in einem verschlossenen Wahlbriefumschlag an die Gemeindeverwaltung zu übersenden war.

Die Betroffenen wurden darauf hingewiesen, dass die amtlichen verschlossenen Wahlbriefumschläge nach den Vorschriften der Kommunalwahlordnung erst am Tag der Wahl durch einen Wahlvorstand geöffnet werden dürfen. Bis dahin müssen sie sicher und verschlossen aufbewahrt werden. Bei der Öffnung am Tag der Wahl *sollen* nach § 5 der Kommunalwahlordnung alle Mitglieder des Wahlvorstandes (zwischen sechs und elf Personen) anwesend sein; es *müssen* mindestens fünf Mitglieder anwesend sein. Nach Abschluss der Wahlhandlung öffnet ein Mitglied des Wahlvorstands die Wahlbriefe einzeln und entnimmt ihnen den Wahlschein und den Wahlumschlag. Nach Prüfung der Wahlberechtigung entnimmt der Wahlvorsteher den Stimmzettel dem Wahlumschlag und legt ihn uneingesehen in gefaltetem Zustand in die Wahlurne. Erst wenn sich alle Stimmzettel der Briefwahl in der Wahlurne befinden, wird diese geöffnet und die Auszählung beginnt.

Eine Verletzung des Wahlgeheimnisses in diesem Verfahren durch Kenntnisnahme der Stimmzettel vor dem Einlegen in die Wahlurne wäre nur dann möglich, wenn die Mitglieder des Wahlvorstandes gemeinsam und einvernehmlich eine solche strafbare Handlung begehen würden. Bestünde dieser gemeinsame und einvernehmliche Handlungswille des Wahlvorstandes, könnte das Wahlgeheimnis auch in anderer Weise verletzt und das Wahlergebnis schwer wiegend manipuliert werden.

Dass der Wahlumschlag nach § 59 der Europawahlordnung zu verschließen ist, bietet keinen wesentlich stärkeren Schutz. Begreiflicherweise stoßen die unterschiedlichen Verfahrensweisen in der Öffentlichkeit aber auf Unverständnis. Eine Angleichung wäre auch aus der Sicht des Datenschutzes zu begrüßen, der freilich von der Problematik nur am Rande berührt ist.

18.3 Datenschutz und Volksbegehren

Datenschutzfragen in Zusammenhang mit der Durchführung von Volksbegehren sind immer wieder Gegenstand von Anfragen an den LfD. So beschwerte sich ein Petent über die Veröffentlichung seines Geburtsdatums im Eintragungsberechtigungsverzeichnis durch eine Verbandsgemeinde.

Der Gesetzgeber hat jedoch in den §§ 76 Abs. 2, 15 Abs. 2 LWO festgelegt, dass der Eintragungsberechtigte die Unkenntlichmachung des Tages seiner Geburt im Eintragungsberechtigungsverzeichnis während der Auslegungsfrist verlangen kann und sich damit für eine besondere Form der Widerspruchslösung entschieden. Diese gesetzliche Regelung ist auch aus der Sicht des Datenschutzes verhältnismäßig, denn sie berücksichtigt einerseits die schutzwürdigen Interessen von Betroffenen, gewährleistet aber andererseits die eindeutige Identifizierung der Vielzahl von Wahlberechtigten. Mit der Anschrift allein ist dies häufig nicht möglich.

Die Bekanntmachung der Verbandsgemeindeverwaltung entsprach somit den gesetzlichen Vorgaben und war datenschutzrechtlich nicht zu beanstanden.

In Bezug auf die Eintragungslisten von Volksbegehren hat der Landesgesetzgeber eine Änderung des Landeswahlgesetzes beschlossen, die aus der Sicht des Datenschutzes zu begrüßen ist: Geburtsdatum, Geburtsort und der Beruf sind im Zusammenhang mit der Unterschriftsleistung nicht mehr anzugeben (Landesgesetz vom 26. Oktober 1998, GVBl. S. 283). Damit wird der Datenschutz im Zusammenhang mit der Durchführung eines Volksbegehrens weiter verbessert.

18.4 Ausübung des Vorkaufsrechts

Eine Verbandsgemeinde fragte an, ob es zulässig sei, dass der Gemeinde zur Prüfung ihres Vorkaufsrechts nach § 24 Abs. 1 BauGB der gesamte notarielle Kaufvertrag übersandt wird.

Zum Zwecke der Entscheidung über die Ausübung des gemeindlichen Vorkaufsrechts sind Grundstücksverkäufer oder -käufer gem. § 28 Abs. 1 Satz 1 BauBG verpflichtet, der Gemeinde den Inhalt des Kaufvertrages unverzüglich mitzuteilen. In der Praxis werden diese Mitteilungspflichten in der Regel durch die Notare wahrgenommen, die eine vollständige Ausfertigung des Kaufvertrages an die jeweilige Gemeinde übermitteln. Diese Vorgehensweise ist schon in der Vergangenheit auf datenschutzrechtliche Bedenken gestoßen (vgl. hierzu 13. Tb., Tz. 15.2). Denn zunächst ist von den Gemeinden nur zu prüfen, ob überhaupt ein Vorkaufsrecht besteht. Für diese Prüfung ist aber nicht die Kenntnis aller im notariellen Kaufvertrag enthaltenen Daten erforderlich. Bedenklich ist insbesondere die Nutzung dieser Daten zur Errichtung einer inoffiziellen Kaufpreissammlung. Aufgrund dieser durch den Datenschutz bereits früher geäußerten Bedenken hat sich auch das Ministerium des Innern und für Sport schon 1991 für ein gestuftes Mitteilungsverfahren ausgesprochen (1. Mitteilung der Daten, die zur Überprüfung des Bestehens eines Vorkaufsrechts benötigt werden, 2. Mitteilung der ergänzenden Daten für die Entscheidung, ob ein bestehendes Vorkaufsrecht ausgeübt wird) und darüber auch den Gemeinde- und Städtebund Rheinland-Pfalz sowie den Städtetag Rheinland-Pfalz informiert mit der Bitte, den Mitgliedern die Anwendung des zweistufigen Mitteilungsverfahrens zu empfehlen. Die angeregte Änderung des § 28 Abs. 1 BauGB dergestalt, dass das gestufte Übermittlungsverfahren auch gesetzlich vorgeschrieben wird, wurde nicht umgesetzt.

Weiterhin wollte die Verbandsgemeinde wissen, ob es datenschutzrechtlich zulässig sei, eine Liste mit Namen von Veräußerern und Erwerbern und der genauen Grundstücksbezeichnung (Gemarkung, Flurstück, Parzelle, evtl. Straße und Hausnummer) an sämtliche Abteilungen der Gemeindeverwaltung zu geben, wenn die Gemeinde aufgrund der Prüfung ihres Vorkaufsrechts Kenntnis von der beabsichtigten Veräußerung erhält. Das Verteilen solcher Listen sei wünschenswert, da dadurch die einzelnen das Grundstück betreffenden Register und Verzeichnisse berichtigt bzw. ergänzt werden könnten.

Die Nutzung personenbeziehbarer Daten ist grundsätzlich nur für den Zweck zulässig, für den die Daten erhoben worden sind (§ 13 Abs. 1 Nr. 2 LDSG), also hier für die Prüfung des Vorkaufsrechts der Gemeinde. Eine Zweckänderung ist nur unter den Voraussetzungen des § 13 Abs. 2 LDSG zulässig. Gegen eine generelle Weitergabe auch der eingeschränkten Verkaufsdaten an alle Abteilungen der Verwaltung spricht das Erfordernis, dass stets im Einzelfall die Voraussetzungen für eine Zweckänderung geprüft werden müssen. Nicht jede Abteilung der Gemeinde führt ein Register oder Verzeichnis, das evtl. aufgrund der Verkaufsdaten angepasst werden müsste. Damit ist es auch nicht erforderlich, dass jede Abteilung Kenntnis dieser Daten erhält. Im Einzelfall kann eine Weitergabe an eine einzelne, ein bestimmtes Register oder Verzeichnis führende Abteilung durchaus im Rahmen einer Zweckänderung zulässig sein, nicht aber eine generelle Weitergabe ohne Prüfung des jeweiligen Zwecks.

18.5 Das illegale Wochenendhaus

Die Bearbeitung einer Eingabe brachte in dem nachfolgend geschilderten Fall zu Tage, wie eng gelegentlich Behörden mit Unternehmen der privaten Wirtschaft zu Lasten der Bürger zusammenarbeiten.

Der Petent hatte ein Wochenendhaus übernommen, welches sich auf dem Grundstück einer Firma befand, nichts ahnend, dass weder für sein Wochenendhaus noch für viele andere in der Nachbarschaft errichtete Wochenendhäuser eine Baugenehmigung vorlag. Da sein Nachbar einige „unschöne Bauten“ errichtete, fragte der Petent bei der Verbandsgemeinde nach der rechtlichen Zulässigkeit nach. Die Verbandsgemeinde, obwohl in der Sache gar nicht zuständig, gab diese Anfrage vollständig an das Unternehmen als Grundstückseigentümerin weiter, woraufhin diese das Mietverhältnis u. a. mit der Begründung „Sie haben in Verkennung Ihrer Rechte auch die Verbandsgemeinde ... eingeschaltet, was zu erheblichen Unruhen führte“ fristlos kündigte und Räumungsklage erhob.

Die Aufklärung des Sachverhaltes durch den LfD gestaltete sich schwierig. Über ihre vertraglichen Beziehungen zu dem Unternehmen wollte die Verbandsgemeinde zunächst „aus datenschutzrechtlichen Gründen“ keine Angaben machen. An die Beantwortung nahezu jedes Schreibens musste erinnert werden. Schließlich machte die Verbandsgemeinde gegenüber dem LfD zum Umfang der Datenübermittlung noch objektiv falsche Angaben.

Der LfD beanstandete die Datenübermittlung durch die Verbandsgemeinde an das Unternehmen als Verstoß gegen datenschutzrechtliche Bestimmungen.

18.6 „Den Widerstand aufgeben“; das Datenschutzverständnis eines Kommunalpolitikers

Mit der Überschrift „Den Widerstand aufgeben“ berichtete eine Tageszeitung im Regionalteil, dass der Fraktionsvorsitzende einer im Stadtrat vertretenen Partei die Namen der Gegner eines Bauprojekts, die keine Bereitschaft zeigten, ihren Einspruch zurückzunehmen, der Öffentlichkeit preisgeben wolle. Nach der Veröffentlichung der Gegner des Projekts seien diese dann gefordert, „Auge in Auge“ den übrigen Bürgern gegenüberzutreten und sich zu der Ablehnung des Projekts zu bekennen.

Der LfD wurde in der Sache sofort tätig, recherchierte den Sachverhalt und wies in einem offenen Brief an die beteiligte Verwaltung, den Fraktionsvorsitzenden und die Tageszeitung darauf hin, dass die Bekanntgabe von Adressdaten der Einwender gegen eine Baumaßnahme in der Öffentlichkeit unzulässig wäre, und zwar unabhängig davon, ob sie dem Mandatsträger durch eine Behörde zur Verfügung gestellt oder in anderer Weise bekannt wurden. Der Inhaber eines Ehrenamtes würde damit die ihm nach § 20 GemO obliegende Schweigepflicht verletzen. Außerdem dürften Straftatbestände nach dem LDSG und dem StGB verwirklicht sein.

Die Veröffentlichung der Adressen von Gegnern des Projekts unterblieb.

18.7 Nebentätigkeiten, Wahrnehmung von öffentlichen Ehrenämtern, ehrenamtliche und sonstige Tätigkeiten

Eine ganze Reihe parlamentarischer Anfragen in der zweiten Jahreshälfte 1998 betraf die Wahrnehmung von Nebentätigkeiten durch Landesbedienstete und kommunale Wahlbeamte. Bei der Beantwortung dieser Anfragen spielte auch der Datenschutz eine Rolle. Betroffene beriefen sich auf ihr informationelles Selbstbestimmungsrecht; das Ministerium des Innern und für Sport verwies auf den Interessenkonflikt zwischen dem Informationsanspruch des Parlaments und der Pflicht zur Geheimhaltung von Personaldaten. Der Datenschutz stehe bei der Beantwortung im Vordergrund.

Die Rechtsfragen um die Beantwortung der parlamentarischen Anfragen wurden öffentlich diskutiert; der Antwort des Ministeriums des Innern und für Sport auf die Große Anfrage der Fraktion BÜNDNIS 90/DIE GRÜNEN – Drucksache 13/3518 – und einer Ergänzung dieser Antwort (Drucksachen 13/3668 und 13/4223) ist zu entnehmen, dass die Frage nach dem Umfang und der Art und Weise der Auskunftserteilung letztendlich gelöst wurde.

Die Kommission beim Landesbeauftragten für den Datenschutz hatte sich aus gegebener Veranlassung bereits im Jahre 1994 mit den Fragestellungen befasst, die jetzt erneut in der Diskussion waren. Der LfD griff die Ergebnisse dieser Diskussion auf. Er wies darauf hin, dass dem Interessenausgleich zwischen dem Informationsanspruch des Parlaments und dem Geheimhaltungsinteresse Betroffener regelmäßig bereits dadurch Rechnung getragen werden kann, dass die entsprechenden Informationen lediglich in anonymisierter Form in der jeweiligen Antwort auf die parlamentarische Anfrage mitgeteilt werden.

In denjenigen Fällen, in denen eine Anonymisierung faktisch nicht möglich ist oder es sich gerade um einen auf eine bestimmte Person bezogenen konkreten Einzelfall handelt, wird die Erteilung der Antwort gemäß § 97 der Geschäftsordnung des Landtags regelmäßig im zuständigen Ausschuss in nichtöffentlicher oder vertraulicher Sitzung zu erfolgen haben. Voraussetzung hierfür ist allerdings, dass die Landesregierung geltend macht, dass die Veröffentlichung der Antwort auf eine Anfrage oder die Beantwortung einer Anfrage in öffentlicher Sitzung des Landtags in unzulässiger Weise in Grundrechte eingreife oder in sonstiger Weise gegen Geheimhaltungsbestimmungen verstoßen würde.

Bei der Beurteilung der Rechtsfragen wird leicht übersehen, dass die verfassungsrechtlichen Auskunftsansprüche des Parlaments gegenüber der Exekutive einfachgesetzlich weder durch Bundes- noch durch Landesrecht – also auch nicht durch Datenschutzgesetze – eingeschränkt werden können. Selbst einfachgesetzliche Geheimhaltungsbestimmungen setzen sich, auch wenn sie keine Ausnahmebestimmungen zugunsten der parlamentarischen Aktenvorlage- und Informationsrechte enthalten, nicht ohne weiteres gegenüber den Parlamentsrechten durch. Das parlamentarische Fragerecht hat Verfassungsrang; es ist sowohl für die parlamentarische Demokratie als auch für das Ansehen des Staates von herausragender Bedeutung (vgl. BVerfGE 67, 100). Ohne Zweifel erstreckt es sich auch auf die Wahrnehmung der Rechtsaufsicht über die Kommunen.

Vor dem Hintergrund dieser verfassungsmäßigen Einordnung des parlamentarischen Fragerechts hielt es der LfD für geboten, zunächst die Vorfrage zu klären, ob sich aus dem parlamentarischen Fragerecht eine Verpflichtung für die Landesregierung ergibt, die für die Beantwortung der Anfragen erforderlichen Informationen bei kommunalen Wahlbeamten zu erfragen und sie dann an das Parlament zu übermitteln. Er wies darauf hin, dass seine Kontroll- und Beratungszuständigkeit nur insoweit berührt

ist, als es um die Erhebung von Daten und deren Übermittlung durch die Landesregierung geht. Die Vorfrage, ob das Parlament oder Teile desselben zur Datenerhebung befugt sind, fällt unter den Parlamentsvorbehalt des § 2 Abs. 2 LDSG; insoweit hat der LfD keine Kompetenz.

Sofern Fragen der in Rede stehenden Art vom parlamentarischen Kontrollrecht gedeckt sind, besteht die Verpflichtung der Landesregierung, sie in personenbezogener Form unter Beachtung des Verfahrens nach § 97 GOLT zu beantworten. Sofern das Informationsrecht des Parlaments mit den Persönlichkeitsrechten der Betroffenen kollidiert, ist der Ausgleich zwischen ihnen nach dem Prinzip der praktischen Konkordanz herbeizuführen. Hierbei ist zu berücksichtigen, dass das Parlament wirksame rechtliche, organisatorische und verfahrensmäßige Schutzvorkehrungen getroffen hat. Es ist, bezogen auf die konkreten Fälle, ferner zu berücksichtigen, dass die Art und Höhe von Nebentätigkeitsvergütungen nicht ohne sachlichen Bezug zum Hauptamt sind. Sie gehören nach Auffassung des LfD nicht zu den Informationen, deren Weitergabe wegen ihres streng persönlichen Charakters für die Betroffenen unzumutbar ist (BVerfGE 65,1, 46) und sie sind auch nicht jener unantastbaren Sphäre privater Lebensgestaltung zuzuordnen, die von vornherein jeglicher Einwirkung der öffentlichen Hand entzogen ist.

18.8 Verwendung einer Videokamera für Überwachungszwecke

Eine Stadtverwaltung sah sich mit dem Problem konfrontiert, dass Besucher und Mitarbeiter der Bibliothek zunehmend durch Personen belästigt wurden, die sich im Eingangsbereich aufhielten. Beklagt wurden Pöbeleien, Beleidigungen, Sachbeschädigungen und exhibitionische Handlungen. Man kam auf den Gedanken, zu Beweissicherungszwecken eine Videokamera zu installieren und alle Bewegungen im Eingangsbereich kurzzeitig aufzuzeichnen. Der LfD wurde aufgefordert, die Zulässigkeit einer solchen Maßnahme zu beurteilen.

Die Fertigung von Videoaufnahmen stellt einen Eingriff in das allgemeine Persönlichkeitsrecht der Betroffenen dar. Dies ist durch die Rechtsprechung allgemein anerkannt (Landgericht Berlin, Urteil vom 22. August 1986, NJW 88, 346; OLG Frankfurt, Urteil vom 21. Januar 1987, NJW 87, 1087).

In das allgemeine Persönlichkeitsrecht der Betroffenen kann aufgrund eines Gesetzes eingegriffen werden. Eine gesetzliche Grundlage für die Fertigung von Videoaufnahmen durch die Stadtverwaltung als Grundstückseigentümerin zu Beweissicherungszwecken war nicht ersichtlich.

Für die dem Hausrecht unterworfenen Personen kann indessen auch die Einwilligung eine Rechtsgrundlage für die Fertigung von Videoaufnahmen bilden. Vom Vorliegen der Einwilligung kann im Bereich der fiskalischen Verwaltungstätigkeit ausgegangen werden, wenn jedem, der den vom Hausrecht umfassten Bereich betritt, deutlich ist, dass Videoaufnahmen gefertigt werden und er nur unter der Bedingung Zutritt hat, dass er die Fertigung von Videoaufnahmen duldet.

Die Videoaufzeichnungen müssen schnellstmöglich ausgewertet und, wenn die weitere Speicherung für die Aufgabenerfüllung nicht erforderlich ist, gelöscht werden.

18.9 Personenstandswesen

18.9.1 Datenschutz und Familienforschung

Der Zugang und die Verwendung von Personenstandsdaten für Zwecke der Familienforschung ist immer wieder Gegenstand von Eingaben an die Behörde des LfD. Sie bildeten den Hintergrund für die klarstellenden Hinweise im 16. Tb., Tz. 18.7.

Die Rechtslage ist unverändert; Zugangsrechte – Einsicht und Durchsicht – zu Personenstandsdaten haben für Zwecke der Familienforschung die Ehegatten, Vorfahren und Abkömmlinge. Andere Personen haben, weil das Forschungsinteresse nicht als rechtliches Interesse i. S. von § 61 Abs. 1 PStG anerkannt wird, aufgrund § 4 Abs. 2 der LVO zur Durchführung des PStG nur Zugang zu den Zivilstandsregistern, die vor dem 1. Januar 1876 geführt wurden.

Bisweilen gewähren die Standesbeamten in richtiger Anwendung der gesetzlichen Vorschriften zwar Einsicht in Personenstandsbücher, lehnen es aber unter Hinweis auf den Datenschutz ab, der Anfertigung von Kopien zuzustimmen.

Mit Datenschutz hat dies nichts zu tun. Datenschutzrelevant kann einzig der Übermittlungsvorgang sein. Ob die im Rahmen der Einsichtnahme übermittelten Daten handschriftlich aufgezeichnet werden oder ob die Anfertigung einer Ablichtung zugelassen wird, spielt keine Rolle. Man wird den Standesbeamten freilich zugute halten müssen, dass die Durchführungsverordnung zum PStG nur die Einsicht und die Erteilung von Personenstandsurkunden regelt. Es wird wohl kaum zu beanstanden sein, wenn ein Standesbeamter diese Vorschrift eng auslegt und die Anfertigung von Kopien ablehnt. Er könnte sich auch darauf stützen, dass der Gesetzgeber vereinzelt die Anfertigung von Kopien im Zusammenhang mit der Wahrnehmung von Einsichtsrechten ausdrücklich geregelt hat (z. B. § 25 Abs. 5 SGB X) und im Umkehrschluss aus einer Nichtregelung die Folgerung ziehen, dass das Anfertigen von Kopien nicht zugelassen ist.

Die Anfertigung von Kopien wird aber bisweilen auch deshalb abgelehnt, weil Standesbeamte befürchten, dass die Personenstandsbücher beschädigt werden. Auch dies ist kein Datenschutzgesichtspunkt; dass der Standesbeamte bei seiner Entscheidung solchen Überlegungen Raum gibt, ist aber gleichwohl nicht zu beanstanden.

18.9.2 Zwangsvollstreckung gegen Transsexuelle

Ein Rechtsanwalt hatte in einem Schadensersatzprozess einen Vollstreckungstitel erwirkt. Bei der Vollstreckung gab es jedoch Schwierigkeiten, da sich beim Vollstreckungsschuldner gem. § 1 des TSG bereits der Vorname geändert hatte. Um die Personenidentität nachzuweisen, wandte sich der Anwalt an das Standesamt einer Verbandsgemeinde und bat um eine Abschrift aus dem Familienbuch. Die Verbandsgemeinde entsprach dieser Bitte, da sie davon ausging, dies sei für die Umschreibung des Titels erforderlich.

Diese auf den ersten Blick einleuchtende Vorgehensweise stellte sich im Ergebnis als Verstoß gegen die Vorschriften des Personenstandsgesetzes dar:

Rechtsgrundlage für die Erteilung von Personenstandsurkunden, zu denen gem. § 61 a Nr. 4 PStG auch Auszüge aus dem Familienbuch gehören, ist § 61 PStG. Grundsätzlich hängt die Erteilung von Personenstandsurkunden vom Vorliegen eines rechtlichen Interesses ab (§ 61 Abs. 1 Satz 3 PStG). § 61 Abs. 3 enthält jedoch eine spezialgesetzliche und damit vorrangig anzuwendende Regelung für Transsexuelle: Hiernach darf bei Personen, bei denen auf Grund des Transsexuellengesetzes die Vornamen geändert sind, ein Auszug aus dem Familienbuch nur Behörden oder der betroffenen Person selbst erteilt werden.

Da im vorliegenden Fall der Vorname bereits geändert war, erfolgte die Erteilung des Auszugs aus dem Familienbuch an den Rechtsanwalt unter Verstoß gegen § 61 Abs. 3 PStG.

Dieser benötigte auch keinen personenstandsrechtlichen Nachweis, um den Titel umschreiben zu lassen. Nur im Fall der Rechtsnachfolge, die durch Vorlage von öffentlichen oder öffentlich beglaubigten Urkunden nachzuweisen ist, bedarf es gem. § 727 ZPO einer Titelumschreibung. Eine Rechtsnachfolge lag jedoch hier nicht vor, sondern lediglich eine Namensänderung. In einem solchen Fall steht der nunmehr falsch gewordene Name im Vollstreckungstitel der Vollstreckung grundsätzlich nicht entgegen; bei feststehender Identität kann ohne Berichtigung oder Umschreibung des Titels vollstreckt werden (Thomas-Putzo, Kommentar zur Zivilprozessordnung, § 750, Rdnr. 3 und 5).

Schließlich war im Rahmen der datenschutzrechtlichen Bewertung auch der Umfang der erfolgten Datenübermittlung zu berücksichtigen. Der Auszug aus dem Familienbuch enthielt z.T. sensible Informationen (z. B. Kirchenaustritt der Ehefrau), auf die es im konkreten Fall aber gar nicht ankam.

Die Verbandsgemeinde kam, wie sie es ausdrückte, „nicht umhin, formaljuristisch diese Ausführungen anerkennen zu müssen“.

18.10 Übersendung von Gräberlisten an die Landeszentrale für politische Bildung

Das Friedhofsamt einer Stadtverwaltung wurde von der Landeszentrale für politische Bildung gebeten, Gräberlisten ausländischer Zwangsarbeiter zu übersenden. Hintergrund der Anfrage war die geplante Herausgabe eines „Heimatgeschichtlichen Wegweisers zu den Stätten des Widerstandes und der Verfolgung 1933 bis 1945 in Rheinland-Pfalz“. Das Friedhofsamt hatte datenschutzrechtliche Bedenken und bat den LfD um eine Stellungnahme.

Hinzuweisen war zunächst auf den Umstand, dass die Daten Verstorbener – weil diese nicht mehr Inhaber eines Persönlichkeitsrechts im Sinne des Rechts auf informationelle Selbstbestimmung sind – durch das Landesdatenschutzgesetz nicht geschützt sind.

Eine Anwendung des Landesdatenschutzgesetzes kommt daher allenfalls analog oder dann in Betracht, wenn durch die Übermittlung von Daten ausländischer Zwangsarbeiter an die Landeszentrale für politische Bildung und die Veröffentlichung im „Heimatgeschichtlichen Wegweiser“ schutzwürdige Belange noch lebender Personen, insbesondere von Angehörigen berührt werden.

Die Gräberlisten beinhalteten vorliegend lediglich die Namen, Geburts- und Sterbedaten sowie die Staatsangehörigkeit der Verstorbenen. Die Veröffentlichung im „Heimatgeschichtlichen Wegweiser“ war nicht in personenbezogener Form beabsichtigt. Es sollte vielmehr lediglich die Anzahl bestimmter ausländischer Zwangsarbeiter/Kriegsarbeiter in den betreffenden Orten genannt werden.

Die Datenerhebungsbefugnis der Landeszentrale für politische Bildung ließ sich nach Auffassung des LfD auf § 12 Abs. 4 Ziff. 6 und 9 LDSG (analog) und die Datenübermittlungsbefugnis der Stadtverwaltung auf § 14 Abs. 1 LDSG (analog) stützen. Gegen die Übermittlung der Gräberlisten bestanden daher keine datenschutzrechtlichen Bedenken.

19. Telekommunikation

19.1 Schutzgut Fernmeldegeheimnis

Das Fernmeldegeheimnis schützt jede Form der Telekommunikation, d. h. in Anlehnung an die Definition des § 3 Nr. 16 TKG jede durch eine technische Anlage vermittelte individuelle Nachrichtenübertragung.

19.1.1 Die gesetzliche Absicherung des Fernmeldegeheimnisses

Das Grundrecht auf Wahrung des Fernmeldegeheimnisses gem. Artikel 10 GG ist bei der Erbringung von Dienstleistungen seit der Privatisierung der Telekommunikation nicht mehr allein für staatliche Stellen, wie dies bei der Deutschen Bundespost der Fall war, von Bedeutung.

Nach allgemeiner Auffassung dient Art. 10 Abs. 1 GG in erster Linie dem Schutz der Privatsphäre (BVerfGE 85, 386, 395 f.). Das durch diese Norm garantierte verfassungsrechtliche Fernmeldegeheimnis wirkt als Abwehrgrundrecht gegen staatliche Eingriffe direkt weiterhin im Verhältnis Staat – Bürger. Es schützt den Einzelnen davor, dass der Inhalt einer von ihm durchgeführten Telekommunikation sowie deren nähere Umstände (z. B. Zeitpunkt und Dauer eines Telefongesprächs, Rufnummer) staatlichen Stellen zur Kenntnis gelangen. Beschränkungen dieses Grundrechts dürfen nur aufgrund eines Gesetzes angeordnet werden. Das verfassungsrechtliche Fernmeldegeheimnis hat indessen keine unmittelbare Wirkung für den privaten Rechtsverkehr, beispielsweise für das Verhältnis zwischen Telekommunikationsunternehmen und ihren Kunden. Die Bürgerinnen und Bürger sind aber nur dann gesetzlich ausreichend geschützt, wenn wirksame Instrumente auch gegen die Eingriffsmöglichkeiten der privaten Telekommunikationsbetreiber und unbefugte Dritte (z. B. Hacker) vorhanden sind.

Das einfachgesetzliche Fernmeldegeheimnis ist in § 85 TKG normiert. Diese Vorschrift verpflichtet alle, die geschäftsmäßig Telekommunikationsdienste erbringen, zur Geheimhaltung der Inhalte und der Umstände der von ihnen vermittelten Kommunikation. Mit „Inhalt“ sind die mittels Telekommunikationsanlage übermittelten individuellen Nachrichten gemeint, während die „näheren Umstände“ insbesondere die Verbindungsdaten eines Kommunikationsvorgangs umfassen. Ferner wird klargestellt, dass auch erfolglose Verbindungsversuche dem Fernmeldegeheimnis unterliegen. Ausnahmen sind nur zulässig, soweit sie betriebsnotwendig sind oder auf einer spezialgesetzlichen Grundlage beruhen (vgl. Büchner in: Beck’scher TKG-Kommentar, 1997, § 85 Rdnrn. 8 ff.). Zusätzlich verpflichtet § 87 TKG die Telekommunikationsunternehmen zu angemessenen technischen Schutzmaßnahmen. Hierzu hat die Regulierungsbehörde für Telekommunikation und Post einen Katalog von Sicherheitsanforderungen veröffentlicht (vgl. Bundesanzeiger Nr. 208 a vom 7. November 1997). Lizenzpflichtige Betreiber müssen zudem nach § 87 Abs. 2 TKG ein Sicherheitskonzept erstellen und der Regulierungsbehörde vorlegen. Zur Kontrolle dieser Verpflichtungen steht der Regulierungsbehörde das gesamte Spektrum der aufsichtsbehördlichen Instrumente zu. Sie kann nach § 91 TKG Anordnungen und andere geeignete Maßnahmen, einschließlich einer Untersagung, treffen.

Im Bereich des Strafrechts ist insbesondere der neue Tatbestand der Verletzung des Fernmeldegeheimnisses nach § 206 StGB einschlägig, der an die Stelle von § 354 StGB getreten ist. Als Täter kommen insbesondere die Inhaber oder Beschäftigten eines Unternehmens, das geschäftsmäßig Telekommunikationsdienste erbringt, in Betracht.

Schließlich sieht § 40 TKG auch eine zivilrechtliche Schadensersatzpflicht für vorsätzliche oder fahrlässige Verletzungen der Verpflichtungen vor, die sich aus dem Gesetz, einer darauf beruhenden Verordnung oder einer Anordnung der Regulierungsbehörde ergeben. Sie besteht also auch bei Verletzung des Fernmeldegeheimnisses. Des Weiteren kommt ein Unterlassungsanspruch nach § 40 Satz 2 TKG in Betracht.

Erwähnenswert ist auch die zusätzliche Absicherung des Fernmeldegeheimnisses durch Art. 5 der EG-Richtlinie über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation (vgl. 16. Tb., Tz. 19.1). Danach sind die Mitgliedstaaten verpflichtet, die Vertraulichkeit der mit öffentlichen Telekommunikationsnetzen und öffentlich zugänglichen Telekommunikationsdiensten erfolgenden Kommunikation sicherzustellen. Darüber hinaus wird die Zuständigkeit der nach Art. 29 der allgemeinen EG-Datenschutzrichtlinie geschaffenen Datenschutzgruppe auf die Überwachung der Einhaltung der Pflichten aus der Telekommunikationsdatenschutzrichtlinie erweitert.

Auf der Ebene der nationalen Netzstruktur der Telekommunikationsanbieter erscheinen die beschriebenen Schutzfunktionen geeignet, das kommunikative Selbstbestimmungsrecht zu wahren.

19.1.2 Private Vorsorge zum Schutz des Fernmeldegeheimnisses

Im Zeitalter der internationalen Vernetzung bleiben nationalstaatliche Regelungen allerdings weitgehend wirkungslos. Man denke hier nur an den Datenstrom im Internet, der sich einer einzelstaatlichen Regulierung entzieht. So fehlt es beispielsweise an einer Festlegung der Kommunikationswege, denn die Internetprotokolle tragen lediglich dafür Sorge, dass die Nachrichten an ihrem Bestimmungsort ankommen, legen aber nicht den Weg fest. Der Datenverkehr im Internet ist, soweit nicht eigene Vorkehrungen getroffen wurden, weitgehend ungesichert gegenüber einem unbefugten Mitlesen, Kopieren, Verändern oder Löschen. Man kann sich also nicht darauf verlassen, aufgrund nationaler gesetzlicher Regelungen vor fremden rechtswidrigen Eingriffen geschützt zu sein. Hier ist vielmehr eigene Vorsorge notwendig. Die Möglichkeiten der Nutzer, sich autonom zu schützen, sind vorhanden. So wird durch die Anwendung von Verschlüsselungstechniken (Kryptographie, Steganographie) beispielsweise ein „elektronisches Kuvert“ für die Nachricht erzeugt, das lediglich von jenen geöffnet werden kann, die den passenden Schlüssel („Brieföffner“) haben. In Deutschland ist die Verschlüsselung gesetzlich nicht eingeschränkt. Ihre Verwendung fällt in den Schutzbereich des Art. 10 Abs. 1 GG. Es steht den Teilnehmern frei, in welcher Form sie ihre individuelle Kommunikation gestalten. Mit dem Einsatz wirksamer technischer Vorkehrungen zum Schutz des Kommunikationsgeheimnisses wird sichergestellt, dass man sich mit einem Kommunikationspartner in einem für Dritte unverständlichen Zeichen-Zuordnungssystem bewegt.

19.1.3 Gesetzliche Reglementierung des Einsatzes von Verschlüsselungsverfahren?

Im Berichtszeitraum wurde erneut die Frage diskutiert, ob das Erfordernis einer rechtlichen Regelung des Einsatzes von Verschlüsselungsverfahren besteht. Wenn nämlich der Bürger die Möglichkeit hat, das Fernmeldegeheimnis mit eigenen Mitteln zu schützen, verhindert eine wirksame Geheimhaltung auch die Überwachung zum Zwecke der Strafverfolgung. So gab es konkrete Pläne, Verschlüsselung zu verbieten. Die Befürworter solcher Maßnahmen führten an, dass bei einer breiten Nutzung der Verschlüsselungsmöglichkeiten durch Straftäter ohne eine Möglichkeit der Entschlüsselung durch die Stafverfolgungs- bzw. Sicherheitsbehörden die Bekämpfung der Kriminalität künftig erheblich erschwert werde. Es seien Regelungen notwendig, die bei Vorliegen einer rechtmäßigen Überwachungsanordnung nach §§ 100 a , 100 b StPO, § 39 AWG oder dem G-10-Gesetz im Falle einer verschlüsselten Kommunikation eine Entschlüsselung ermöglichten. Nicht hinnehmbar sei, dass die Sicherheitsbehörden durch die Anwendung kryptographischer Verfahren nicht mehr in der Lage wären, Maßnahmen zum Abhören und Überwachen im Bereich der Telefon- , Fax- und Datenkommunikation vorzunehmen. In der Fachdiskussion wurde jedoch deutlich nachgewiesen, dass gesetzliche Verbote oder Beschränkungen aufgrund der technischen Umgehungsmöglichkeiten ungeeignet sind. Es gibt beispielsweise vielfältige Möglichkeiten unerkennbar zu verschlüsseln. Beispiele aus dem Bereich der Steganographie machen dies deutlich. So lassen sich in harmlosen und unverdächtigen Daten (etwa multimedialen Dokumenten, Bilddateien oder Videokonferenzbildern) geheime Informationen verstecken und übertragen, ohne dass Außenstehende, z. B. Strafverfolger, eine Chance haben, dies überhaupt zu bemerken. Vor diesem Hintergrund wird deutlich, dass eine Kryptoreglementierung nicht geeignet ist, einen effektiven Beitrag zur Verbrechensbekämpfung zu leisten. Die Kryptographie wird heute zudem weltweit an Universitäten gelehrt und nicht zu überwindende Verschlüsselungsverfahren können z. B. über das Internet bezogen werden. Damit wird jede der Aufrechterhaltung der Abhörmöglichkeiten von Sicherheitsbehörden dienende Regulierung der Verschlüsselung zwangsläufig ins Leere laufen. In der rechtspolitischen Diskussion wurde auch hinterfragt, wie hoch die Strafdrohung ausfallen solle, damit es ein Straftäter vorzieht, unverschlüsselt über seine Tatpläne zu korrespondieren. Es ist offensichtlich, dass jede Beschränkung der Kryptographie zur Bekämpfung der organisierten Kriminalität ungeeignet ist. Sie gefährdet indessen den dringend notwendigen Schutz personenbezogener Daten. Zu dieser Einschätzung ist auch das Bundeskabinett gelangt, das in seiner Sitzung am 2. Juni 1999 die deutsche Haltung zur Frage der Nutzung kryptographischer Verfahren in Form von „Eckpunkten der deutschen Kryptopolitik“ entschieden hat. Die Kabinettsentscheidung stellt klar, dass in Deutschland auch künftig Verschlüsselungsverfahren und -produkte ohne Restriktion entwickelt, hergestellt, vermarktet und genutzt werden dürfen. Zentrales Anliegen der Kabinettsentscheidung ist der verbesserte Schutz deutscher Nutzer in den weltweiten Informationsnetzen durch Einsatz sicherer kryptographischer Verfahren. Auf der Grundlage der bisherigen nationalen Diskussion sowie der internationalen Entwicklung hat die Bundesregierung die im Folgenden wiedergegebenen Eckpunkte ihrer Kryptopolitik beschlossen:

– „Die Bundesregierung beabsichtigt nicht, die freie Verfügbarkeit von Verschlüsselungsprodukten in Deutschland einzuschränken. Sie sieht in der Anwendung sicherer Verschlüsselung eine entscheidende Voraussetzung für den Datenschutz der Bürger, für die Entwicklung des elektronischen Geschäftsverkehrs sowie für den Schutz von Unternehmensgeheimnissen. Die Bundesregierung wird deshalb die Verbreitung sicherer Verschlüsselung in Deutschland aktiv unterstützen. Dazu zählt insbesondere die Förderung des Sicherheitsbewusstseins bei den Bürgern, der Wirtschaft und der Verwaltung.

– Die Bundesregierung strebt an, das Vertrauen der Nutzer in die Sicherheit der Verschlüsselung zu stärken. Sie wird deshalb Maßnahmen ergreifen, um einen Vertrauensrahmen für sichere Verschlüsselung zu schaffen, insbesondere indem sie die Überprüfbarkeit von Verschlüsselungsprodukten auf ihre Sicherheitsfunktionen verbessert und die Nutzung geprüfter Produkte empfiehlt.

– Die Bundesregierung hält aus Gründen der Sicherheit von Staat, Wirtschaft und Gesellschaft die Fähigkeit deutscher Hersteller zur Entwicklung und Herstellung von sicheren und leistungsfähigen Verschlüsselungsprodukten für unverzichtbar. Sie wird Maßnahmen ergreifen, um die internationale Wettbewerbsfähigkeit des Sektors zu stärken.

– Durch die Verbreitung starker Verschlüsselungsverfahren dürfen die gesetzlichen Befugnisse der Strafverfolgungs- und Sicherheitsbehörden zur Telekommunikationsüberwachung nicht ausgehöhlt werden. Die zuständigen Bundesministerien werden deshalb die Entwicklung weiterhin aufmerksam beobachten und nach Ablauf von zwei Jahren hierzu berichten. Unabhängig hiervon setzt sich die Bundesregierung im Rahmen ihrer Möglichkeiten für die Verbesserung der technischen Kompetenzen der Strafverfolgungs- und Sicherheitsbehörden ein.

– Die Bundesregierung legt großen Wert auf die internationale Zusammenarbeit im Bereich der Verschlüsselungspolitik. Sie tritt ein für am Markt entwickelte offene Standards und interoperable Systeme und wird sich für die Stärkung der multilateralen und bilateralen Zusammenarbeit einsetzen.“

Damit ist die Regulierungsdebatte im Bereich der Kryptographie vom Tisch. Nach Jahren nationaler und internationaler Diskussion wird die Position der Bundesregierung aus datenschutzrechtlicher Sicht ausdrücklich begrüßt.

Verschlüsselung in Nutzerhand ist als Basistechnologie für sichere Kommunikation unentbehrlich; denn sie gewährleistet den dringend notwendigen Schutz personenbezogener Daten in offenen Netzen. Die freie und uneingeschränkte Kryptographie wird auch als Basis für die Sicherheit im Internet dienen.

19.2 Entwurf einer neuen Telekommunikations-Datenschutzverordnung

Die Telekommunikations-Datenschutzverordnung soll an die Stelle der bisherigen Telekommunikationsdienstunternehmen-Datenschutzverordnung vom 12. Juli 1996 treten. Deren Überarbeitung ist wegen der Umstellung auf die Rechtsgrundlage im Telekommunikationsgesetz erforderlich. Die neue Verordnung hat zugleich die Richtlinie 97/66/EG vom 15. Dezember 1997 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation („ISDN-Richtlinie“) zu berücksichtigen (vgl. hierzu 16. Tb., Tz. 19.1).

Bereits in einem frühen Stadium der Digitalisierung des Telekommunikationsnetzes hat der LfD auf die Gefahren hingewiesen, die dadurch entstehen, dass im Gegensatz zur früheren analogen Vermittlungstechnik in großem Umfang personenbezogene Verbindungsdaten erzeugt und verarbeitet werden. Das ISDN-Netz hat vor allem deshalb zu datenschutzrechtlichen Problemen und zu immer komplizierter werdenden Regelungen geführt, weil seine Struktur nicht am Grundsatz der Datensparsamkeit orientiert ist. Das Entstehen großer Mengen von personenbezogenen Datenspuren im Telekommunikationsnetz zwingt zu begrenzenden Regelungen wie z. B. Löschungspflichten, um das informationelle Selbstbestimmungsrecht der Telefonkunden zu garantieren (vgl. dazu auch 14. Tb., Tz. 20.1).

Der zwischenzeitlich vorgelegte Entwurf der Telekommunikations-Datenschutzverordnung hat seine Ermächtigungsgrundlage in § 89 Abs. 1 TKG. Die Verordnung bezieht sich auf Unternehmen, die geschäftsmäßig Telekommunikationsdienste erbringen oder an der Erbringung solcher Dienste mitwirken. Damit fallen auch Nebenstellenanlagen in Hotels, Krankenhäusern und Betrieben sowie Corporate Networks, also geschlossene Benutzergruppen, die nicht für jedermann öffentlich zugänglich sind, in den Anwendungsbereich der Telekommunikations-Datenschutzverordnung.

Der Grundsatz der Verhältnismäßigkeit ist gem. § 89 Abs. 1 Satz 2 TKG Maßstab für den Regelungsgehalt. In diesem Zusammenhang ist bemerkenswert, dass nach dem Entwurf alle Verbindungsdaten in der Regel selbst bei unbestrittenen oder bezahlten Rechnungen zwei Jahre nach Ende der Verbindung gespeichert bleiben können. Die bisher geltende Telekommunikationsdienstunternehmen-Datenschutzverordnung sieht vor, dass die Verbindungsdaten unter Kürzung der Zielrufnummer bis zu 80 Tagen nach Versendung der Rechnung gespeichert werden dürfen, wenn der Kunde nicht entweder eine vollständige Speicherung oder vollständige Löschung mit Versendung der Rechnung verlangt. Über diese Frist hinaus dürfen Verbindungsdaten nur gespeichert bleiben, wenn Streit zwischen dem Telekommunikationsunternehmen und dem Kunden über die Richtigkeit der Abrechnung entsteht. Die nunmehr vorgesehene Speicherungsdauer von zwei Jahren ist weder für Zwecke der Verbindungsherstellung noch der Abrechnung erforderlich und würde zu einem unverhältnismäßigen Eingriff in das Recht der Telefonkunden auf unbeobachtete Kommunikation führen. Der Regelungs- und Kontrollaufwand, um die dann entstehenden Datenbestände zu beherrschen, wäre erheblich. Damit verbunden ist die Gefahr, dass diese Daten auch für telekommunikationsfremde Zwecke genutzt werden könnten. In ihrer Entschließung vom 25./26. März 1999 haben die Datenschutzbeauftragten des Bundes und der Länder daher gefordert, dass personenbezogene Daten, die für Zwecke der Telekommunikation erhoben und verarbeitet werden, nur so lange gespeichert bleiben dürfen, wie es zu diesen Zwecken erforderlich ist. Auch die vom Gesetz geforderte Höchstfrist für die Speicherung von Verbindungsdaten muss sich am Grundsatz der Datensparsamkeit orientieren, solange sich die Kundin oder der Kunde nicht ausdrücklich für eine längere Speicherung entscheiden (vgl. Anlage 13).

Bei der Gestaltung von Einzelverbindungsnachweisen sollte der Verordnungsgeber sich die Erfahrungen insbesondere in den Niederlanden zu Nutze machen, wo jeder einzelne Telefonkunde entscheiden kann, ob er auf einem Einzelverbindungsnachweis dessen, der ihn anruft, erscheinen will oder nicht. Dieses „holländische Modell“ trägt der informationellen Selbstbestimmung aller Beteiligten besser Rechnung als die weiterhin vorgesehene komplizierte Regelung im deutschen Telekommunikationsrecht (vgl. dazu 16. Tb., Tz. 19.6). Damit würden auch die Probleme gelöst, die bisher beim Schutz der Vertraulichkeit von Anrufen bei Beratungsstellen in sozialen oder kirchlichen Bereichen auftreten und nur mit hohem bürokratischem Aufwand zu bewältigen sind.

19.3 Eckpunktepapier zur Telekommunikations-Überwachungsverordnung

Die Bundesregierung hat bisher keine Rechtsverordnung über die technische und organisatorische Umsetzung von Überwachungsmaßnahmen in der Telekommunikation nach § 88 TKG erlassen, die an die Stelle der bisher geltenden Fernmeldeüberwachungsverordnung treten soll.

Nachdem der im Mai 1998 zur Diskussion gestellte erste Entwurf der TKÜV aufgrund vielfältiger Kritik zurückgezogen worden ist, hat das Bundesministerium für Wirtschaft und Technologie im April 1999 ein in Abstimmung mit den zuständigen Ressorts der Bundesregierung erstelltes Eckpunktepapier für einen neuen Entwurf vorgelegt.

Die Kritik wurde teilweise durch die vorgesehene Strukturierung des Kreises der Verpflichteten sowie durch neue Ansätze zum Umfang der jeweiligen Verpflichtungen berücksichtigt. Insbesondere sieht das Papier eine Verpflichtung zum ständigen Vorhalten von technischen Einrichtungen zur Umsetzung von Überwachungsmaßnahmen für Corporate Networks und geschäftsmäßige Erbringer von Telekommunikationsdiensten aus Gründen der Verhältnismäßigkeit nicht mehr vor.

Das Eckpunktepapier empfiehlt insbesondere die Überarbeitung folgender Regelungsbereiche:

- Anforderungen an die Gestaltung der technischen Einrichtungen.
- Anforderungen an die organisatorische Umsetzung von Überwachungsmaßnahmen.
- Sachgerechte Differenzierung des Kreises der Verpflichteten, die Vorkehrungen für die Umsetzung angeordneter Überwachungsmaßnahmen zu treffen haben, sowie des Umfanges der jeweils erforderlichen Vorkehrungen.

Die äußerst stringenten Regelungen des ersten Entwurfs zur TKÜV sind also hiermit vom Tisch. Damit wäre nämlich nicht nur jedes Telekommunikationsunternehmen, sondern auch jedes Hotel, Krankenhaus und Firmennetz verpflichtet gewesen, Überwachungsschnittstellen auf eigene Kosten bereitzustellen. Mindestens 40 Milliarden Mark hätten die nach Angaben der Regulierungsbehörde rund 400 000 Betroffenen pro Jahr investieren müssen. Noch ist unklar, wer von dem neuen Entwurf betroffen ist. Vermutlich müssen Hotels und Krankenhäuser keine Überwachungseinrichtungen bereitstellen. Generell sind Überwachungsschnittstellen Sollbruchstellen, die Eindringlingen eine zusätzliche Angriffsmöglichkeit eröffnen.

Die Datenschutzbeauftragten des Bundes und der Länder begrüßen es, dass der erste Verordnungsentwurf zurückgezogen worden ist und gegenwärtig überarbeitet wird.

Der Regelungsrahmen ist durch die Strafprozessordnung, das Gesetz zu Artikel 10 GG, das Außenwirtschaftsgesetz sowie durch das Telekommunikationsgesetz vorgegeben. So hat aufgrund der Vorschriften des Art. 1 Abs. 2 G 10, des § 100 Abs. 3 StPO und des § 39 Abs. 5 AWG jeder, der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt, die Überwachung und Aufzeichnung der Telekommunikation zu ermöglichen. Ob und in welchem Umfang hierfür Vorkehrungen zu treffen sind, ergibt sich aus § 88 TKG und der auf dieser Grundlage zu erlassenden Rechtsverordnung zur technischen und organisatorischen Umsetzung von Überwachungsmaßnahmen.

In § 88 Abs. 1 TKG ist festgelegt, dass die technischen Einrichtungen zur Umsetzung von gesetzlich vorgesehenen Maßnahmen zur Überwachung der Telekommunikation vom (geschäftsmäßigen) Betreiber der Telekommunikationsanlage zu gestalten und vorzuhalten sind. § 88 Abs. 2 TKG sieht vor, dass in der Rechtsverordnung Eingrenzungen bestimmt werden können. Das Telekommunikationsgesetz gibt zugleich den zu beachtenden Rahmen vor, nämlich grundlegende technische Erwägungen oder Gründe der Verhältnismäßigkeit.

19.4 Auswirkungen des Telekommunikationsrechts im Krankenhausbereich

Den LfD erreichten zahlreiche Anfragen hinsichtlich der datenschutzrechtlichen Auswirkungen des Telekommunikationsrechts im Krankenhausbereich. Sind Krankenhäuser verpflichtet, gem. § 90 Abs. 1 TKG eine Kundendatei einzurichten und zu führen sowie nach § 90 Abs. 2 TKG dafür Sorge zu tragen, dass die Regulierungsbehörde eine ständige Zugriffsmöglichkeit auf diese Kundendatei besitzt?

Mit diesen Fragen hat sich der Kooperationskreis „Informations- und Kommunikationsdienste“ der Datenschutzaufsichtsbehörden und der Datenschutzbeauftragten des Bundes und der Länder im Februar 1998 beschäftigt und folgende gemeinsame Position zur Frage der Anwendung des § 90 TKG auf Nebenstellenanlagen (insbesondere in Krankenhäusern) erarbeitet:

> „Die Pflicht zur Führung von Kundendateien und zur Bereithaltung dieser Dateien zum Online-Abruf durch die Regulierungsbehörde nach § 90 TKG gilt nicht für Nebenstellenanlagen in Krankenhäusern, Hotels, Unternehmen und Behörden. Sie gilt lediglich für die Deutsche Telekom AG und ihre Konkurrenten auf dem liberalisierten Telekommunikationsmarkt.
>
> Begründung: § 90 TKG verfolgt das Ziel, den Gerichten, Sicherheitsbehörden und Geheimdiensten auf dem liberalisierten Telekommunikationsmarkt auch bei einer Vielzahl von konkurrierenden Anbietern die Ermittlung eines bestimmten Anschlussinhabers zu ermöglichen, gegen den unter Umständen Maßnahmen der Telefonüberwachung angeordnet werden sollen. In der Monopolsituation im Sprachtelefondienst bis Ende 1997 war dies jedenfalls im Festnetz insoweit problemlos möglich, als die Deutsche Telekom AG zur Auskunft über den Hauptanschlussinhaber verpflichtet werden konnte. Auch bisher war es allerdings nicht möglich, durch Online-Abruf beim Netzbetreiber die Namen von Patienten in Erfahrung zu bringen, die in einem bestimmten Zeitraum Nebenstellenanschlüsse eines Krankenhauses genutzt haben, weil die Deutsche Telekom AG über diese Informationen nicht verfügte. Der Bundesgesetzgeber wollte diesen Rechtszustand nicht ändern, sondern lediglich bei der Vielzahl jetzt konkurrierender Telekommunikationsunternehmen die Ermittlungsmöglichkeiten der Sicherheitsbehörden nicht einschränken. Für eine Erweiterung der Zugriffsmöglichkeiten über den bisherigen Rechtszustand hinaus besteht kein Anlass. Insbesondere wäre ein bundesweiter zentraler Zugriff auf Patientendateien neben der Krankenhausmeldepflicht (§ 16 Abs. 3 MRRG) unverhältnismäßig. § 90 TKG ist insoweit restriktiv auszulegen.“

19.5 Fehlleitungen bei Telefax

Immer wieder kommt es zu vermeidbaren Irrläufern beim Faxbetrieb. In der Regel ergeben die Nachforschungen des LfD, dass im Bereich der öffentlichen Stellen durch einen Bedienungsfehler am sendenden Faxgerät die Fehlverbindung zustande gekommen ist. Diese Vorfälle bestätigen, dass beim Einsatz von Telefaxgeräten der Datenschutz nicht genügend beachtet wird, obwohl gerade bei dieser Kommunikationsart besondere Gefahren für das Recht auf informationelle Selbstbestimmung bestehen. Ursache einer entsprechenden Fehlleitung ist oftmals, dass das Überprüfen der eingegebenen Nummer vor der Übermittlung unterbleibt. Der LfD wirkt dann stets darauf hin, dass die Bediensteten nochmals eindringlich auf die datenschutzrechtlichen Erfordernisse beim Einsatz von Telefaxgeräten hingewiesen und insbesondere die Empfehlungen des LfD zu dem Problembereich der Telefaxnutzung beachtet werden (s. Anlage 20). Die Sensibilisierung im Bereich der praktischen Handhabung des Telefaxverkehrs bleibt insoweit eine Daueraufgabe.

Dies belegen auch Fehlleitungen beim Faxversand aufgrund einer (Teil-)Identität der Rufnummer eines Anschlussnehmers und einer Ortsvorwahl. Zum Hintergrund dieses Phänomens: Häufig sind Nebenstellenanlagen der Verwaltung so eingerichtet, dass sie die Verbindung ins öffentliche Netz erst durch Eingabe einer „0“ bereitstellen. Wenn nun im Rahmen einer beabsichtigten Fernverbindung aufgrund eines Bedienungsfehlers am sendenden Faxgerät vergessen wird, die „Amts-0“ vor die Vorwahl (beginnend ebenfalls mit „0“) zu setzen, also lediglich eine „0“ am Anfang der Wählfolge eingegeben wird, interpretiert das Faxgerät dies als Amtsholung und wählt dann weiter, wobei die Ortsvorwahl nun keine „0“ mehr enthält, was dazu führt, dass im Ergebnis eine Rufnummer im Ortsbereich gewählt wird, beispielsweise „123“, ohne führende „0“ für die Ortsvorwahl, dann 4567 für die Teilnehmerkennung.

Dem LfD ist in diesem Zusammenhang ein Fall bekannt geworden, in dem sehr sensible Daten von einer Stadt- an eine Kreisverwaltung per Fernkopie übermittelt werden sollten, das Faxschreiben allerdings nicht dort, sondern bei einem Teilnehmer im städtischen Ortsbereich ankam, der den LfD dankenswerterweise darauf aufmerksam machte. Es hat sich herausgestellt, dass jener Anschlussinhaber nicht das erste Mal auf diese Art und Weise „Post“ bekam, die nicht für ihn bestimmt war.

Die aus diesen praktischen Problemen ableitbare Empfehlung des LfD lautet: Sofern technisch möglich, sollte die Nebenstellenanlage so eingerichtet werden, dass sie eine Verbindung ins öffentliche Netz nicht nach Eingabe einer „0“, sondern nach Eingabe eines Zeichens oder einer Zeichenfolge bereitstellt, die in „normalen“ Telefaxnummern nicht vorkommen können (beispielsweise „*“ oder „#“).

20. Medien

20.1 Der Datenschutz beim Internet-Zugang in öffentlichen Stellen

Immer häufiger stellen Behörden ihren Bediensteten einen Internet-Anschluss zur Verfügung. Dies führt zur Frage, inwieweit hier die Bestimmungen des Teledienstesrechts bzw. des Mediendienstestaatsvertrages Anwendung finden. Ist die öffentliche Stelle als Teledienstanbieterin etwa verpflichtet, den Bediensteten als Nutzerinnen und Nutzern von Telediensten beispielsweise die anonyme Nutzung dieser Dienste zu ermöglichen?

Im Folgenden sollen die Probleme, die an den LfD im Berichtszeitraum herangetragen wurden, kurz dargestellt werden:

Die Anwendbarkeit der vorgenannten Regelwerke auf die Beziehungen zwischen der öffentlichen Stelle und ihren Bediensteten setzt zunächst voraus, dass ein „Anbieter-Nutzer-Verhältnis“ i. S. v. § 3 TDG, § 2 TDDSG, § 3 MDStV vorliegt, es sich bei Diensteanbieter und -nutzer also um zwei verschiedene Personen bzw. Stellen handelt. Hier kommt es entscheidend auf die Ausgestaltung der Nutzung an.

20.1.1 Vermittlung des Internet-Zugangs an Bedienstete für dienstliche Zwecke

Ist die Privatnutzung untersagt, handeln die Beschäftigten stets als Angehörige der nutzenden Stelle in deren Namen und Auftrag, so dass es begrifflich an dem vorgenannten „Anbieter-Nutzer-Verhältnis“ fehlt. Mit anderen Worten: Nutzer des Dienstes sind nicht die Bediensteten, sondern die jeweilige öffentliche Stelle, für deren dienstliche Zwecke der Internet-Zugang eröffnet wird. Die Bediensteten sind bei der dienstlichen Nutzung des Internet-Zugangs der jeweiligen öffentlichen Stelle, bei der sie beschäftigt sind, zuzurechnen. Mithin ist die öffentliche Stelle nicht als Tele- bzw. Mediendiensteanbieter im Sinne des Teledienstegesetzes oder des Mediendienstestaatsvertrages anzusehen, soweit den Bediensteten ausschließlich die dienstliche Nutzung der zur Verfügung gestellten Dienste gestattet und eine private Nutzung ausdrücklich ausgeschlossen ist. Die Zulässigkeit der Datenverarbeitung richtet sich also nicht nach den Bestimmungen des Teledienstesrechts bzw. des Mediendienstestaatsvertrages.

Aus datenschutzrechtlicher Sicht bestehen keine grundsätzlichen Bedenken dagegen, die dienstlichen Nutzungsdaten zu protokollieren. Insoweit sollte erwogen werden, die für die Erfassung und Nutzung von dienstlichen Telefongesprächsdaten bei den öffentlichen Stellen geltenden Regelungen als Modell heranzuziehen. In diesem Zusammenhang ist darauf hinzuweisen, dass Regelungen über die Protokollierung und Auswertung von Nutzungsdaten in einer Dienstvereinbarung mit der Personalvertretung getroffen werden sollten.

20.1.2 Private Nutzung des Internet-Zugangs

Soweit eine öffentliche Stelle ihren Bediensteten die private Nutzung von behördlichen Telekommunikations- bzw. Informationsdiensten gestattet, erbringt sie als Anbieterin – unabhängig von einer Gewinnerzielungsabsicht – geschäftsmäßig diese Dienste. Damit unterliegt sie den Vorschriften zum Schutz des Fernmeldegeheimnisses und den Datenschutzbestimmungen der vorgenannten Regelwerke (vgl. 16. Tb., Tz. 20.3.2 und 20.4). Hier stehen öffentliche Stelle und Bedienstete eindeutig in einem „Anbieter-Nutzer-Verhältnis“.

20.1.3 Elektronische Post

Bezüglich der E-mail-Dienste ist auf der Grundlage der vorstehenden Überlegungen zwischen privater und dienstlicher Nutzung zu unterscheiden. Dies kann dadurch sichergestellt werden, dass den Bediensteten zur Unterscheidung der verschiedenen Nutzungsformen unterschiedliche E-mail-Adressen zugeordnet werden, aus denen sich der dienstliche oder private Charakter der

Adresse ergibt. Daten aus dem dienstlichen E-mail-Verkehr stehen grundsätzlich der jeweiligen öffentlichen Stelle zu. Dies gilt sowohl für die Inhalte empfangener und versandter E-mails als auch für die Verbindungsdaten. Soweit eine private Nutzung von E-mail-Diensten durch die Bediensteten gestattet ist, gilt hinsichtlich der Inhaltsdaten der elektronischen Post sowie der Verbindungsdaten das – seitens der öffentlichen Stelle zu wahrende – Fernmeldegeheimnis. Verbindungsdaten kann die öffentliche Stelle in geeigneter Form speichern, soweit diese notwendig sind, um die Inanspruchnahme des E-mail-Dienstes gegenüber Bediensteten unmittelbar abzurechnen oder zur Abrechnung an Dritte weiterzugeben (§ 6 TDDSG).

Der LfD hat zu dem dargestellten Themenkreis Hinweise herausgegeben, die als Anlagen 21 und 22 abgedruckt sind.

20.2 Anwendung des Medienrechts

Der Betrieb eines WWW-Servers wird unter gewissen Voraussetzungen dem medienrechtlichen Bereich zugerechnet. Die Abgrenzung, wann Inhalte unter den Mediendienste-Staatsvertrag oder unter das Teledienstegesetz fallen, ist mitunter schwierig. Kriterien zur Abgrenzung liefert der Erwägungsgrund zu § 2 Abs. 2 Nr. 2 TDG (vgl. Bundestagsdrucksache 13/7385): „Die hier erfassten Dienste können unterschiedliche Informationen zum Inhalt haben. Beispielhaft aufgeführt sind für die individuelle Nutzung bestimmte Datendienste wie Verkehrs-, Wetter-, Umwelt- und Börsendaten; hierzu zählen aber auch Einzelgewerbeangebote über Waren und Dienstleistungen sowie sonstige Angebote und Anzeigen (z. B. Homepages). Nicht erfasst sind Datendienste, die mit dem Ziel der Meinungsbildung für die Allgemeinheit redaktionell aufbereitet sind, beispielsweise Textdienste in der elektronischen Presse."

Nach § 7 MDStV gilt für die Angebote in allen Mediendiensten die „verfassungsmäßige Ordnung". Dieser Begriff ist gleichzusetzen mit dem Begriff der verfassungsmäßigen Ordnung in Artikel 2 Abs. 1 GG. Er umfasst auch die in § 7 Abs. 1 Satz 2 MDStV genannten allgemeinen Gesetze und gesetzlichen Bestimmungen zum Schutz der persönlichen Ehre. Dieser Bereich hat im Hinblick auf die Mediendienste besondere Bedeutung. Bei journalistisch-redaktionell gestalteten Angeboten sind, soweit sie der Berichterstattung dienen und Informationsangebote enthalten, die anerkannten journalistischen Grundsätze – insbesondere die Sorgfaltspflicht sowie die Pflicht zur Trennung zwischen Kommentar und Berichterstattung – zu beachten.

Bei Mediendiensten können personenbezogene Daten in vielfältiger Weise anfallen, kombiniert oder verändert werden. Eine Erhebung, Verarbeitung und Nutzung personenbezogener Daten findet nicht nur in einer Datenverarbeitungsanlage, sondern auch im Netz unter Beteiligung zahlreicher anderer Stellen statt. Normadressat ist der einzelne Anbieter. Er soll das Angebot seiner Mediendienste an dem Ziel ausrichten, dass keine oder jedenfalls so wenige personenbezogene Daten der Nutzer wie unbedingt notwendig erhoben, verarbeitet und genutzt werden. Die Datenschutzbestimmungen des Staatsvertrages knüpfen an das vorhandene Instrumentarium des Datenschutzrechts an. Ausgangspunkt für die Regelungen ist das verfassungsrechtlich verbürgte Recht auf informationelle Selbstbestimmung. Das traditionelle Datenschutzkonzept wird ergänzt, soweit die Risiken der neuen Mediendienste dies erforderlich machen (vgl. dazu auch 16. Tb., Tz. 20.4).

Wird beispielsweise festgestellt, dass eine WWW-Seite als Mediendienst einzuordnen ist, greifen u. U. auch die Regelungen zur Gegendarstellung. In diesem Zusammenhang ist darauf hinzuweisen, dass der Gegendarstellungsanspruch nur gegen einen Anbieter i. S. v. § 6 Abs. 2 MDStV besteht. Davon zu unterscheiden ist die Regelung in § 3 Nr. 1 MDStV, wonach Anbieter ist, wer Mediendienste zur Nutzung bereitstellt oder den Zugang zur Nutzung vermittelt. Indessen betrifft § 6 Abs. 2 MDStV einschränkend lediglich Anbieter von journalistisch-redaktionell gestalteten Angeboten, in denen vollständig oder teilweise Inhalte periodischer Druckerzeugnisse in Text oder Bild wiedergegeben oder in periodischer Folge Texte verbreitet werden.

Diese Gesichtspunkte hat der LfD besonders gegenüber Schulen und Kommunen hervorgehoben, die in ihrem Internet-Angebot über bloße Sachinformationen hinausgegangen sind und z. B. auch Presseerklärungen über ihre Tätigkeit veröffentlicht haben.

20.3 Vierter Rundfunkänderungsstaatsvertrag

Im Rahmen der Ministerpräsidentenkonferenzen im April und Juni 1999 konnten von den Chefs der Staats- und Senatskanzleien die letzten offenen Punkte des Vierten Rundfunkänderungsstaatsvertrages geklärt werden. Er dient sowohl der Umsetzung der 1997 verabschiedeten EG-Ergänzungsrichtlinie zur Fernsehrichtlinie von 1989 als auch des 1998 zur Ratifikation aufgelegten Änderungsprotokolls zum Europaratsübereinkommen über das grenzüberschreitende Fernsehen. Des Weiteren werden Regelungen zum digitalen Fernsehen getroffen.

Mit der Markteinführung des digitalen Fernsehens eröffnen sich für die Veranstalter 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 Interessen und Sehgewohnheiten registriert und damit Mediennutzungsprofile einzelner Zuschauer erstellt werden. Die Staats- und Senatskanzleien hatten in Abstimmung mit Vertretern der Landesdatenschutzbeauftragten Vorschläge für die Änderung des Rundfunkstaatsvertrages vorgelegt. Von Bedeutung sind insbesondere folgende Regelungen:

– Die Gestaltung technischer Einrichtungen muss sich an dem Ziel ausrichten, dass so wenig personenbezogene Daten wie möglich verarbeitet werden;

– die Rundfunkveranstalter müssen dem Nutzer die Inanspruchnahme von Rundfunk und seine Bezahlung anonym oder unter Pseudonym ermöglichen, soweit dies technisch möglich und zumutbar ist;

– personenbezogene Daten über die Inanspruchnahme einzelner Sendungen dürfen für Abrechnungszwecke nur gespeichert werden, wenn der Nutzer einen Einzelnachweis verlangt.

Insgesamt wurden die Datenschutzbestimmungen des Rundfunkstaatsvertrages mit denen des Mediendienste-Staatsvertrages aus dem Jahre 1997 harmonisiert, also die Vorgaben des Mediendienste-Staatsvertrages an die Bedingungen des Rundfunks angepasst, um für Mediendienste und Rundfunk einen gleichmäßig hohen Datenschutzstandard sicherzustellen.

Die Position der Datenschutzbeauftragten des Bundes und der Länder zu diesem Thema wurde in einer Entschließung der DSB-Konferenz verdeutlicht (s. Anlage 4).

Der Staatsvertrag ist zwischenzeitlich den Landtagen zur Beratung und Beschlussfassung zugeleitet worden und soll bis zum 1. April 2000 in Kraft treten.

20.4 Rundfunkrechtliche Überwachungskompetenz des LfD

Der LfD hat anlässlich der Erörterung der Aufsichtsregelungen des Entwurfs eines Vierten Rundfunkänderungsstaatsvertrages seine Überwachungskompetenz bei den (privaten) Veranstaltern nach § 53 LRG thematisiert. Danach könnte der für öffentliche Stellen des Landes Rheinland-Pfalz zuständige LfD beispielsweise einen in Mainz angesiedelten privaten Veranstalter bezüglich der Einhaltung der Datenschutzbestimmungen überwachen. Nach Satz 2 dieser Vorschrift gelten die Bestimmungen des LDSG über die Aufgaben und Befugnisse des LfD entsprechend, so dass der private Veranstalter auch Einsicht in die nicht dem Medienprivileg zuzuordnenden Unterlagen und Akten, die im Zusammenhang mit der Verarbeitung personenbezogener Daten stehen, sowie jederzeit Zutritt zu allen Diensträumen zu gewähren hätte.

Da dies einen Systembruch in der Aufsichtsregelung des Landesrundfunkgesetzes darstellt, ist beabsichtigt, im Rahmen der Anpassung des Landesrundfunkgesetzes an den Rundfunkstaatsvertrag nunmehr die Überwachungskompetenz des LfD bei den privaten Veranstaltern (§ 53 LRG) in anderer Weise zu regeln. Es ist vorgesehen, den entsprechenden Gesetzentwurf noch in diesem Jahr dem Landtag zuzuleiten.

20.5 Evaluierung des Informations- und Kommunikationsdienste-Gesetzes

Die Bundesregierung hat im Juni 1999 den vom Bundeswirtschaftsministerium vorgelegten Erfahrungsbericht zum Informations- und Kommunikationsdienste-Gesetz beschlossen, das zeitgleich mit dem Mediendienste-Staatsvertrag der Länder am 1. August 1997 in Kraft getreten ist. Dieses Gesetz enthält nach Auffassung des LfD richtungsweisende Ansätze, wobei neue Wege in der Gestaltung rechtlicher Rahmenbedingungen beschritten wurden, mit denen dem grundlegenden Wandel und der Dynamik der technischen Entwicklung bei den neuen Informations- und Kommunikationsdiensten Rechnung getragen werden soll (vgl. 16. Tb., Tz. 20.3).

Bei der Verabschiedung des Informations- und Kommunikationsdienste-Gesetzes hat der Deutsche Bundestag einen Entschließungsantrag zur Evaluierung des Gesetzes angenommen. Darin wird die Bundesregierung aufgefordert, die technische und rechtliche Entwicklung bei den neuen Diensten zu beobachten und darzulegen, ob und ggf. in welchen Bereichen Anpassungs- bzw. Ergänzungsbedarf besteht. Dabei sollten auch die Erfahrungen der Länder bei der Umsetzung des Mediendienste-Staatsvertrages, die Entwicklung in Deutschland im Vergleich zu anderen Nationen sowie u. a. die folgenden Punkte Berücksichtigung finden:

– Abgrenzung des Informations- und Kommunikationsdienste-Gesetzes gegenüber dem Mediendienste-Staatsvertrag,
– Verantwortlichkeit der Diensteanbieter,
– Akzeptanz der neuen Dienste im Hinblick auf den Datenschutz,
– Entwicklung digitaler Signaturen.

In dem Zeitraum seit dem In-Kraft-Treten dieses Gesetzes im Juli 1997 hat sich gezeigt, dass insbesondere das Teledienstedatenschutzgesetz mit seinen modernen Regelungen zur Datensparsamkeit, zu anonymen und pseudonymen Nutzungsmöglichkeiten von Telediensten und zur strikten Begrenzung der Verarbeitung von Nutzungsdaten und der Profilbildung eine wichtige Voraussetzung dafür geschaffen hat, dass Tele- und Mediendienste datenschutzgerecht gestaltet werden. Die Datenschutzbeauftragten des Bundes und der Länder haben die Übernahme dieser Grundsätze bei der Novellierung des Bundesdatenschutzgesetzes empfohlen.

In einer Pressemitteilung der Bundesregierung zum Evaluierungsbericht heißt es:

> „Das Multimediagesetz hat eine wichtige Grundlage für die Entwicklung von E-Commerce in Deutschland gelegt. Die moderne Ausgestaltung des Gesetzes hat auch zu einer breiten Akzeptanz neuer Medien in Deutschland geführt. Insbesondere die Gewährleistung eines sicheren elektronischen Geschäftsverkehrs hat zu einem starken Anstieg der Internetnutzer beigetragen. Allein 1998 stieg die deutsche Internetgemeinde um 32 Prozent auf 7,3 Mio Nutzer. Im Jahr 1999 wird voraussichtlich die Zehn-Millionen-Schwelle überschritten. (...).

Mit dem IuKDG wurden verlässliche rechtliche Rahmenbedingungen für Anbieter und Nutzer geschaffen. Diese sind wesentliche Voraussetzung für die wirtschaftliche Erschließung der neuen Dienste in Deutschland. Mit der Neuorientierung der Medienordnung, d. h. der Dreiteilung der Medienangebote in Teledienste, Mediendienste und Rundfunk, wurde ein tragfähiges, wenn auch mit Blick auf die Globalisierung der Märkte und Konvergenz der einzelnen Branchen weiter zu entwickelndes Regulierungsmodell geschaffen. Die bisherige Praxis hat gezeigt, dass in wichtigen Angebots- und Nutzungsbereichen eine eindeutige Zuordnung zu den einzelnen Kategorien möglich ist. Deutschland hat mit dem Multimediagesetz die internationale Diskussion zu EU- und weltweiten Standards für die neuen Dienste maßgeblich bestimmt; dies betrifft die Zulassungs- und Anmeldefreiheit für neue Dienste ebenso wie die Regelungen zur Haftungsprivilegierung der Provider, die Regelungen zu sicheren digitalen Signaturen und zum Jugendschutz mit der gesetzlichen Verankerung der freiwilligen Selbstkontrolle und dem technischen Selbstschutz (z. B. Filtertechnologien). Ansatzpunkte für einen grundlegenden Novellierungsbedarf beim IuKDG haben sich bisher nicht ergeben. Es hat sich aber gezeigt, dass in einzelnen Regelungsbereichen, insbesondere beim Verbraucherschutz und Jugendschutz, gesetzlicher Anpassungsbedarf besteht, um die Akzeptanz der neuen Dienste auf der Nutzerseite zu erhöhen und die Bedingungen für die Informationsgesellschaft in diesem Bereich zu verbessern. Im Datenschutz müssen die verschiedenen Regelungen besser aufeinander abgestimmt und damit mehr Transparenz für die Anbieter geschaffen werden. Weiterer Anpassungsbedarf ergibt sich aus der Umsetzung der zurzeit beratenen EG-Richtlinien zu elektronischen Signaturen und zu rechtlichen Aspekten des elektronischen Geschäftsverkehrs."

20.6 Schlussbericht der Enquete-Kommission „Zukunft der Medien in Wirtschaft und Verwaltung"

Die mit den neuen Medien entstandenen Risiken für das informationelle Selbstbestimmungsrecht beruhen auf spezifischen Merkmalen der Datenverarbeitung in den globalen Datennetzen: Dort fallen in erheblichem Umfang personenbezogene Daten an. Sie können leicht gespeichert, übermittelt, verarbeitet und zusammengeführt werden. Daraus ergeben sich Möglichkeiten der Überwachung und der Profilbildung.

Die datenschutzpolitische Forderung, zur Förderung der Akzeptanz neuer Anwendungen der Informationstechnik auch anonyme Nutzungsmöglichkeiten vorzusehen (vgl. u. a. Entschließung der 54. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 23./24. Oktober 1997, Anlage 3) hat in der Zwischenzeit erfreulicherweise an Dynamik gewonnen. Dies kommt in dem Schlussbericht der Enquete-Kommission „Zukunft der Medien in Wirtschaft und Verwaltung" des Deutschen Bundestages zum Ausdruck (Bundesratsdrucksache 13/1104). So werden dort „Maßnahmen gefordert, die eine datensparsame Gestaltung der in Telekommunikationsnetzen verwendeten Geräte, Programme und Übertragungswege vorsehen (...). Um die Gebote der Datensparsamkeit und der Datenvermeidung zu erfüllen, sollte die anonyme und pseudonyme Nutzung der neuen Dienste gefördert werden."

Ein weiterer begrüßenswerter Ansatz ist dem Schlussbericht zu entnehmen: Es wurde die Einrichtung eines Bund-Länder-Kommunikationsrates gefordert (S. 27, 119). Der Rat soll Koordinierungsaufgaben im Bereich von Rundfunk, Mediendiensten und Telekommunikation wahrnehmen und damit das „Risiko von Fehlentscheidungen" aufgrund der „jetzigen Zersplitterung von medienpolitischen Zuständigkeiten" verhindern. Hintergrund dieser Forderung sind befürchtete Rechts- und Kompetenzstreitigkeiten, die letztlich zu Lasten der betroffenen Nutzerinnen und Nutzer gehen.

20.7 Einigung auf EG-Signaturrichtlinie

Mit ihrem Richtlinienvorschlag vom Mai 1998 über gemeinsame Rahmenbedingungen für elektronische Signaturen hat die Europäische Kommission das Gesetzgebungsverfahren für eine einheitliche europäische Regelung eingeleitet. Im April 1999 haben sich die für Telekommunikation zuständigen EU-Minister auf einen gemeinsamen Richtlinienvorschlag für elektronische Signaturen geeinigt. Der Richtlinienvorschlag wurde dem Europäischen Parlament vorgelegt. Mit einer Annahme der Richtlinie ist im Dezember 1999 zu rechnen. Einige Bestimmungen der Richtlinie weichen erheblich vom deutschen Signaturgesetz ab. Beispielsweise sieht der Richtlinienvorschlag im Gegensatz zum deutschen Recht in Artikel 3 einen freien Marktzugang für Zertifizierungsstellen ohne vorherige zwingende Genehmigung vor. Bezogen auf die Bundesrepublik Deutschland bedeutet dies, dass Unternehmen nach Umsetzung des Richtlinienvorschlages keinen Antrag mehr bei der Regulierungsbehörde stellen müssen, um eine Zertifizierungsstelle zu gründen, die rechtsverbindliche Signaturen ermöglicht. Die Mitgliedstaaten können allerdings so genannte Akkreditierungssysteme einführen oder beibehalten, nach denen Zertifizierungsstellen auf freiwilliger Basis lizenziert werden können.

Entscheidungsspielraum verbleibt dem deutschen Gesetzgeber hinsichtlich elektronischer Signaturen im öffentlichen Bereich. Hier sieht Artikel 3 Abs. 4 des Richtlinienvorschlags ausdrücklich vor, dass solche Signaturen von weiteren Anforderungen abhängig gemacht werden können. Dennoch besteht im Hinblick auf die grundsätzliche Genehmigungsfreiheit nach europäischem Recht Anpassungsbedarf für das deutsche Signaturgesetz.

Die nunmehr in Artikel 6 vorgesehene Haftungsregelung für Zertifizierungsstellen war zwischen den Mitgliedstaaten äußerst umstritten. So sieht der Richtlinienvorschlag eine Gefährdungshaftung mit Umkehr der Beweislast vor, um die rechtliche Sicherheit der Signaturen sowie der mit ihnen abgeschlossenen Verträge zu garantieren. Das deutsche Signaturgesetz hingegen enthält keine Regelungen zur Frage der Haftung. Auch hier besteht also Anpassungsbedarf. Der deutsche Ansatz (hohe Sicherheitsanforderungen an Stelle einer Haftungsregelung) hat sich nicht durchsetzen können.

21. Technischer und organisatorischer Datenschutz

21.1 Kontroll- und Beratungstätigkeit

Im Berichtszeitraum wurden in 39 Fällen unter technisch-organisatorischen Gesichtspunkten örtliche Feststellungen nach § 24 Abs. 1 LDSG in unterschiedlichen Bereichen der staatlichen und kommunalen Verwaltung getroffen, u. a. bei folgenden Stellen:

- AOK Rheinland-Pfalz,
- Beauftragte der Länder für den Jugendschutz,
- Berufsbildungszentrum Worms,
- Daten- und Informationszentrum,
- Gymnasien,
- Krebsregister Rheinland-Pfalz,
- Kreisverwaltungen Bitburg und Bernkastel-Wittlich,
- Landeskriminalamt Rheinland-Pfalz,
- Ministerium des Innern und für Sport,
- Oberfinanzdirektion Koblenz,
- Polizeidirektion Landau,
- Polizeipräsidium Ludwigshafen,
- Stadtverwaltung Ludwigshafen,
- Stadtverwaltung Neuwied,
- Statistisches Landesamt,
- Universität Trier,
- Verfassungsschutz,
- Zentrum für Benutzerservice und Informationstechnik der Forstverwaltung.

Ergänzt wurden diese durch 27 Beratungen nach § 24 Abs. 4 LDSG.

Die Kontrollen erfolgten sowohl anlassbezogen, z. B. aufgrund von Eingaben oder Anmeldungen, als auch in Form allgemeiner Prüfungen der getroffenen technisch-organisatorischen Maßnahmen beim Einsatz der Informationstechnik. Im Vordergrund standen dabei jeweils die Zugriffsmöglichkeiten auf gespeicherte personenbezogene Daten, die Nachvollziehbarkeit der automatisierten Verarbeitung und die Löschung nicht mehr erforderlicher Daten. Soweit die getroffenen Maßnahmen datenschutzrechtlichen Anforderungen nicht entsprachen, 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. Daneben hat er in Einzelfragen zu technisch-organisatorischen Punkten Unterstützung geleistet.

Die Schulungsaktivitäten wurden fortgeführt. Angesichts der sich aus der Nutzung des Internets ergebenden Fragestellungen ist in diesem Bereich eine gewisse Ausweitung erfolgt. Darüber hinaus hat der LfD die Angebote des DIZ wahrgenommen, auf dessen Anwenderforen zu einzelnen Technikfragen die datenschutzrechtliche Beurteilung darzustellen.

21.2 Technisch-organisatorische Datenschutzfragen in ausgewählten Verfahren

21.2.1 Internet-Firewall des LDKN

Im 16. Tb. (Tz. 21.4.2) hatte der LfD zum vorgesehenen Konzept des DIZ zur Sicherung des LDKN gegenüber Zugriffen aus dem Internet Stellung genommen und Empfehlungen zur Konfiguration und zum Betrieb ausgesprochen. Zwischenzeitlich wurde eine Firewall-Struktur aufgebaut und in Betrieb genommen. Hierzu sind örtliche Feststellungen hinsichtlich

- der Sicherheitsrichtlinien des DIZ,
- dem sicheren Einsatz der Internet-Protokolle und -Dienste,
- der Anordnung der Firewall-Komponenten,
- der Implementierung geeigneter Filterregeln,
- der Protokollierung sowie
- der Notfallvorsorge

erfolgt. Die technische Umsetzung des seinerzeitigen Konzepts ist im Wesentlichen abgeschlossen; die Empfehlungen des LfD hierzu wurden dabei weitgehend berücksichtigt. Es handelt sich um eine gestaffelte Firewall-Lösung, bei der sowohl am zentralen Übergang zum Internet als auch den Übergängen zum Verwaltungsnetz eine Kontrolle, Filterung und Protokollierung von Zugriffen erfolgt.

Den gegenwärtig bedeutsamen Risiken bei der Internet-Kommunikation wird, soweit es den Verantwortungsbereich des DIZ betrifft, weitgehend Rechnung getragen. Gleichwohl verbleiben, nicht zuletzt aufgrund der technischen Entwicklungen im Internet, Gefährdungen für die angeschlossenen Endsysteme.

So stellt das zugrunde liegende TCP/IP-Protokoll bislang keine sicheren Mechanismen zur Wahrung der Vertraulichkeit bereit. Bei vielen gängigen Diensten werden die Inhaltsdaten im Klartext übertragen. Mit speziellen Programmen kann der Datenverkehr im Netz abgehört, mitgeschnitten und nach relevanten Informationen durchsucht oder auch manipuliert werden. Datenpakete können abgefangen werden, so dass sie nicht an ihrem Ziel ankommen; ein Angreifer kann sie durch eigene Pakete ersetzen. Nicht allen protokoll- und dienstespezifischen Risiken kann durch eine zentrale Firewall begegnet werden. Je nach genutztem Dienst muss die erforderliche Sicherheit bis auf Anwendungsebene bzw. für das jeweilige Endsystem gewährleistet sein. Dies gilt nicht zuletzt für die in vielen Internet-Angeboten enthaltenen aktiven Komponenten (ActiveX, Java-Scripts). Zwar können diese über geeignete Programme ausgefiltert oder ihre Ausführung in den Browsern der Endsysteme unterbunden werden, in der Regel ist dies jedoch mit einer Einschränkung der Nutzungsmöglichkeit verbunden. Die betroffenen Verwaltungen stehen damit in der Pflicht, in den von der DIZ-Firewall nicht erfassten Bereichen für eine verantwortungsvolle Nutzung des Internets Sorge zu tragen und ggf. zusätzliche Maßnahmen zu ergreifen (vgl. die Orientierungshilfe der Datenschutzbeauftragten des Bundes und der Länder zum Anschluss öffentlicher Stellen an das Internet, Anlage 23).

Eine Prüfung auf per elektronischer Post übertragene Computerviren wird von der Firewall des DIZ bislang lediglich für den Bereich der X.400-Kommunikation gewährleistet. Die Ausweitung auf Internet-Mail steht noch aus. Ohnehin erfasst die Prüfung des DIZ nur die Kommunikation, die über den zentralen Internet-Zugang des DIZ abgewickelt wird. Nachrichten, die via elektronischer Post innerhalb des Verwaltungsnetzes ausgetauscht werden, unterliegen dieser Virenprüfung nicht. Hier sind die angeschlossenen Verwaltungen im Rahmen der gegenwärtig bereits bestehenden Anforderungen gehalten, einen ausreichenden Virenschutz in eigener Verantwortung sicherzustellen.

Die Notwendigkeit von Anpassungen besteht aus Sicht des LfD weiterhin im Bereich organisatorischer bzw. übergreifender Regelungen. So liegen die Sicherheitsrichtlinien für die Internet-Anbindung des LDKN (Sicherheitspolitik) bislang nicht in schriftlicher Form vor. Eine generelle, verbindliche Vorgabe für DIZ-Mitarbeiter bzw. als Vertragsbestandteil für die angeschlossenen Verwaltungen steht damit aus, ebenso eine vom LfD geforderte Risikoanalyse mit daraus resultierender Schutzbedarfsfeststellung (vgl. 16. Tb., Tz. 21.4.1).

Die im Falle einer Kompromittierung des Netzes zu treffenden Maßnahmen sowie ein entsprechender Notfallplan sind bislang nicht schriftlich dokumentiert. Damit besteht aus Sicht des LfD die Gefahr, dass bei möglichen Sicherheitsvorfällen nicht in angemessener Weise reagiert werden kann.

Die technischen Maßnahmen sind, soweit bereits implementiert, zur Absicherung des Internet-Zugangs des LDKN grundsätzlich geeignet. In Teilbereichen steht die Umsetzung noch aus. Um eine Kontrolle der Firewall unter realistischen Bedingungen zu ermöglichen, hat der LfD u. a. empfohlen, von außerhalb einen „Penetrationstest“ unter Einsatz des hierzu verfügbaren Instrumentariums durchführen zu lassen. Eine angemessene Sicherheit ist dauerhaft nur zu erzielen, wenn sichergestellt ist, dass eine permanente Pflege der Konfiguration und die Anpassung an sich ändernde Risiken erfolgt. Die Organisation der Firewall-Administration muss darauf abgestimmt sein.

Entsprechend der Empfehlung des LfD sollte im Rahmen eines LDKN-Sicherheitskonzepts eine Schutzbedarfsfeststellung vorgenommen werden, um die hinsichtlich der Vertraulichkeit, Integrität und Verfügbarkeit bestehenden Anforderungen zu konkretisieren und gezielt darauf abgestimmte technische Maßnahmen zu treffen.

Um eine schnelle und angemessene Reaktion im Fall einer Kompromittierung des Netzes zu ermöglichen, hat der LfD empfohlen, die einzuleitenden Schritte und zu treffenden Maßnahmen in einem Notfallhandbuch festzulegen.

21.2.2 Verschlüsselung auf dem ATM-Backbone des LDKN

Für die Bereitstellung höherer Bandbreiten im LDKN beabsichtigte das DIZ, den bislang ausschließlich im separaten Bildungsnetz des Landes genutzten ATM-Backbone auch für die Kommunikation der übrigen Landesverwaltung – einschließlich der Polizei – zur Verfügung zu stellen. Bei den hierbei genutzten Netzknoten handelt es sich um Rechner im Eigentum und unter der Kontrolle der Deutschen Telekom. Dies stellte eine Änderung gegenüber der seitherigen Situation dar, bei der die Knotenrechner des LDKN ausschließlich bei Stellen der Landesverwaltung untergebracht waren.

Mit der Einbeziehung von Knotenrechnern eines privaten Kommunikationsanbieters in die Struktur des LDKN stehen diese Übertragungswege nur eingeschränkt unter der Kontrolle des DIZ. Um das bisherige Sicherheitsniveau beizubehalten, waren somit Maßnahmen erforderlich, die der geänderten Situation Rechnung tragen. Dabei war aus Sicht des LfD ein hoher Schutzbedarf zugrunde zu legen. Eine endgültige Einordnung sollte auf der Grundlage einer entsprechenden Risikoanalyse erfolgen.

Zur Sicherung einer ausreichenden Vertraulichkeit und Integrität hat der LfD die kryptografische Verschlüsselung der übertragenen Daten empfohlen (vgl. 16. Tb., Tz. 21.4.1). Damit unabhängig vom gewählten Übertragungsweg eine ausreichende Sicherheit erreicht werden kann, sollte eine technische Lösung folgende Anforderungen berücksichtigen:

– Automatisierte, benutzertransparente Leitungsverschlüsselung zwischen den von der allgemeinen Verwaltung genutzten ATM-Backbone-Knoten. Soweit für einzelne Bereiche des LDKN darüber hinausgehende Sicherheitsanforderungen bestehen (z. B. VPN Polizei), sollte dem ggf. im Wege einer Ende-zu-Ende-Verschlüsselung Rechnung getragen werden.

- Nutzung als sicher anerkannter Verschlüsselungsverfahren (z. B. Triple DES, RSA, IDEA) mit ausreichender Schlüssellänge. Proprietäre Lösungen kommen alternativ in Betracht, wenn diese nachgewiesenermaßen eine vergleichbare Sicherheit bieten.
- Ausreichende Flexibilität hinsichtlich der nutzbaren Algorithmen und Schlüssellängen, um bei geänderter Risikolage oder technischen Änderungen Anpassungen vornehmen zu können.
- Einsatz und Betrieb der Verschlüsselungskomponenten unter der Kontrolle des DIZ. Im Hinblick auf eine zeitnahe Auswertung sicherheitsrelevanter Status- und Fehlermeldungen sollten die Komponenten in das Netzmanagement des DIZ integriert werden.

Zur Orientierung hat der LfD auf die Empfehlungen des BSI zur Umsetzung des Signaturgesetzes verwiesen. Diese sehen u. a. bei den kryptografischen Algorithmen Schlüssellängen von mindestens 1024 Bit (RSA bzw. DSS) und 75 Bit (DES) vor. Die Entscheidung für eine technische Lösung sollte sich jedoch nicht ausschließlich auf die verwendeten Algorithmen und Schlüssellängen stützen. Für die Beurteilung des mit einer bestimmten Lösung verbundenen Sicherheitsniveaus sind darüber hinaus weitere Faktoren wie Schlüsselerzeugung, -verteilung und -management, organisatorische Regelungen oder die Verwendung zertifizierter Produkte von Bedeutung. Soweit im Rahmen der Leitungsverschlüsselung z. B. ein regelmäßiger Wechsel von Session-Keys in kurzen Intervallen erfolgt, kann auch bei kürzerer Schlüssellänge ein ausreichendes Maß an Datensicherheit gewährleistet werden.

Die vom DIZ ins Auge gefassten Anschlusskomponenten unterstützen grundsätzlich die o. g. Empfehlungen. Das im praktischen Einsatz erreichte Maß an Sicherheit hängt jedoch von der konkreten Umsetzung und Nutzung der bereitgestellten Funktionen ab. Neben den kryptografischen Aspekten wird daher die Einbettung in die vorhandene organisatorische und technische Struktur des LDKN zu prüfen sein.

21.2.3 Zugangskontrolle der Knotenrechner des LDKN

Die Knotenrechner des LDKN sind mit wenigen Ausnahmen jeweils in Polizeidienststellen des Landes untergebracht. Neben einer jederzeitigen Zugänglichkeit ist damit insbesondere die Absicht verbunden, die bei der Polizei vorhandene Sicherheitsinfrastruktur für die Zugangskontrolle zu nutzen.

Die bei einzelnen Kontrollen durch den LfD vorgefundene Situation entsprach nicht in jedem Fall den datenschutzrechtlichen Anforderungen. Vorhandene Möglichkeiten wurden teilweise nicht genutzt oder blieben aufgrund von Nachlässigkeiten wirkungslos. Damit der mit der Aufstellung der Knotenrechner in Polizeidienststellen angestrebte Sicherheitseffekt in der Praxis erzielt wird, hat der LfD für die künftige Verfahrensweise Folgendes empfohlen:

- Die Verantwortlichkeiten für die Zugangskontrolle, insbesondere die Schlüsselverwaltung, sind eindeutig festzulegen. Die Räume der Knotenrechner sollten aus der allgemeinen Schließanlage des Gebäudes herausgenommen und mit einem separaten Schloss/Schlüssel ausgestattet werden. Die Zahl vorhandener Schlüssel und (soweit auf Dauer ausgehändigt) deren Empfänger sind zu dokumentieren.
- Beim Zugang durch Fremdpersonal sind Name, Stelle, Datum und Anlass festzuhalten, um eine Nachvollziehbarkeit zu gewährleisten.
- Die Zugangstüren der Räume sollten mit einer automatischen Schließhilfe und mit einem Knauf statt einem Türgriff an der Außenseite ausgestattet werden.
- Die betroffenen Stellen haben mit der Bereitschaft, für die Knotenrechner des LDKN geeignete Räumlichkeiten zur Verfügung zu stellen, einen Teil der Verantwortung für die Sicherheit des LDKN übernommen. Die Bedeutung der Zugangskontrolle für diese Räume wird im Zusammenhang mit der zunehmenden Nutzung der Informationstechnik steigen. Die zuständigen Mitarbeiter sind daher in geeigneter Weise hinsichtlich der bestehenden Sicherheitsanforderungen zu sensibilisieren.

Das Innenministerium hat die erforderlichen Maßnahmen zur Gewährleistung einer den datenschutzrechtlichen Anforderungen entsprechenden Zugangskontrolle zwischenzeitlich in die Wege geleitet.

Die jeweiligen Verwaltungen stellen lediglich die erforderlichen Räumlichkeiten zur Verfügung, die Betreuung und Administration der Komponenten obliegen dem DIZ im Rahmen des LDKN-Betriebs. Welche Anforderungen an die Zugangskontrolle zu berücksichtigen sind, war für die Verwaltungen offenbar nicht mit hinreichender Deutlichkeit erkennbar. Um ein einheitliches Sicherheitsniveau zu gewährleisten, sollten die bestehenden Anforderungen im Vorfeld der Aufstellung klar formuliert werden. Gegenüber dem DIZ wurden in diesem Zusammenhang folgende Empfehlungen ausgesprochen:

- Die Dienststellen sind gegenwärtig nicht in der Lage zu erkennen, welcher Personenkreis eine Zutrittsberechtigung zu den LDKN-Knotenrechnern besitzt. Hier ist es erforderlich, eine Liste der zugangsberechtigten Stellen zur Verfügung zu stellen.
- Für telefonische Rückfragen in Zweifelsfällen ist ein Ansprechpartner beim DIZ, z. B. im Network Information Center, zu benennen.
- Die bestehenden Anforderungen des DIZ für die Aufstellung der Knotenrechner sollten festgeschrieben werden. Hierzu zählen insbesondere die sich aus einem Sicherheitskonzept des DIZ ergebenden räumlichen, technischen und verfahrensmäßigen Anforderungen.

21.2.4 X.500-Verzeichnisdienst der Landesverwaltung

Im Rahmen des Projekts EuroView wurde unter Federführung des DIZ ein X.500-Verzeichnisdienst der Landesverwaltung Rheinland-Pfalz aufgebaut. Für die E-Mail-Kommunikation zwischen Behörden der Landesverwaltung sowie mit Landesverwaltungen anderer Bundesländer via X.400 und SMTP werden darin Angaben über die elektronische Erreichbarkeit gespeichert (Name, Amts- bzw. Funktionsbezeichnung, Dienststelle, Postanschrift, Telefon-/Telefaxnummer, X.400- bzw. Internet-Mailadresse). Nach der vorgesehenen Integration aller staatlichen und kommunalen Verwaltungen wird das Verzeichnis ca. 65 000 elektronische Adressen enthalten.

Nach der vom LfD vertretenen Auffassung (vgl. 16.Tb., Tz. 17.3) unterliegen Amtsträgerdaten wie Name, Amts- und Funktionsbezeichung sowie dienstliche Erreichbarkeitsangaben nicht dem informationellen Selbstbestimmungsrecht. Gegen die Aufnahme der vorgesehenen Adressbestandteile bestanden daher aus datenschutzrechtlicher Sicht keine Bedenken.

Die Möglichkeit, Daten Bediensteter zum elektronischen Abruf für die Allgemeinheit bereitzustellen, ohne dass hierzu die Einwilligung der Betroffenen erforderlich ist, beschränkt sich jedoch grundsätzlich auf Funktionsträger, die im Rahmen ihrer Aufgabenerfüllung nach außen hin tätig werden. Bei einer Bereitstellung der in erster Linie für die Landesverwaltung bereitgestellten Verzeichniseinträge auch außerhalb dieses Bereichs für die Allgemeinheit muss insoweit eine Reduzierung erfolgen bzw. die Einwilligung der Betroffenen eingeholt werden. In bestimmten Fällen kann auch aufgrund von Fürsorgegesichtspunkten eine Beschränkung der Angaben erforderlich werden.

Der LfD hat daher dem DIZ empfohlen, in diesem Fall eine Filterung der Verzeichniseinträge nach dem Gesichtspunkt der internen/externen Bereitstellung vorzunehmen oder die Möglichkeit zu schaffen, dass die Betroffenen selbst eine Sperrung oder Freischaltung bestimmter Attribute vornehmen können. Es ist vorgesehen, das vom DIZ geführte Verzeichnis in das im Aufbau befindliche Trust-Center des DIZ zu integrieren. Im Rahmen des geplanten Einsatzes der digitalen Signatur im elektronischen Schriftverkehr zwischen den Behörden in Rheinland-Pfalz soll das X.500-Verzeichnis für die Verwaltung der erforderlichen Zertifikate genutzt werden.

21.2.5 Elektronische Steuererklärung (ELSTER)

Seit Januar dieses Jahres können Bürger, die über die entsprechende technische Ausstattung verfügen, im Rahmen eines Feldversuchs ihre Steuererklärung auf elektronischem Weg via Internet abgeben. Von der Finanzverwaltung wurde hierzu ein Modul für die Erstellung und elektronische Übermittlung der Einkommensteuererklärung entwickelt, das in die am Markt angebotenen Steuerprogramme integriert werden kann. Das Modul steht den Herstellern von Steuersoftware auf Anfrage kostenlos zur Verfügung. Die Entwicklung des ELSTER-Moduls erfolgte federführend durch die bayerische Finanzverwaltung.

Das Verfahren stellt eine Fortführung der u. a. in Rheinland-Pfalz bereits seit einigen Jahren eingesetzten Datenfernübertragung bei der Abgabe von Einkommensteuererklärungen dar, bei welcher zwischen festgelegten Stellen (DATEV/OFD) Steuerdaten auf elektronischem Weg ausgetauscht wurden. Die nunmehr praktizierte Nutzung des Internets als Transportmedium und die Ausweitung des Teilnehmerkreises erfordern entsprechende Maßnahmen zur Wahrung der Vertraulichkeit und Integrität der Steuerdaten. Diese stellen sich für das ELSTER-Verfahren folgendermaßen dar:

Die im jeweiligen Steuererklärungsprogramm erzeugten Steuerdaten werden vom Anwender via Internet zu einem ELSTER-Server in München übermittelt und von dort weiter an die jeweilige Landesstelle weitergeleitet. In Rheinland-Pfalz handelt es sich hierbei um die Zentrale Datenverarbeitungsstelle der Finanzverwaltung bei der OFD Koblenz. Die weitere Behandlung der Daten entspricht dem bereits bestehenden Verfahren mit der DATEV e. G., d. h. der Zwischenspeicherung auf einem separaten Rechner und der Übernahme der Daten in das reguläre Steuerverfahren nach entsprechenden Plausibilitäts- und Sicherheitsprüfungen. Der Zugriff durch das zuständige Finanzamt erfolgt über die so genannte Telenummer, die gleich lautend in den elektronisch bereitgestellten Steuerdaten sowie der in verkürzter Form weiterhin auf Papier eingereichten Steuererklärung enthalten ist.

Vor der Übertragung werden die Steuerdaten benutzertransparent verschlüsselt und digital signiert. Bei der EDV-Stelle München erfolgt keine Entschlüsselung, hier werden lediglich die im Klartext vorhandenen Angaben über den Empfänger ausgelesen, um via Telebox400-Verfahren der Deutschen Telekom die Weiterleitung zur jeweiligen Landesstelle vorzunehmen. Die Nutzdaten werden bereits auf Anwenderseite vom ELSTER-Modul mit dem Triple DES-Verfahren verschlüsselt. Für jeden Übermittlungsvorgang wird hierzu über einen Zufallsgenerator ein neuer DES-Schlüssel erzeugt (Session-Key). Der Schlüsselaustausch wird über RSA 1024 Bit abgesichert. Hierzu existiert für jedes Bundesland ein eigenes RSA-Schlüsselpaar. Diese werden mit einer von der EDV-Stelle München bereitgestellten Software dezentral in den einzelnen Ländern erzeugt und besitzen eine Gültigkeitsdauer von einem Jahr. Anhand der Landeskennung in der Steuernummer wählt das ELSTER-Modul aus einer internen Tabelle den jeweils erforderlichen öffentlichen RSA-Schlüssel des Empfängers aus. Zur Sicherung der Integrität werden die Steuerdaten vom ELSTER-Modul mit einem weiteren RSA-Schlüssel digital signiert. Der hierfür erforderliche geheime RSA-Schlüssel ist im ELSTER-Modul enthalten.

In einer ersten Stellungnahme hat der LfD das Verfahren folgendermaßen bewertet:

Die genannte Verschlüsselung dient ausschließlich der Sicherung der Steuerdaten bei der Übertragung. Mit den gewählten Algorithmen und Schlüssellängen wird hierfür bei korrekter Implementierung ein ausreichendes Maß an Vertraulichkeit erreicht. Die Verschlüsselung bietet hingegen keinen Schutz gegenüber den Risiken, die sich für den PC des Anwenders bzw. den Server der EDV-Stelle aus einer Internet-Anbindung ergeben. Die hierzu erforderlichen Maßnahmen liegen in der Verantwortung der Anwender. Sowohl die Verschlüsselung als auch die digitale Signatur sind als reine Softwarelösungen realisiert, woraus sich bestimmte Risiken ergeben. Das Ausmaß technisch möglicher Manipulationen hängt davon ab, in welchem Umfang unbefugte Zugriffe auf den PC des Anwenders möglich sind. Eine Gesamtaussage zur Sicherheit des Verfahrens, insbesondere auch im Hinblick auf die Vertraulichkeit der Steuerdaten gegenüber Dritten im Umfeld des Anwenders, muss etwaige Sicherheitsfunktionen der genutzten Steuererklärungsprogramme berücksichtigen. Hierbei handelt es sich regelmäßig um Softwarelösungen von Drittanbietern. Die Verantwortung der Finanzverwaltung erstreckt sich in diesem Zusammenhang lediglich auf die Bereitstellung vertrauenswürdiger, manipulationsfester Programmmodule.

Für das Verfahren werden sich in absehbarer Zeit Veränderungen im Bereich der Kommunikation zwischen dem ELSTER-Server und den Landesstellen ergeben. Der LfD wird daher den weiteren Fortgang des Verfahrens verfolgen.

21.2.6 Internet-Angebot der Polizei Rheinland-Pfalz

Die Polizei Rheinland-Pfalz ist mit einem unterschiedliche Bereiche abdeckenden Informationsangebot im Internet vertreten. Unter anderem werden Fahndungsaufrufe nach Straftätern, Suchmeldungen zu vermissten Personen und Pressemitteilungen bereitgehalten. Zu den in diesem Zusammenhang relevanten datenschutzrechtlichen Aspekten siehe Tz. 21.3.5. Zur technischen Gestaltung des Internet-Angebots hat der LfD in folgender Hinsicht Stellung genommen:

Kopie der im Internet bereitgestellten Inhalte

Nach dem gegenwärtigen Kenntnisstand ist bei für den allgemeinen Zugriff im World Wide Web (WWW) bereitgestellten Daten eine Einschränkung der freien Kopierbarkeit nicht möglich. Damit können Inhalte des Internet-Angebots der Polizei von Dritten beliebig kopiert und auf eigenen Internet-Servern vorgehalten werden (vgl. EUSIS). Dies kann insbesondere für personenbezogene Daten, die lediglich zeitlich befristet im Internet eingestellt werden, von Bedeutung sein (z. B. Fahndungen).

Die Möglichkeiten der Polizei zu erreichen, dass Kopien von Inhalten, deren Speicherungsfrist abgelaufen ist, aus dem Netz entfernt werden, sind daher begrenzt. Eine gewisse Einflussnahme ist dort möglich, wo einem Kreis von Abonnenten Inhalte über Mailing-Listen oder Informationskanäle automatisch zur Verfügung gestellt werden. Soweit auf diesem Weg personenbezogene Daten verteilt werden, sollte die Aufnahme in einen Verteiler von der Verpflichtung abhängig gemacht werden, im Internet-Angebot der Polizei nicht mehr vorgehaltene personenbezogene Daten ebenfalls zu löschen. Dies könnte z. B. als zu bestätigender Hinweis im Rahmen der Abonnementsfunktion realisiert werden.

Authentizität und Manipulationssicherheit der Internet-Inhalte

Die im Internet bereitgestellten Web-Seiten unterliegen dem Risiko der unbefugten Veränderung und Verfälschung; entsprechende und zum Teil spektakuläre Fälle sind aus der Vergangenheit bekannt. Für das Internet-Angebot der Polizei ergibt sich aufgrund der größeren Öffentlichkeitswirkung erfolgreicher vorsätzlicher Manipulationen u. U. eine höhere Gefährdung. Der sicheren Konfiguration und dem sicheren Betrieb der Web-Server kommt damit besondere Bedeutung zu. Insoweit ist auf die Maßnahmenempfehlungen des BSI im IT-Grundschutzhandbuch zu verweisen. Unter anderem sollte sichergestellt sein, dass bei erkannten Schwachstellen, z. B. über CERT-Advisories, regelmäßig eine Überprüfung und ggf. Anpassung der eingesetzten Programme erfolgt.

Gegen Manipulationen, die auf Schwächen der eingesetzten Protokolle beruhen (z. B. DNS-Spoofing) können Vorkehrungen nur in begrenztem Umfang getroffen werden. Die bestehenden Möglichkeiten sind jedoch zu nutzen. Hierzu zählen die Vergabe zufälliger statt aufsteigender Anfragenummern durch den eingesetzten DNS-Server sowie die Protokollierung von Paketen mit unerwarteten Query-IDs. Weiterhin sollte die Möglichkeit, bei DNS-Anfragen IP-Zuordnungen als so genannte „additional information“ mitzuliefern, unterbunden werden.

Da vorsätzliche Manipulationen an den Internet-Seiten der Polizei nicht grundsätzlich auszuschließen sind, sollte zumindest sichergestellt sein, dass Manipulationen oder entsprechende Versuche frühzeitig erkannt werden. Neben einer aussagefähigen Protokollierung ist hierzu die Integrität der im Internet bereitgestellten Daten anhand von Checksummen zu überprüfen und bei Abweichungen eine Meldung an die Systembetreuung zu erzeugen. Auf längere Sicht hält der LfD den Einsatz digitaler Signaturverfahren für geboten. Bei der inhaltlichen Betreuung und Pflege des Angebots ist der Zugriff auf den WWW-Server durch geeignete Maßnahmen der Zugriffskontrolle abzusichern.

Verschlüsselung personenbezogener Daten bei der Übertragung im Internet

Im Rahmen des Zugriffs einzelner Dienststellen bei der Bearbeitung des Internet-Angebots sowie bei der Kommunikation zwischen Bürger und Polizei über HTML-Formulare ist eine Verschlüsselung auf der Basis des Secure Socket Layer-Protokolls (SSL) vorgesehen. Für die bislang vorgesehene Nutzung wird dies als ausreichend angesehen. Für den Fall, dass diese Form der

Verschlüsselung auch zur Absicherung bei der Übertragung vertraulicher Daten vorgesehen ist, wurde darauf hingewiesen, dass die standardmäßige Schlüssellänge im SSL-Protokoll mit 40 Bit nur eine eingeschränkte Sicherheit bietet. Nachgewiesenermaßen ist es mit der verfügbaren Technik möglich, die Verschlüsselung innerhalb kurzer Zeit aufzuheben. Für Anwendungen mit höheren Anforderungen an die Vertraulichkeit ist daher eine größere Schlüssellänge zu wählen (s. Tz. 21.3.11).

Einbindung in die IT-Struktur der Polizei

Gegenwärtig erfolgt der Zugriff auf das Internet-Angebot aus dem Bereich der Polizei über separate Rechner, die über keine Verbindung zu anderen polizeilichen Anwendungen verfügen. Mit der IT-Ausstattung der Polizei im Zusammenhang mit der Entwicklung von INPOL/POLADIS-Neu werden sich hierbei jedoch Änderungen ergeben. Der LfD hält es daher für erforderlich, die besonderen Gefährdungen, die sich aus einer Internet-Anbindung ergeben, in einer Risikoanalyse darzustellen und die notwendigen Maßnahmen in einem Sicherheitskonzept festzulegen.

Den Empfehlungen des LfD wurde, soweit sie den gegenwärtigen Realisierungsstand betreffen, zum Teil direkt durch den Einsatz entsprechender Software und Anpassungen des Angebots Rechnung getragen. Der Einsatz von Signaturverfahren soll erfolgen, sobald die erforderlichen Voraussetzungen im Zusammenhang mit dem X.500-Verzeichnis der Landesverwaltung geschaffen sind (vgl. Tz. 21.2.4).

Für die Absicherung des Remote-Zugriffs auf den WWW-Server im Rahmen der inhaltlichen Pflege des Angebots wird eine Router-Lösung, ergänzt um eine Authentifizierung der beteiligten Komponenten und Benutzer sowie Filterfunktionen eingesetzt.

Wegen der angestrebten Einbindung der Internet/Intranet-Funktionalität auf den Arbeitsplätzen wurden die damit einhergehenden Gefährdungen in Zusammenarbeit mit dem BSI in einer Risikoanalyse dargestellt und die notwendigen Maßnahmen in einem Sicherheitskonzept festgelegt.

Im Blick auf die Information der Internet-Nutzer bei einer Kontaktaufnahme von Bürgern mit der Polizei via E-Mail wurde auf Empfehlung des LfD ein Hinweis in das Angebot eingebaut, mit dem die Absender einer Nachricht vor dem Versand auf die bei der Übertragung bestehenden Risiken, die Verarbeitung der Angaben bei der Polizei, den Verwendungszweck und den möglichen Empfängerkreis hingewiesen werden.

21.2.7 Stimmenauszählungsprogramme bei der Kommunalwahl 1999

Die Unterstützung der diesjährigen Kommunalwahl mit Informationstechnik entsprach weitgehend der des Jahres 1994. Für insgesamt drei Programme zur Stimmenauszählung und -verteilung wurde eine Freigabe durch den Landeswahlleiter erteilt; der LfD wurde zuvor um Stellungnahme gebeten. Die hinsichtlich der eingereichten Programme abgegebenen Empfehlungen des LfD orientierten sich dabei an den im 15.Tb., Tz. 21.2.2 dargestellten Gesichtspunkten.

Danach sollten die eingesetzten Lösungen u. a. zur Sicherstellung der Integrität der Programme und der Wahldaten über geeignete Prüfsummenfunktionen verfügen. Dies wurde vom Landeswahlleiter in den Anforderungskatalog für die Freigabe nach § 53 Abs. 10 KWO übernommen.

Tests der vorgelegten Programme ergaben, dass diese Empfehlung nicht überall umgesetzt war. In einem Fall bestand die Möglichkeit, im Wahllokal anstelle der vorgesehenen eine andere, gegebenenfalls manipulierte, Programmversion einzusetzen, ohne dass dies für die Anwender erkennbar gewesen wäre. In einem weiteren Fall war die Prüfsummenfunktion bei der Zusammenführung der Wahlbezirksergebnisse nicht implementiert. Unzulässige Veränderungen an den Dateien mit den Ergebnissen der Stimmenauszählung auf Wahlbezirksebene hätten damit nicht mit hinreichender Sicherheit erkannt werden können.

Die genannten Defizite wurden bis zur Freigabe durch den Landeswahlleiter behoben und die Integrität der eingesetzten Programme und Wahldaten damit in ausreichendem Umfang sichergestellt.

21.2.8 Overlay-Netz der Verwaltungen des Bundes und der Länder (TESTA)

Bei TESTA handelt es um ein Overlay-Netz der Verwaltungen des Bundes und der Länder, d. h. einen Zusammenschluss der einzelnen Landesnetze. Der direkte Anschluss einzelner Bundesbehörden sowie des Informationsverbunds Berlin-Bonn (IVBB) ist vorgesehen. Netzprovider ist eine Tochterfirma der Deutschen Telekom. Das LDKN ist seit etwa einem halben Jahr an das TESTA-Netz angeschlossen.

Technisch ist das Netz über den Zusammenschluss von Gateways realisiert, die über ein besonderes Protokoll (Frame Relay Link Plus) kommunizieren. Jedes Bundesland verfügt über eine TESTA-Kopfstelle und ist mit drei weiteren Gateways direkt verbunden. Es handelt sich jeweils um Festverbindungen. Das TESTA-Netz ist als geschlossene Teilnehmergruppe konzipiert. An Kommunikationsdiensten sind gegenwärtig lediglich X.400 und SMTP-Mail realisiert, direkte Zugriffe auf Rechner oder Anwendungen des LDKN sind nicht möglich. Das Management des TESTA-Netzes und die Administration der Router liegen beim Provider.

Das TESTA-Netz bildet damit das Rückgrat eines „Corporate Network Verwaltung“ für die länderübergreifende Kommunikation. In datenschutzrechtlicher Hinsicht ist dabei von Bedeutung, dass die Administration der Gateways nicht unter der Kontrolle der angeschlossenen Länder steht. Der Provider hat damit grundsätzlich vollständigen Zugriff auf die über das TESTA-Netz

übertragene Kommunikation. Um eine ausreichende Vertraulichkeit der Daten zu gewährleisten, ist im TESTA-Konzept eine Leitungsverschlüsselung vorgesehen. Diese wurde bislang nicht realisiert, da seitens der beteiligten Stellen keine Einigung über die einzusetzenden Komponenten erzielt wurde. Diese müssen einheitlich, zumindest jedoch kompatibel hinsichtlich der genutzten Algorithmen und Schlüssel sein. Die über das TESTA-Netz übertragenen Daten werden damit in einer für den Provider lesbaren Form übertragen. Da sich die im TESTA-Netz verfügbaren Dienste bislang auf die Mail-Kommunikation beschränken, besteht bei besonderen Vertraulichkeits- oder Integritätsanforderungen gegenwärtig die Möglichkeit der Absicherung auf Anwendungsebene (vgl. Tz. 21.3.11). Diese muss jedoch durch die beteiligten Stellen jeweils gesondert eingesetzt werden. Falls wie vorgesehen, die über TESTA verfügbaren Dienste ausgeweitet werden und direkte Verbindungen zu Systemen innerhalb der jeweiligen Sub-Netze hergestellt werden können, wäre ohne Verschlüsselung gegebenenfalls der Zugriff auf Login-Vorgänge, d. h. insbesondere Passworte, möglich. Der LfD hat daher auf die Notwendigkeit hingewiesen, baldmöglichst die vorgesehene Leitungsverschlüsselung zu realisieren und damit eine generelle, von den auf Anwendungsebene genutzten Diensten unabhängige, Vertraulichkeit sicherzustellen. Dies entspräche der gegenwärtig bereits im Informationsverbund Berlin-Bonn bestehenden Situation.

21.2.9 Vorgangsbearbeitungs- und -verwaltungssystem der Polizei (POLADIS-neu)

Die Vorgangsbearbeitung im Bereich der Polizei stützt sich, soweit sie automatisiert erfolgt, im Wesentlichen auf das Verfahren POLADIS (siehe hierzu insbesondere 13. Tb., Tz. 5.9 und 14. Tb., Tz. 5.11). Aufgrund technischer Entwicklungen und geänderter Anforderungen an die Funktionalität des Verfahrens wurde eine Neuentwicklung in Angriff genommen.

Die als künftige INPOL-Landeskomponente für Rheinland-Pfalz vorgesehene Vorgangsbearbeitung wird gegenwärtig unter der Bezeichnung „POLADIS-neu“ entwickelt. Wegen des engen Zusammenhangs dieses Landesmoduls und INPOL-neu wurde mit dem Ministerium des Innern und für Sport eine entwicklungsbegleitende Beteiligung des LfD vereinbart, um datenschutzrechtlich relevante Fragen zu einem möglichst frühen Zeitpunkt klären zu können.

Gegenwärtig werden in Rheinland-Pfalz drei Verfahren für die Vorgangsbearbeitung bzw. -verwaltung der Polizei eingesetzt:

- „POLADIS“, eine proprietäre Mehrplatzlösung auf Systemen der mittleren Datentechnik als Standardlösung der Polizeidienststellen für zentrale Aufgaben der Vorgangsverwaltung und -bearbeitung,
- „POLADIS 95“, eine windowsbasierte Einzelplatzlösung mit den wesentlichen Bearbeitungsfunktionen für Stellen, die nicht über POLADIS (alt) verfügen, sowie
- „AVP“ als DOS PC-Einzelplatzlösung einzelner Dienststellen für die Asservaten- und Vorgangsverwaltung.

Mit der flächendeckenden Einführung von POLADIS-neu werden in Rheinland-Pfalz die bisherigen Verfahren vollständig abgelöst. Ein Migrationskonzept für vorhandene Datenbestände wird gegenwärtig entwickelt. Parallel zur Entwicklung von POLADIS-neu erfolgt der Aufbau einer entsprechenden IT-Infrastruktur auf der Basis vernetzter NT-Systeme. Insgesamt werden ca. 150 Lokationen der Polizei mit aktueller Informationstechnik ausgestattet.

Von den ca. 300 bis 400 Anwendungsfällen der Vorgangsbearbeitung und -verwaltung der Polizei sind bislang ca. 80 beschrieben; diese decken etwa 80 % der in der Praxis vorkommenden Fälle ab. Für ca. 50 Anwendungsfälle wurde bereits eine Schutzbedarfsanalyse vorgenommen. Die Bereiche Fahndung/Recherche, Statistik und Gefahrenabwehr stehen noch aus. Diese sowie weitere Anwendungsfälle sollen in der Teilleistung 2 (Projektteil INPOL-neu) beschrieben werden. Noch nicht endgültig entschieden ist über das Datenhaltungskonzept für POLADIS-neu (zentral/dezentral/Mischform).

Eine grundsätzliche Thematisierung datenschutzrechtlicher Aspekte der polizeilichen Vorgangsverwaltung ist im Übrigen seinerzeit im Zusammenhang mit der ursprünglich vorgesehenen Übernahme des Hamburger Verfahrens COMVOR erfolgt (siehe 15. Tb., Tz. 21.2.1). Die hierbei angesprochenen Punkte bilden auch weiterhin die Grundlage bei der Beurteilung des künftigen Vorgangsverwaltungssystems durch den LfD.

21.2.9.1 Risikoanalyse und Sicherheitskonzept

Eine eigene Arbeitsgruppe „Informationssicherheit“ befasst sich im Rahmen der Entwicklung von POLADIS-neu mit den Datenschutz- und Datensicherheitsanforderungen an die künftige Lösung. Hierzu wurde auf der Grundlage des IT-Grundschutz- und IT-Sicherheitshandbuchs eine Schutzbedarfsanalyse der „polizeilichen Anwendungsfälle“ erstellt. Weiterhin ist die Einrichtung eines IT-Sicherheitsmanagements für den Bereich der Polizei vorgesehen. Die vorgelegte Schutzbedarfsanalyse wurde vom LfD in folgender Hinsicht problematisiert:

Die Analyse berücksichtigt lediglich die Grundbedrohungen Vertraulichkeits-, Integritäts- und Verfügbarkeitsverlust. Ausführungen zur Gewährleistung der Authentizität bzw. Verbindlichkeit gespeicherter Daten sind bislang nicht enthalten. Aus Sicht des LfD ist insbesondere im Zusammenhang mit der Ausweitung der elektronischen Kommunikationsmöglichkeiten im Bereich der Polizei (E-Mail, Datenaustausch mit den Staatsanwaltschaften) davon auszugehen, dass dieser Punkt künftig an Bedeutung gewinnt. Der LfD hat daher empfohlen, dies bei weiteren Risikoanalysen zu berücksichtigen.

Für die Vorgangsverwaltungsdaten bestimmter Anwendungsfälle wurde der festgelegte „mittlere“ Schutzbedarf problematisiert, da sich hierbei nach Ansicht des LfD bei bestimmten Delikten bzw. Täter-/Opferpersonen eine besondere Sensibilität der Daten ergeben kann, für die ein mittleres Schutzniveau nicht ausreicht. Dies betrifft insbesondere die Fälle „Strafanzeigenaufnahme, Vorgangsverwaltung, Bericht ans Jugendamt, Anschlussinhaber ermitteln“.

Zum Vergleich wurde auf einen im Zusammenhang mit der Computerunterstützung der Staatsanwaltschaften formulierten Deliktskatalog verwiesen, anhand dessen eine besondere Zugriffsprotokollierung erfolgt. Den Bedenken des LfD soll durch eine entsprechende Gestaltung der Zugriffsrechte (Rollenkonzept) Rechnung getragen werden. Darüber hinaus soll die Anregung des LfD geprüft werden, die Bearbeitung bestimmter Vorgänge an die Beachtung besonderer Zugriffs- oder Protokollmechanismen zu knüpfen.

21.2.9.2 Rollen- und Zugriffskonzept

Den POLADIS-Anwendern (Personen) werden sog. Rollen (Aufgaben/Zuständigkeiten) zugewiesen, diesen wiederum sind einzelne Anwendungsfälle bzw. Funktionen der Geschäftskontrolle (Tätigkeiten) zugeordnet, die auf Objekte (Daten/Programmfunktionen) mit bestimmten Attributen zugreifen. Vorgänge sind ebenso wie Personen einer oder mehreren Dienststellen zugeordnet, beides kann geändert werden. Einzelne Objekte können mit einem Objektschutz (Passwort) versehen werden. Einer Person können bei Bedarf mehrere Rollen zugewiesen werden, so dass sich Zugriffsberechtigungen addieren. Die Definition von Rollen und die Änderung deren Rechte kann nur an zentraler Stelle und landesweit verbindlich erfolgen.

Das vorliegende Rollenkonzept umfasst alle gegenwärtig für den Einsatz von POLADIS-neu relevanten Rollen. Die Empfehlungen des Landesbeauftragten aus der entwicklungsbegleitenden Beteiligung wurden dabei berücksichtigt; gegen das Konzept bestehen aus datenschutzrechtlicher Sicht keine Bedenken.

21.2.9.3 Löschkonzept

Für abgeschlossene Fälle ist anhand vorgegebener Fristen wie bisher eine Prüfung auf Aussonderung bzw. Löschung vorgesehen. Danach sollen halbjährlich bzw. jährlich Kontroll-Listen für abgeschlossene Vorgänge gefertigt werden. Soweit keine ausdrückliche Aufhebung der Löschungsvormerkung erfolgt, werden die Vorgänge nach Ablauf weiterer vier Wochen automatisch gelöscht. Eine Auslagerung abgeschlossener Vorgänge auf ein separates Speichermedium, z. B. eine Archivierung auf Band, wurde vom LfD nicht gefordert. Den datenschutzrechtlichen Anforderungen wird entsprochen, wenn die Vorgänge bis zum Zeitpunkt der Löschung durch besondere Zugriffsregelungen gegen unbefugte Zugriffe geschützt sind und Änderungen des Status oder Aufhebungen der Löschungsvormerkung von der Protokollierung erfasst werden.

21.2.9.4 Protokollierungskonzept

Den Empfehlungen des LfD zur Protokollierung in POLAIDS-neu wurde entsprochen. Danach sollte nachvollziehbar sein, wer wann welche Verarbeitung im Sinne des § 3 Abs. 2 LDSG veranlasst oder durchgeführt hat, wobei Art und Umfang der Protokollierung an der Sensibilität der zu verarbeitenden Daten sowie des Verwendungszwecks zu orientieren sind. Im Einzelnen werden künftig folgende Vorgänge in POLADIS-neu einer Protokollierung unterzogen:

- Funktionsaufrufe in der Vorgangsbearbeitung (Anwendungsfälle/Masken),
- Einrichten, Löschen und Sperren von Benutzern,
- Vergabe und Änderung von Zugriffsrechten,
- Speichern, Ändern und Löschen personenbezogener Daten,
- anwendungsfallbezogene Lesezugriffe auf Vorgangsdaten,
- Abfragen und Recherchen im Datenbestand.

Die Auswertung der Protokolldaten soll nach folgenden Kriterien möglich sein:

- Bearbeitername,
- Dienststelle bzw. Organisationseinheit,
- Vorgangsnummer,
- Datum von/bis (Zeit ist ebenfalls verzichtbar),
- Anwendungsfall bzw. Funktion,
- Art der Änderung.

Um die Zahl der Suchkriterien gering zu halten, sollte nach Auffassung des LfD ein Eingabefeld vorhanden sein, das unabhängig oder in Kombination mit den obigen Kriterien die freie Suche nach Zeichenfolgen in den Protokolltabellen ermöglicht (z. B. „müller“ in Verbindung mit einer Datums- oder Dienststellenangabe).

Für die Ergebnisse von Protokollauswertungen soll die Möglichkeit des Ausdrucks bestehen. Seitens der Projektgruppe wurde der Umfang der Protokolldaten problematisiert. Von Bedeutung war dabei weniger die Länge eines einzelnen Protokollsatzes als vielmehr deren große Zahl, insbesondere der lesenden Zugriffe (80 % der Einträge). Aus Sicht des LfD sind Protokolleinträge, die

lediglich aufgrund lesender Zugriffe automatischer Prozesse erzeugt werden, z. B. durch die regelmäßige Anzeige einer Vorgangsliste bei der Anmeldung des Sachbearbeiters, nicht auswertungsrelevant und können entfallen. Ähnliches gilt für Angaben, die bereits aus den Vorgangsverwaltungsdaten ersichtlich sind (z. B. Erstellungsdatum).

Für die Speicherung der Protokolldaten reicht aus Sicht des LfD unter Berücksichtigung der Erforderlichkeit und der Erfordernisse einer ordnungsgemäßen Dokumentation in der Regel eine Aufbewahrungsdauer von sechs Monaten bis zu einem Jahr aus.

21.2.10 Elektronische Verarbeitung von Arbeitszeit, Abwesenheit und Mehrarbeit bei der Polizei (EVA)

Für den Bereich der Polizei ist vorgesehen, unter der Bezeichnung EVA ein Verfahren für die elektronische Verarbeitung der geleisteten Mehrarbeit einzusetzen. Das Verfahren geht nach den Feststellungen des LfD jedoch über die Erfassung und Abrechnung von Mehrarbeitsvergütungen hinaus. Wesentliche weitere Bestandteile sind die Erfassung und Verwaltung der Arbeitszeit und von Zeiten der Abwesenheit. Zur Gestaltung des Verfahrens im Hinblick auf Zugriffsberechtigungen, Auswertungsmöglichkeiten, Löschungsfristen und Protokollierung hat der LfD daher folgende Empfehlungen ausgesprochen:

Benutzerverwaltung, Zugriffskontrolle, Auswertungsmöglichkeiten

Grundsätzlich soll das Verfahren bei den jeweiligen personalverwaltenden Stellen der Polizei betrieben werden. Die bestehenden Zugriffs- und Auswertungsmöglichkeiten für Vorgesetzte und vorgesetzte Dienststellen, Geschäftszimmer sowie die einzelnen Polizeibediensteten waren nicht hinreichend deutlich unterschieden. Dies wurde zwischenzeitlich geändert. Hinsichtlich der Auswertungsfunktionen hat der LfD empfohlen, diese weitgehend in standardisierter Form (Regelauswertungen) zur Verfügung zu stellen und freie Auswertungsmöglichkeiten inhaltlich und vom Zugriff her zu beschränken.

Speicherungsfristen, Löschungen

Als Speicherungsfrist war im Fachkonzept lediglich die in § 105 a Abs. 1 LBG genannte Frist von fünf Jahren vorgesehen. Die Speicherung von Angaben, aus denen sich keine finanziellen Ansprüche ergeben, sollte aus Sicht des LfD jedoch lediglich für einen kürzeren Zeitraum erfolgen. Er hat in diesem Zusammenhang auf die Regelungen der Dienstvereinbarung des Ministeriums des Innern und für Sport verwiesen, die für Zeiterfassungsdaten die Löschung spätestens sechs Monate nach dem Ende des jeweiligen Abrechnungszeitraums vorsieht.

Protokollierung

§ 9 Abs. 2 Nr. 7 LDSG sieht vor, dass überprüft werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem eingegeben worden sind (Eingabekontrolle). Ähnliche Vorgaben bestehen mit § 9 Abs. 2 Nr. 6 LDSG für die Übermittlungskontrolle. Dementsprechend ist in der o. g. Dienstvereinbarung festgelegt, dass – für Eingaben und Auswertungen – in einer Protokolldatei Zeitpunkt, Veranlasser(in) sowie Art und Inhalt der Aktivität aufgezeichnet werden. Der LfD hat gebeten, dies auch für das Verfahren EVA sicherzustellen.

Die Empfehlungen des LfD wurden in der weiteren Verfahrensentwicklung angemessen berücksichtigt.

21.2.11 Überwachung der Telekommunikation mit dem System ATIS/MCMR

Über die Neukonzeption der im Bereich der Polizei eingesetzten Technik zur Überwachung des Fernmeldeverkehrs wurde bereits im 16. Tb. (Tz. 21.2.2.2) berichtet. Zwischenzeitlich wurde auf der Grundlage des dort genannten Anforderungskatalogs eine Ausschreibung durchgeführt und eine erste Ausbaustufe beim LKA Rheinland-Pfalz installiert. Die technische Funktionalität orientiert sich in weiten Bereichen an der im 16. Tb. dargestellten Lösung. Gegenwärtig besteht damit die Möglichkeit der Überwachung von Telekommunikationsdiensten – im Wesentlichen Telefonie und Telefax – in Mobilfunknetzen und im digitalen Festnetz der Telekom. Die in Rheinland-Pfalz eingesetzte Lösung ist in ähnlicher Weise auch in anderen Bundesländern vorgesehen. Parallel zur wachsenden Zahl von Providern und Telekommunikationsdiensten soll der technische Ausbau des Systems erfolgen.

Zum derzeitigen Sachstand wurden örtliche Feststellungen beim LKA getroffen. Dabei ergab sich, dass die im seinerzeitigen Anforderungskatalog enthaltenen Funktionen aufgrund ausstehender Entwicklungsarbeiten bislang erst zum Teil umgesetzt waren. Wegen der Digitalisierung der Vermittlungstechnik der Telekom sollte das System jedoch bereits zu Beginn des Jahres 1999 genutzt werden. Anhand eines Fragenkatalogs wurde daher die Umsetzung der technisch-organisatorischen Datenschutzanforderungen der Ausschreibungsunterlagen einschließlich der ergänzenden Empfehlungen des LfD mit dem Ministerium des Innern und für Sport abgestimmt. Unter technisch-organisatorischen Gesichtspunkten ergibt sich daraus folgende Bewertung des Telekommunikationsüberwachungssystems ATIS/MCMR:

21.2.11.1 Sicherung von Integrität durch kryptografische Maßnahmen

Das System stellt bislang keine Möglichkeiten der Sicherung der Integrität durch kryptografische Verfahren zur Verfügung. Einem Schutz vor unbefugten Veränderungen wird vor allem durch Maßnahmen der Zugriffs- und Speicherkontrolle Rechnung getragen. Die Sicherung der Integrität elektronisch gespeicherter Daten über Hash-Verfahren oder eine digitale Signatur bietet jedoch eine Ergänzung dieser Maßnahmen insoweit, als damit ein nachprüfbares Kriterium (Hashwert, Message Authentication Code)

für den Nachweis der Unverfälschtheit der Daten zur Verfügung steht. Vergleichbare Lösungen werden auf der Grundlage frei verfügbarer Algorithmen vielfach bereits als Bestandteil von PC-Sicherheitslösungen oder im Bereich elektronischer Zahlungsverfahren eingesetzt. Die Möglichkeit der technischen Umsetzung ist damit gegeben, der erforderliche Aufwand ist überschaubar. Angesichts der möglichen Bedeutung der Integrität der Beweisband-Daten im Gerichtsverfahren hat der LfD die Empfehlung des Einsatzes kryptografischer Verfahren zur Sicherung der Integrität der TÜ-Daten weiter aufrechterhalten. Die Frage, ob und an welcher Stelle z. B. Prüfsummenverfahren eingesetzt werden könnten, ist derzeit zwischen dem LKA und der Herstellerfirma in Abstimmung.

21.2.11.2 Aufzeichnung von Verteidigertelefonaten

Mehrfach wurde vom LfD die Aufzeichnung von Verteidigertelefonaten problematisiert. Aufgrund der technischen Gegebenheiten ist zum Zeitpunkt der Aufzeichnung ein Verteidigeranschluss nicht in jedem Fall erkennbar. Die für eine Unterdrückung der Aufzeichnung von Verteidigertelefonaten erforderlichen Verbindungsdaten liegen zum Zeitpunkt der Gesprächsaufzeichnung nur bei vom überwachten Anschluss abgehenden Gesprächen im digitalen Festnetz vor. In allen anderen Fällen werden die Verbindungsdaten zeitversetzt nachgeliefert, in der Regel ist eine Aufzeichnung dann bereits erfolgt. Neben verfahrensmäßigen Aspekten ist dies auch darauf zurückzuführen, dass in der Praxis nicht von allen Betreibern die in § 3 Abs. 2 FÜV geforderten Angaben zur Verfügung gestellt werden. Die Empfehlung des LfD lautete daher, angesichts des bestehenden Beweiserhebungsverbots das technisch Machbare umzusetzen. Aus Sicht des LfD bedeutet dies im digitalen Festnetz den Abgleich der Zielnummern der vom überwachten Anschluss abgehenden Gespräche mit einer „Verteidigerdatenbank“ und gegebenenfalls die Unterdrückung der Aufzeichnung sowie die automationsunterstützte Prüfung der Verbindungsdaten bereits aufgezeichneter Verteidigergespräche und nachfolgend die Löschung der Gespräche.

Die Empfehlungen wurden vom Ministerium des Innern und für Sport insoweit aufgegriffen, als mit dem Hersteller die technische Umsetzbarkeit geklärt werden soll.

21.2.11.3 Verschlüsselung bei der Bereitstellung über öffentliche Übertragungswege

Da der Zugriff auf die TÜ-Daten häufig über externe Arbeitsstationen der ermittlungsführenden Dienststellen erfolgen soll, hatte der LfD zur Sicherung der Vertraulichkeit der TÜ-Daten sowie der für die Anmeldung am System ATIS/MCMR erforderlichen Angaben bei der Übertragung auf öffentlichen Kommunikationswegen – z. B. einer ISDN-Verbindung zwischen LKA und externer Dienststelle – den Einsatz kryptografischer Verfahren empfohlen. Das Ministerium des Innern und für Sport hat in diesem Zusammenhang die Absicht bekundet, im Rahmen der finanziellen Möglichkeiten Verschlüsselungsgeräte sukzessive beschaffen zu lassen.

Vom LfD wurde seinerzeit auf die aus seiner Sicht bestehende Notwendigkeit hingewiesen, Informationen zu Überwachungsmaßnahmen auch gegenüber den Providern so weit wie möglich geheim zu halten. Die hierzu angeregte Verschlüsselung bei der Übertragung vom Network Service Centrum (NSC) des Providers zum Bedarfsträger ist gegenwärtig in der Fernmeldeüberwachungsverordnung bzw. den technischen Richtlinien für die Überwachungsschnittstelle nicht vorgesehen und wird vom System ATIS/MCMR nicht unterstützt. Der notwendigen Absicherung wird durch eine geschlossenen Benutzergruppe (ISDN-Leistungsmerkmal CUG) Rechnung getragen. Nach Auffassung des LfD ist die Tatsache, dass für bestimmte Anschlüsse Überwachungsmaßnahmen durchgeführt werden, auch gegenüber dem Personal des Netzbetreibers geheimhaltungsbedürftig.

21.2.11.4 Protokollierung der Erstellung von Ausdrucken

Entgegen der entsprechenden Forderung in den Ausschreibungsunterlagen wird die Erstellung von Ausdrucken der TÜ-Daten nicht protokolliert. Gegenwärtig ist damit nicht zu unterscheiden, ob für TÜ-Daten lediglich die Bildschirmdarstellung (d. h. lesender Zugriff) oder auch eine weitergabefähige Form (Ausdruck) gewählt wurde. Die Frage des Verbleibs etwaiger Ausdrucke kann daher nur bedingt beantwortet werden. Um den Bedenken des LfD Rechnung zu tragen, werden jedoch künftig der zugrunde liegende Zugriff auf die Datenbank protokolliert und auf Ausdrucken die Angaben Datum, Uhrzeit, Benutzerkennung und Auswertestation ausgegeben.

Die Empfehlungen des LfD wurden damit weitgehend berücksichtigt. Die noch offenen Punkte bedürfen zwar der abschließenden Klärung, sie begründen jedoch keine grundsätzlichen Bedenken gegen den Einsatz der vorgesehenen technischen Lösung.

21.2.12 Einbindung der Gesundheitsämter in die IT-Struktur der Kreisverwaltungen

Im Zusammenhang mit der Übertragung der Aufgaben der unteren Gesundheitsbehörden auf die Kreisverwaltungen haben sich im Berichtszeitraum mehrfach Fragen ergeben, ob und in welchem Umfang eine Eingliederung der eingesetzten Datenverarbeitungssysteme in die IT-Struktur der Kreisverwaltungen möglich sei.

Die datenschutzgerechte Gestaltung von Verfahren der Gesundheitsämter war hinsichtlich der technisch-organisatorischen Maßnahmen in den letzten Jahren mehrfach Gegenstand von Erörterungen zwischen dem Ministerim für Arbeit, Soziales und Gesundheit und dem LfD. Sowohl für die Absicherung der eingesetzten Mobilcomputer als auch der stationären Rechner des Gesundheitsamtes wurde letztlich ein Sicherheitskonzept realisiert, welches die besondere Sensibilität der Daten berücksichtigt. Kernpunkte des Sicherheitskonzepts sind u. a.

– die Speicherung der Schulgesundheitsdaten auf gesonderten Systemen im Gesundheitsamt,

– der Einsatz einer Sicherheitssoftware für die Zugriffs-, Eingabe- und Speicherkontrolle und

– die kryptografische Online-Verschlüsselung der gespeicherten Daten.

Bei Weiterentwicklungen muss sichergestellt sein, dass das erreichte Sicherheitsniveau nicht unterschritten wird. Auch nach der organisatorischen Eingliederung der Gesundheitsämter in die Kreisverwaltungen ist der besonderen Sensibilität der dem Arztgeheimnis unterliegenden Daten Rechnung zu tragen. Mit den bisherigen Sicherungsmaßnahmen ist dies in der Regel gewährleistet; diese sollten daher beibehalten werden. Da die gegenwärtig getroffenen Maßnahmen u. a. aus der für das Verfahren genutzten Informationstechnik resultieren, kommen bei Änderungen der Hard- oder Software grundsätzlich auch alternative Maßnahmen in Betracht. Dabei muss jedoch hinsichtlich der in § 9 Abs. 2 LDSG angesprochenen Bereiche eine gleichwertige Sicherheit gewährleistet sein. Die bisherige Verschlüsselung sensibler Daten ist in jedem Fall beizubehalten.

Aus Sicht des LfD bestehen keine Bedenken gegenüber einer Unterstützung der Anwender und der technischen Betreuung der eingesetzten Geräte durch Bedienstete der Kreisverwaltung, soweit dies unter Kontrolle des Gesundheitsamtes erfolgt. Auch eine Eingliederung der Rechner des Gesundheitsamtes in ein internes Netzwerk zum Zweck der Teilnahme an der behördeninternen elektronischen Kommunikation (z. B. E-Mail) oder für die gemeinsame Nutzung von Terminkalendern, Telefon- und Adressverzeichnissen o. Ä. ist grundsätzlich unproblematisch, wenn auf den beteiligten Systemen keine dem Arztgeheimnis unterfallenden Daten gespeichert sind (vgl. § 11 Abs. 1 Satz 2 2. Halbsatz ÖGdG). Soweit allerdings derartige Daten betroffen sind, müssen geeignete Sicherungsmaßnahmen ergriffen werden. Dies betrifft sowohl in Datenbanken gespeicherte Daten als auch solche in Textverarbeitungsdokumenten, z. B. ärztliche Gutachten.

Aus datenschutzrechtlicher Sicht ist weiterhin die Übernahme von Datenbeständen auf einen zentralen Server der Kreisverwaltung problematisch. Hintergrund entsprechender Anfragen war meist der Wunsch, die Bestände bei der routinemäßigen Sicherung der Serverdaten zu berücksichtigen und den Aufwand einer separaten Sicherung zu vermeiden. Eine Änderung kann nur in Betracht kommen, wenn die Aufwandsreduzierung in einer Abwägung mit dem durch eine räumlich getrennte Speicherung erzielten zusätzlichen Zugriffsschutz überwiegt. Neben einer effektiven Zugriffskontrolle ist bei der Speicherung auf einem zentralen Server durch kryptografische Verschlüsselung sicherzustellen, dass auf die zentral vorgehaltenen Gesundheitsdaten im Klartext ausschließlich von den hierzu befugten Beschäftigten des Gesundheitsamtes zugegriffen werden kann.

Zusammenfassend kommt die Einbindung der Systeme eines Gesundheitsamtes in das Netzwerk einer Kreisverwaltung oder eine Speicherung auf einem zentralen Server nicht in Betracht, wenn damit unbefugt Zugriffe auf dem Arztgeheimnis unterliegende Daten im Klartext möglich werden (§ 11 Abs. 6 ÖGdG). Dies gilt auch für Zugriffe der Systembetreuung. Der LfD hat das Ministerium für Arbeit, Soziales und Gesundheit gebeten, bei entsprechenden Anfragen auf die vorstehenden Überlegungen hinzuweisen. Angesichts der Sensibilität der Daten sollte Änderungen, die lediglich durch eine Vereinheitlichung der Informationstechnik im Bereich der Kreisverwaltung intendiert sind, mit Zurückhaltung begegnet werden.

21.2.13 Zugriffsberechtigung im Vertretungsfall im Verfahren Finanzamt 2000

Die Möglichkeit, bei der Verarbeitung von Steuerdaten im Verfahren Finanzamt 2000 auf Programmfunktionen und Daten zuzugreifen, wird über die für die Beschäftigten der Finanzämter im Einzelnen festgelegten Zugriffsberechtigungen gesteuert. Die in Vertretungsfällen notwendigen Änderungen führten nach Darstellung des Ministeriums der Finanzen zu einem erheblichen Aufwand und zeitlichen Verzögerungen bei der Bearbeitung. Das Ministerium beabsichtigte daher, auf der Grundlage der Geschäftsverteilungspläne dauerhafte Zugriffsberechtigungen für die Arbeitsgebiete der jeweils Vertretenen einzurichten.

Aus Sicht des LfD ist grundsätzlich anzustreben, vorübergehend benötigte Zugriffsberechtigungen nur für den erforderlichen Zeitraum zu erteilen. Jeder „unnötige“ Zugriff erhöht das Missbrauchsrisiko. Er empfiehlt eine Verfahrensweise, wie sie in anderen Bereichen bereits praktiziert wird. Danach werden bei Eingabe eines Abwesenheitszeitraums durch die Systembetreuung oder den zu Vertretenden dem Vertreter für seine Benutzerkennung automatisch und zeitlich begrenzt die Rechte des Vertretenen eingeräumt. Bei Inanspruchnahme der Vertretungsberechtigung muss im Rahmen der Eingabekontrolle erkennbar sein, dass nicht der eigentlich zuständige Bearbeiter, sondern die Vertretung zugegriffen hat. Unter diesen Voraussetzungen bestehen keine Bedenken, eine zeitlich begrenzte Vergabe von Zugriffsrechten für den Vertretungsfall einzurichten. Insbesondere bei absehbaren Vertretungsfällen wie Urlaub, Weiterbildung usw. können damit vorübergehend erforderliche Berechtigungen selbständig und in eigener Verantwortung erteilt und zurückgenommen werden.

Das Finanzministerium hat die Anregungen des LfD aufgegriffen und zwischenzeitlich eine entsprechende Anpassung des Verfahrens vorgenommen. Mit der gefundenen Lösung ergeben sich zudem Vorteile bei der Pflege der Zugriffsberechtigungen von in der Ausbildung stehenden Personen und Bediensteten mit Mischbezirken.

21.2.14 Sicherstellung der Zweckbindung bei der Verarbeitung personenbezogener Daten durch Krankenkassen

Die für den Umgang mit personenbezogenen Daten geltenden Rechtsgrundlagen sind weitgehend in §§ 284 bis 305 SGB V geregelt. Die Verarbeitung der von den Krankenkassen nach § 284 SGB V erhobenen bzw. von den Leistungserbringern nach

§ 294 ff. SGB V übermittelten Daten unterliegt dabei besonderen Zweckbindungen. Der Einsatz der Informationstechnik im Bereich der Krankenkassen sowie der Aufbau und die Organisation der Kassen sind gegenwärtig erheblichen Veränderungen unterworfen, von Bedeutung sind dabei insbesondere folgende Entwicklungen:

- Im Krankenkassenbereich eingesetzte Verfahren der Informationsverarbeitung werden durch den Einsatz relationaler Datenbanksysteme mit erweiterten Auswertungsmöglichkeiten („freie Abfragesprachen“) ergänzt bzw. abgelöst. Durch grundsätzlich frei wähl- und kombinierbare Suchkriterien können Zweckbindungsregelungen umgangen werden.
- Der elektronische Datenaustausch zwischen Leistungserbringern und Krankenversicherungen führt zu wesentlichen Änderungen bei Art und Umfang der automatisierten Verarbeitung von Versichertendaten. Krankenversicherungsdaten stehen in weit größerem Umfang als bisher in elektronischer Form und damit automatisiert auswertbar zur Verfügung.
- Spezialisierte Aufgabenbereiche werden durch übergreifende Funktionsbereiche abgelöst. Dies führt i. d. R. zu umfangreichen Zugriffsrechten der Mitarbeiter.
- Bislang selbständige Kassen schließen sich zu überregional oder landesweit tätigen Organisationen zusammen. Damit einhergeht die Zusammenführung bislang getrennter Versichertendatenbestände.
- Wesentliche DV-Produktionsarbeiten werden kassenübergreifend auf zentrale Stellen konzentriert, welche im Wege der Auftragsverarbeitung nach § 80 SGB X die automatisierte Verarbeitung übernehmen (z. B. Rechenzentrumsgemeinschaft „AOK ARGE Mitte“ für die AOKen Hessen, Saarland, Rheinland-Pfalz und Thüringen).
- Nach den Reformen im Gesundheitsbereich und der Einführung wettbewerbsähnlicher Strukturen kommen Mitgliederwerbung und -pflege, Marketing und Kostenmanagement steigende Bedeutung zu. Dies birgt die Gefahr, dass Sozialdaten für Zwecke genutzt werden, die durch bestehende Verarbeitungsbefugnisse nicht gedeckt sind.
- Die Einrichtung von Pflegekassen bei den Krankenkassen ermöglicht die gemeinsame Nutzung eines Teils der gespeicherten Krankenversicherungsdaten. Da die für die Durchführung der Pflegeversicherung erforderlichen IT-Anwendungen häufig in die bestehenden Verfahren der Krankenkassen integriert wurden, sind über die Zweckbindungsvorschriften hinausgehende Verarbeitungsmöglichkeiten nicht auszuschließen.
- Entwicklung und Pflege der zentralen im Krankenkassenbereich eingesetzten IT-Verfahren liegen weitgehend in der Hand der jeweiligen Bundesverbände. Auch wenn die einzelnen Kassen für die Umsetzung der Maßnahmen nach § 78 SGB X verantwortlich sind, werden in der Praxis Programmergänzungen regelmäßig nur über Entwicklungen des jeweiligen Bundesverbandes vorgenommen. In Einzelfällen hat dies dazu geführt, dass Realisierungen unterblieben oder nur mit Verzögerung erfolgt sind.

Aus datenschutzrechtlicher Sicht ergibt sich angesichts dieser Veränderungen die Gefahr, dass bei der Verarbeitung von Sozialdaten durch die Krankenversicherungen die Zweckbindungsvorschriften des Sozialgesetzbuchs nicht im gebotenen Umfang berücksichtigt werden. Eine Lösung könnte darin liegen, der Zweckbindung zuwiderlaufende Datennutzungen durch das Zusammenwirken technischer Maßnahmen und organisatorischer Verfahrensregelungen zu erschweren bzw. durch eine transparente Gestaltung der Verfahren erkennbar zu machen. Für die einzelnen Bereiche sind dabei folgende Gesichtspunkte von Bedeutung:

21.2.14.1 Einsatz freier Abfragesprachen

Für den Einsatz freier Abfragesprachen liegen bereits Empfehlungen der Datenschutzbeauftragten vor (vgl. BfD 15.Tb., Anlage 19). Soweit nicht lediglich anonymisierte Auswertungen vorgesehen sind, sollten bei der Anwendung freier Abfragesprachen folgende Punkte berücksichtigt werden:

- Auch bei relationalen Datenbanken besteht in der Regel die Möglichkeit, den Zugriffsumfang zu beschränken. Die Freiheit der Abfrage erstreckt sich damit lediglich auf den bereitgestellten Datenbestand. Es sind daher Festlegungen erforderlich, welchen Stellen, in welchem Umfang und für welche Zwecke freie Abfragemöglichkeiten zur Verfügung stehen. Die Festlegungen sind mit den Zugriffskontrollmechanismen des jeweiligen Datenbanksystems programmtechnisch abzubilden. Die Zugriffsstruktur und Änderungen daran sind zu dokumentieren. Für Auswertungen und Zusammenführungen außerhalb der Festlegungen ist ein besonderes Verfahren vorzusehen. Dieses muss die datenschutzrechtliche Prüfung der Zulässigkeit der vorgesehenen Auswertung sicherstellen.
- Bei regelmäßig wiederkehrenden Auswertungen sollte nur auf vorgegebene Auswertungsfunktionen zurückgegriffen werden können und auf freie Abfragemöglichkeiten verzichtet werden.

21.2.14.2 Kassenübergreifende Konzentration der DV-Produktion

In mehreren Fällen wurde die DV-Produktion der Allgemeinen Ortskrankenkassen verschiedener Länder im Wege der Auftragsdatenverarbeitung nach § 80 SGB X auf eine Stelle konzentriert (ARGE Nord, ARGE Mitte). Vergleichbare Entwicklungen vollziehen sich auch im Bereich anderer Kassen. Neben der konkreten Festlegung der übertragenen Aufgaben und einer datenschutzgerechten Gestaltung der zugrunde liegenden Verträge ist dabei die interne Abschottung der Datenbestände von zentraler

Bedeutung. Bestandsübergreifende Auswertungen müssen wirksam ausgeschlossen werden. Die im Zusammenhang mit der Bildung der Arbeitsgemeinschaft AOK Rechenzentrum Mitte vorgelegten Konzepte zeigen, dass hier in der Praxis tragfähige Lösungen möglich sind. Kernpunkte sind

- die vertragliche Regelung nach § 80 SGB X, einschließlich einer Datenschutzvereinbarung,
- die Trennung der Datenbestände der einzelnen Krankenkassen,
- getrennte System- und Programmumgebungen (virtuelle Systeme) für die Anwendungen der jeweiligen Kasse,
- ein Zugriffskonzept für landesspezifische und zentrale Funktionen,
- ein Test- und Freigabeverfahren für Programme,
- ein Revisionskonzept,
- ein Datensicherungs- sowie
- ein Archivierungs- und Löschkonzept.

21.2.14.3 Zugriffsbefugnisse auf Versichertendaten

In der Regel orientieren sich Zugriffsbefugnisse an den Aufgabenbereichen der Krankenkassen. Tendenziell ist hier eine Zusammenfassung einzelner Aufgabenbereiche zu größeren Funktionsgruppen festzustellen, innerhalb derer im Wesentlichen keine weitere Differenzierung von Zugriffsrechten erfolgt. Ein Problem stellen dabei allgemeine Auskunftsmasken dar, die undifferenziert den Zugriff auf alle oder einen Großteil der Versichertendaten erlauben. Soweit diese über die Abfrage von Versichertenstammdaten (z. B. Name, Anschrift, Vers.-Nr.) hinausgehen, muss eine besondere Prüfung der Erforderlichkeit erfolgen. Insbesondere bei Diagnose- und Leistungsdaten ist auf diese Form der Bereitstellung zu verzichten.

Programmfunktionen, die lesend auf die Versichertendaten zugreifen, werden oft einheitlich allen Benutzern zur Verfügung gestellt. Lediglich bei schreibenden oder ändernden Zugriffsmöglichkeiten erfolgt meist aufgrund finanzieller Auswirkungen eine Differenzierung. Mehr als bisher müssen datenschutzrechtliche Zweckbindungsregelungen in die Vergabe von Zugriffsrechten einfließen. Dies sollte regelmäßig auf der Grundlage eines Zugriffskonzeptes erfolgen, das die Funktionsbereiche der jeweiligen Kasse, die Art der betroffenen Daten und den zulässigen Verarbeitungszweck nach § 284 ff. SGB V berücksichtigt. Soweit, wie in den meisten Fällen, die Verfahrensentwicklung nicht durch die Kassen selbst, sondern durch Bundes- oder Landesverbände erfolgt, muss die Verwaltung der Zugriffsrechte ausreichend flexibel gestaltet sein, um eine Anpassung an unterschiedliche Anforderungen der einzelnen Kassen zu ermöglichen.

Im Bereich landesweit oder überregional tätiger Kassen wird beim Zugriff in aller Regel nicht nach regionalen Gesichtspunkten differenziert. Versichertendaten einschließlich der Angaben zu Diagnosen und Leistungen stehen zum Teil landesweit allen, damit auch unzuständigen, Mitarbeitern einer Krankenkasse zur Verfügung.

21.2.14.4 Archivierung und Löschung von Versichertendaten

Die Löschung der Daten der Krankenversicherung ist in § 304 SGB V i. V. m. § 84 Abs. 2 SGB X geregelt. Danach sind Sozialdaten zu löschen, wenn ihre Kenntnis für die speichernde Stelle zur rechtmäßigen Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben nicht mehr erforderlich ist. In einzelnen Regelungen sind konkrete Vorgaben vorgesehen, wonach

- Angaben über Leistungsvoraussetzungen (§ 292 Abs. 1 SGB V) bis zu zehn Jahren,
- Diagnosen in Fällen von Arbeitsunfähigkeit (§ 292 Abs. 1 SGB V) bis zu zehn Jahren,
- Leistungsdaten im Rahmen der Beitragsrückzahlung (§ 292 Abs. 2 SGB V) bis zu zwei Jahren,
- fallbezogene Daten der Kassenärztlichen Vereinigungen über abgerechnete Leistungen (§ 295 Abs. 2 SGB V) bis zu zwei Jahren,
- im Rahmen der Auffälligkeitsprüfungen übermittelte Daten (§ 296 Abs. 1 und 3 SGB V) bis zu zwei Jahren,
- im Rahmen der Zufälligkeitsprüfungen übermittelte Daten (§ 297 SGB V) bis zu zwei Jahren,
- im Rahmen der Prüfung der Wirtschaftlichkeit und Qualität der Behandlung im Einzelfall übermittelte Daten (§ 298 SGB V) bis zu zwei Jahren

gespeichert werden dürfen.

Die Krankenkassen können für Zwecke der Krankenversicherung Leistungsdaten länger aufbewahren, wenn sichergestellt ist, dass ein Bezug zum Arzt oder Versicherten nicht mehr herstellbar ist (§ 304 Abs. 1 Satz 2 SGB V).

Konkrete Löschfristen sind im Rahmen der automatisierten Verarbeitung der Kassen jedoch, anders als für die Aufbewahrung von Belegen, nur zum Teil festgelegt. Betroffen sind u. a. die Daten ausgeschiedener Versicherter und Diagnoseangaben als Bestandteil der Leistungsdaten. Für letztere wurden vorgesehene Löschungsfristen wegen des sog. Blockfristverfahrens (§ 48 SGB V) ausgesetzt, in dessen Rahmen bei der Suche nach relevanten Vorerkrankungen in Einzelfällen auf Daten bis 1958 zurückgegriffen werden kann. Seitens der Krankenkassen wird auf mögliche Konflikte zwischen der Blockfristenregelung und § 304 Abs. 1 Nr. 1 SGB V hingewiesen.

Für die Umsetzung der Löschungsvorgaben ist, auch soweit sie nicht konkret bestimmt sind (vgl. § 84 SGB X), die Festlegung von Speicherungsfristen erforderlich. Anzustreben ist eine möglichst automationsunterstützte, dokumentierte Löschung bzw. Sperrung. Die Speicherungsfristen von Diagnose- und Leistungsdaten bedürfen dabei einer differenzierten Betrachtung, um auch dem gegebenenfalls erforderlichen Zugriff auf weit zurückliegende Daten Rechnung zu tragen. Die Notwendigkeit, einzelne Angaben für längere Zeit vorzuhalten, kann jedoch keine Rechtfertigung für eine dauerhafte automatisierte Speicherung aller personenbezogenen Gesundheitsdaten im aktuellen Bestand darstellen. Lösungsansätze sind zumindest für den AOK-Bereich bekannt. Hier wurde, weniger wegen einer datenschutzgerechten Verfahrensgestaltung als aus Performancegründen, ein Konzept zur Auslagerung aktuell nicht benötigter Versichertendaten entwickelt. Diese können besonderen Zugriffsberechtigungen unterworfen werden.

21.2.14.5 Protokollierung von Abfragen und Auswertungen

Ähnlich wie bei der Vergabe von Zugriffsrechten ist auch die Protokollierung überwiegend an der Möglichkeit eines ändernden Zugriffs orientiert. Lesende Zugriffe und Auswertungen sind nach den vorliegenden Erkenntnissen hingegen oftmals nur ansatzweise nachvollziehbar. Insgesamt ist die Protokollierung von Abfragen und Auswertungen häufig als unzureichend einzustufen. Abfragen und Auswertungen sind zumindest stichprobenweise revisionssicher zu protokollieren. Für die Festlegung des Umfangs einer Protokollierung könnten analog die Regelungen für die Einrichtung automatisierter Abrufverfahren in § 79 Abs. 4 SGB X herangezogen werden.

Für die Praxis bedürfen die genannten Lösungsansätze der weiteren Konkretisierung. Dies könnte z. B. in Form eines Orientierungsrahmens mit Kriterien erfolgen, anhand derer eine Beurteilung der für die Sicherstellung der Zweckbindung getroffenen bzw. erforderlichen Maßnahmen möglich ist. Dies böte auch die Möglichkeit, den bestehenden Unterschieden der einzelnen Kassen bei Organisation, IT-Struktur, Mitglieder-/Versichertenzahl usw. Rechnung zu tragen.

Die angesprochenen Punkte wurden gegenüber den Spitzenverbänden der gesetzlichen Krankenversicherung thematisiert. Ein zufrieden stellendes Ergebnis konnte dabei jedoch nicht erzielt werden. Auch das in diesem Zusammenhang als notwendig erachtete Datenschutz-Gesamtkonzept liegt bislang nicht vor.

21.2.15 Verteilung personenbezogener Budgetierungsdaten in den Geschäftsbereichen der Ressorts

Für Planungszwecke im Zusammenhang mit der Budgetierung im Personalbereich wurde bei der ZBV der OFD Koblenz eine Datenbank mit personenbezogenen Budgetierungsdaten aufgebaut. Diese steht den jeweiligen Ressorts zur Verfügung, die ihrerseits die Weiterverteilung auf die einzelnen personalbewirtschaftenden Dienststellen vornehmen.

Die Verteilung der Budgetierungsdaten soll nach den Vorstellungen der Ressorts im Wege des Datenträgerversands oder auf elektronischem Weg erfolgen. Angesichts der Sensibilität der Daten hält es der LfD in diesem Zusammenhang für erforderlich, dass geeignete Maßnahmen zum Schutz der Daten vor unbefugter Kenntnisnahme, Kopie oder Veränderung getroffen werden (vgl. § 9 Abs. 2 Nr. 9 LDSG).

Nach einer Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 9. Mai 1996 sind insbesondere kryptografische Verfahren geeignet, Verletzungen des Datenschutzes beim Transport schutzwürdiger elektronisch gespeicherter Daten zu verhindern. Mit ihrer Hilfe lassen sich Manipulationen und Übertragungsfehler nachweisen und eine unberechtigte Kenntnisnahme verhindern. Derartige Verfahren sind heute Stand der Technik und können in vielen Anwendungsfällen mit vertretbarem Aufwand eingesetzt werden. Geeignete Lösungen sind beispielsweise in Form des vom BSI für den behördlichen Bereich kostenfrei abgegebenen Dateiverschlüsselungsprogramms MIC oder vergleichbarer, verbreitet eingesetzter und zu geringen Kosten verfügbarer Programme (z. B. PGP Pretty Good Privacy) vorhanden (vgl. auch Tz. 21.3.10).

Der Einsatz derartiger Lösungen ist vor allem in den Fällen geboten, in welchen beim elektronischen Transport ganz oder teilweise öffentliche Übertragungswege genutzt werden. Dies ist z. B. auch bei der Kommunikation über das LDKN der Fall, wenn z. B. über ein Mail-Gateway die Weiterleitung an nicht über das LDKN erreichbare Empfänger erfolgt. Die genannten Lösungen können weiterhin bei der Weiterleitung der Daten im Wege des Datenträgerversands genutzt werden. Der LfD hat daher für die Verteilung der Budgetierungsdaten im nachgeordneten Bereich den Einsatz derartiger Programme empfohlen.

21.2.16 Dezentrale Datenerfassung bei den Ämtern für Ausbildungsförderung

Für die Bearbeitung von Anträgen auf Ausbildungsförderung sind vom Ministerium für Bildung, Wissenschaft und Weiterbildung organisatorische und technische Änderungen vorgesehen. Anstelle der bisherigen zentralen Datenerfassung bei der OFD Koblenz sollen die Antragsdaten künftig dezentral bei den Ausbildungsförderungsämtern der Landkreise und kreisfreien Städte sowie den Hochschulen erfasst und in elektronischer Form an das Rechenzentrum der Finanzverwaltung übermittelt werden. Die Übermittlung durch die Landkreise soll über das Verwaltungsnetz des Landes im LDKN, die Übermittlung durch die Hochschulen via E-Mail über das offene Bildungsnetz erfolgen. Der LfD hat zu den vorgesehenen Verfahren in technischer Hinsicht Stellung genommen.

21.2.16.1 Datenerfassung und Übermittlung durch die Ausbildungsförderungsämter auf Kreisebene (Verfahren BAFER)

Das Verfahren dient allein der Datenerfassung und -übermittlung. Nach der Programmdokumentation wird für den jeweils relevanten Erfassungszeitraum eine Datei mit Ausbildungsförderungsdaten gebildet. Deren weitere Verarbeitung nach Übermittlung zum Rechenzentrum der Finanzverwaltung entspricht dem bisherigen Verfahren. Da eigene Datenbanken bei den Ämtern für Ausbildungsförderung nicht gebildet werden, beschränken sich die nach § 9 Abs. 2 LDSG erforderlichen Maßnahmen auf die Absicherung der Arbeitsplatzrechner und den Datentransport zur OFD Koblenz. Dies entspricht den allgemein geltenden Anforderungen beim PC-Einsatz und liegt jeweils in der Verantwortung der Ausbildungsförderungsämter.

Für die Erfassungsdateien ergibt sich nach § 19 Abs. 2 Nr. 2 LDSG die Notwendigkeit der Löschung, wenn diese für die Aufgabenerfüllung nicht mehr benötigt werden. Da die Dateien nach Zeiträumen monats- bzw. tageweise gestaffelt sind, sollte daran orientiert eine Löschung vorgenommen werden. Soweit dies nicht programmseitig erfolgt, ist durch organisatorische Regelungen sicherzustellen, dass zeitnah die Löschung der Erfassungsdateien erfolgt. Ähnliches gilt für die Löschung der Protokolldatei mit Angaben über die Aktionen der Benutzer. Nach den Empfehlungen des LfD soll für Protokolldaten ein Aufbewahrungszeitraum von einem Jahr nicht überschritten werden. Die Vorgabe der Speicherungsfristen sollte einheitlich für die Ausbildungsförderungsämter festgelegt werden.

Da die Übermittlung der Erfassungsdaten über das LDKN innerhalb des geschlossenen Netzwerks „VPN Verwaltung“ erfolgen soll, sind besondere Maßnahmen zur Gewährleistung der Vertraulichkeit gegenwärtig nicht erforderlich.

21.2.16.2 Datenerfassung und Übermittlung durch die Ausbildungsförderungsämter der Hochschulen

Die o. g. Gesichtspunkte gelten in gleicher Weise für die Verarbeitung bei den Ausbildungsförderungsämtern der Hochschulen. Im Unterschied zum BAFER-Verfahren steht diesen eine Datenbank mit Angaben zu den laufenden Förderungsfällen zur Verfügung. Soweit beim Datentransfer zwischen Schwerpunktamt und Rechenzentrum bzw. zwischen Außenstellen und Schwerpunktamt im offenen Bildungsnetz eine kryptografische Verschlüsselung über als sicher anerkannte Verfahren (z. B. Triple DES, RSA, IDEA) mit ausreichender Schlüssellänge erfolgt, bestehen gegen die Übermittlung via E-Mail keine Bedenken. Proprietäre Lösungen kommen alternativ in Betracht, wenn diese nachgewiesenermaßen eine vergleichbare Sicherheit bieten. Neben der Auswahl geeigneter Algorithmen ist auf eine ordnungsgemäße Schlüsselerzeugung, -verwaltung und -verteilung zu achten.

Die Sicherung der Vertraulichkeit durch Verschlüsselung sollte dabei losgelöst von der durch die digitale Signatur gewährleisteten Integrität und Zurechenbarkeit behandelt werden. Das in dieser Hinsicht mit einer signaturgesetzkonformen Lösung verbundene Sicherheitsniveau kommt aus Sicht des LfD lediglich dort in Betracht, wo besondere Anforderungen an die Authentizität elektronisch gespeicherter Daten und ein grundsätzlich offener Teilnehmerkreis vorliegen. In den Fällen, bei welchen ausschließlich festgelegte Stellen miteinander kommunizieren, sind aus Sicht des Datenschutzes auch andere Verfahren im Sinne des § 1 Abs. 2 SigG ausreichend.

Soweit Datentransfers zwischen Schwerpunktamt und Außenstellen nicht dateibezogen erfolgen, z. B. via E-Mail, sondern im Wege des direkten Zugriffs auf die Datenbestände der Außenstellen, hat der LfD die Sicherung der Kommunikation auf Protokollebene empfohlen. Die ins Auge gefassten Lösungen auf Basis des SSL-Protokolls mit Schlüssellängen > 40 Bit bzw. der Aufbau eines virtuellen privaten Netzes (VPN) sind hierzu grundsätzlich geeignet.

21.2.17 Behandlung defekter Festplatten im Bereich der Polizei

Aufgrund eines physikalischen Defekts wurde im Bereich der Polizei die Festplatte eines PC mit Daten aus polizeilichen Ermittlungsverfahren ausgesondert und als Anschauungsobjekt weiter verwendet. Obwohl der Zugriff auf die auf der Festplatte weiterhin gespeicherten Daten wegen des Defekts mit regulären Mitteln nicht möglich war, hat der LfD empfohlen, die Festplatte ordnungsgemäß zu vernichten.

Hintergrund hierfür sind die vorhandenen technischen Möglichkeiten, die es in vielen Fällen erlauben, unzureichend gelöschte oder auf defekten Datenträgern gespeicherte Daten wiederherzustellen. Von einschlägigen Firmen wird dies als normale Dienstleistung angeboten. Das Ministerium des Innern und für Sport hat sich nach Prüfung der Auffassung des LfD angeschlossen und die Polizeibehörden und -einrichtungen angewiesen, künftige Löschungen durch mehrfaches Überschreiben mit einem vom BSI empfohlenen Programm vorzunehmen und defekte Festplatten mechanisch zu zerstören.

Gegen diese Vorgehensweise bestehen aus datenschutzrechtlicher Sicht keine Bedenken. Wegen der angesichts der geänderten IT-Ausstattung der Polizei absehbaren Bedeutung der Entsorgung von Datenträgern hat der LfD gebeten, entsprechende Regelungen in die Dienstanweisung für den Bereich der Polizei aufzunehmen.

21.3 Allgemeine technisch-organisatorische Aspekte

Im Zusammenhang mit dem Einsatz der Informationstechnik in den Verwaltungen wurde der LfD vielfach zu technischen Einzelfragen um Stellungnahme gebeten. Einige Punkte mit über den Einzelfall hinausgehender Bedeutung sind nachfolgend dargestellt:

21.3.1 Wählleitungsverbindungen bei an das LDKN angeschlossenen Verwaltungen

Bei den Verwaltungen ist festzustellen, dass vor allem in Fällen, in denen nur ein gelegentlicher Kommunikationsbedarf besteht, in steigendem Umfang Wahlleitungsverbindungen zu entfernten Stellen eingerichtet werden. Im Hinblick auf den zumeist ebenfalls bestehenden Anschluss an das LDKN hat das DIZ den LfD um eine Bewertung der Einrichtung von Wählleitungsverbindungen bei an das LDKN angeschlossenen Verwaltungen gebeten. Im Vordergrund stehen dabei nach Darstellung des DIZ insbesondere die

- Anbindung externer Stellen im Rahmen der Systembetreuung (z. B. Fernwartung),
- Anbindung ausgelagerter einzelner Arbeitsplätze,
- Anbindung von Außenstellen,
- Koppelung lokaler Netze,
- Anbindung von Verwaltungskassen an die jeweilige Hausbank.

Entsprechend den „Benutzungsbedingungen im landesweiten Datenübertragungsnetz“ (MinBl. 1994 S. 131) erstreckt sich die Verantwortlichkeit des DIZ auf alle Netzkomponenten einschließlich der bei den Verwaltungen installierten LDKN-Router. Die Konfiguration und der Betrieb der einzelnen IT-Lösungen der Verwaltungen liegt hingegen in der Verantwortung der jeweiligen Stellen. Dies umfasst auch die Einrichtung grundsätzlich zulässiger Wählverbindungen zu den o. g. Zwecken. Die datenschutzrechtliche Verpflichtung, dabei die erforderlichen technisch-organisatorischen Maßnahmen zu treffen, obliegt ebenfalls den einzelnen Verwaltungen (§ 9 Abs. 1 LDSG). Neben den unter Tz. 21.3.3 genannten Aspekten ist dabei insbesondere die Konfiguration der betroffenen IT-Systeme, hier vor allem die ordnungsgemäße Verwaltung der über die Wählverbindung zugelassenen Benutzer und die Vergabe von Zugriffsrechten von Bedeutung. Da diese Verbindungen u. U. Auswirkungen auf das Sicherheitsniveau des LDKN haben, sehen die o. g. Benutzungsbedingungen daher vor der Einrichtung von Wählleitungsanschlüssen eine Abstimmung mit dem DIZ vor (Abschnitt III, Nr. 3.2). Nach den Erkenntnissen des LfD erfolgt diese Abstimmung gegenwärtig nicht in allen Fällen. Er hat daher das DIZ gebeten, die Netzkunden des LDKN in geeigneter Weise auf die bestehende Verpflichtung hinzuweisen, und empfohlen, die die Nutzer des LDKN betreffenden Anforderungen bereits in der Vertragsgestaltung zu berücksichtigen.

Im Gegensatz zu Wählverbindungen zu den IT-Systemen der Verwaltungen werden – hierüber besteht Einvernehmen mit dem DIZ – Wählzugänge zu Anschlusskomponenten des rlp-Netzes, z. B. zu den bei den Verwaltungen installierten LDKN-Routern, nach der Sicherheitspolitik des DIZ unter den gegenwärtigen Voraussetzungen auch weiterhin ausgeschlossen.

21.3.2 Einsatz von Faxkarten und Faxservern

Im Hinblick auf befürchtete Zugriffe von außerhalb wurde der LfD wegen der mit einer Faxanbindung von IT-Systemen bestehenden Risiken um Stellungnahme gebeten. Besondere Sicherheitsrisiken, die allein auf einer Faxanbindung beruhen, bestehen nach Auffassung des LfD für die angeschlossenen IT-Systeme gegenwärtig nicht. Probleme können sich jedoch dort ergeben, wo die Anschlusskomponenten neben dem Faxdienst weitere Kommunikationsmöglichkeiten eröffnen. Daher sollte bei der Auswahl und dem Einsatz entsprechender Produkte darauf geachtet werden, dass etwaige weitere Dienste deaktiviert werden können. Die Konfigurationsmöglichkeiten sollten die Beschränkung lediglich auf die Faxkommunikation sowie die Unterscheidung und ggf. Sperrung von Dial-in-/Dial-out-Verbindungen erlauben. Im Allgemeinen verfügen ISDN-Router über umfangreichere Konfigurations-, Filter- und Sicherungsmöglichkeiten als einfache ISDN-Karten.

Für die bloße Faxkommunikation nicht benötigte Gerätetreiber sollten grundsätzlich nicht installiert werden. Durch geeignete Maßnahmen (z. B. Passwortsicherung der Anschlusskonfiguration, explizite Zugriffsrechte für die Konfigurationsdateien) ist zu verhindern, dass durch die Anwender Änderungen der eingestellten Konfiguration vorgenommen werden. Unter den genannten Voraussetzungen werden etwaige Sicherheitsrisiken auf ein vertretbares Maß beschränkt; gegen eine auf die bloße Faxkommunikation beschränkte Anbindung von IT-Systemen bestehen insoweit keine Bedenken.

Für den Betrieb eines als Faxserver eingesetzten Rechners ist aus Sicht des LfD ergänzend auf folgende Punkte hinzuweisen:

Bereits bei der Beschaffung von ISDN-Karten und Routern ist darauf zu achten, dass diese über ausreichende Sicherheitsfunktionen verfügen. Hierzu zählen die Möglichkeit, Dienstekennungen nach Kommunikationsrichtung zu differenzieren (Empfang/Versand) bzw. explizit zu sperren, die Unterstützung von Authentisierungs- (PAP, CHAP) und Verschlüsselungsverfahren, die Auswertung von CLIP-Rufnummern bzw. entsprechender Tabellen für die Authentisierung und die Protokollierung erfolgreicher/abgewiesener Verbindungen.

Eine gegebenenfalls vorhandene Funktionalität zur Fernwartung (Remote Control) ist grundsätzlich zu deaktivieren, da über diese Funktion das betreffende IT-System über das öffentliche Netz angerufen werden und u. U. vollständig administriert werden kann. Unter anderem können auf diese Art Seitenspeicher gelesen sowie Rufnummern- und Parameterspeicher unbefugt geändert werden. Soweit eine Fernwartung erforderlich ist, sollte diese entsprechend den Empfehlungen des LfD im 15. Tb., Tz. 21.6.2 erfolgen. Bei hohem Schutzbedarf ist darüber hinaus der Einsatz von D-Kanalfiltern zur Überwachung der Steuerungsinformationen vorzusehen.

Soweit reine Faxserver-Lösungen zum Einsatz kommen, sind nicht benötigte Funktionen zu deaktivieren. Dies betrifft insbesondere die Beschränkung auf die für die Faxkommunikation erforderlichen ISDN-Dienstekennungen 02 (G3-Fax, Modem-DFÜ) und 04 (G4-Fax).

Beim Einsatz nicht allein auf die Faxkommunikation beschränkter ISDN- und Gateway-Lösungen ist durch eine entsprechende Konfiguration der Systeme und der jeweiligen Netze sicherzustellen, dass unbefugte Zugriffe auf personenbezogene Daten ausgeschlossen werden. Auf die Speicherung von Anwendungsdaten auf Kommunikationsservern sollte in diesem Zusammenhang verzichtet werden.

Die datenschutzrechtlichen Empfehlungen zum Einsatz von Telefax-Lösungen sind in einer Orientierungshilfe des LfD zusammengefasst (siehe Anlage 20, Datenschutz und Telefax; vgl. auch Tz. 19.5).

21.3.3 Einrichtung von ISDN-Wählleitungsverbindungen

Im Gegensatz zu Festverbindungen ist bei Wählverbindungen der mögliche Teilnehmerkreis nicht festgelegt, d. h., jede Stelle, die über entsprechende Anschlusskomponenten verfügt, kann grundsätzlich eine Verbindung zum Anschluss der Verwaltung und damit zum jeweiligen IT-System herstellen. Die Administration von Vermittlungskomponenten durch Dritte und bestimmte Leistungsmerkmale des ISDN-Dienstes bergen Risiken für die Vertraulichkeit der übermittelten Passwörter und Daten. Gefährdungen ergeben sich, insbesondere beim Anschluss über digitale Nebenstellenanlagen, weiterhin aus Manipulationsmöglichkeiten über den D-Kanal des ISDN-Protokolls.

Grundlegende Elemente einer datenschutzgerechten Lösung sind daher eine ausreichende Authentifizierung der Anschlusskomponenten und Teilnehmer (§ 9 Abs. 2 Nr. 4 LDSG) sowie eine angemessene Sicherung personenbezogener Daten vor unbefugtem Zugriff (§ 9 Abs. 2 Nr. 9 LDSG). Für die Realisierung von ISDN-Wählverbindungen zu IT-Systemen sollten insbesondere folgende Empfehlungen berücksichtigt werden:

– Einrichten einer geschlossenen Benutzergruppe (Closed User Group)

  ISDN erlaubt die Einrichtung geschlossener Benutzergruppen. Dies ermöglicht, dass alle Teilnehmer einer Benutzergruppe untereinander über das öffentliche ISDN-Netz kommunizieren können, Verbindungswünsche von außerhalb sowie Verbindungswünsche von Closed User Group-Teilnehmern an Teilnehmer des öffentlichen ISDN jedoch abgewiesen werden. Die Konfiguration dieses Leistungsmerkmals ist mit dem jeweiligen Anbieter von Telekommunikationsdienstleistungen (Provider) abzustimmen.

– Nutzung von Sicherheitsmechanismen der ISDN-Komponenten

  ISDN-Anschlusskomponenten bieten in der Regel unterschiedliche Möglichkeiten der Authentisierung der beteiligten Teilnehmer und zur Kontrolle des Verbindungsaufbaus. Beispiele sind Passwort Authentication Protocol (PAP), Challenge Authentication Protocol (CHAP) oder Rufnummernanzeige (Calling Line Identification Protocol – CLIP/Connected Line Identification Presentation – COLP). Die jeweils geeigneten Möglichkeiten sind zu nutzen. Eine Authentisierung über das CHAP-Protokoll ist zu bevorzugen, da hierbei keine Passworte im Klartext übertragen werden. Vorteilhaft an der beschriebenen Funktionalität ist, dass die Identifikation durch Komponenten der jeweiligen Kommunikationspartner (ISDN-Router, TK-Anlage, ISDN-Karte) durchgeführt wird und somit vollständig in deren Kontrollbereich liegt. Voraussetzung ist jedoch, dass die Kommunikationspartner über Anschlusskomponenten mit gleicher Funktionalität verfügen. Dies sollte daher im Rahmen der Beschaffung berücksichtigt werden.

– Einrichtung eines automatischen Rückrufs

  Die Einrichtung eines automatischen Rückrufs (Callback) ist immer dann empfehlenswert, wenn für einen festen Kommunikationspartner die Möglichkeit des automatischen Einwählens gewünscht wird. Dies sollte stets in Verbindung mit dem Leistungsmerkmal „Calling Line Identification Presentation“ (CLIP) erfolgen, um sicherzustellen, dass eine Verbindung nur zu den in einer Rufnummernliste vorgegebenen Anschlüssen aufgebaut werden kann. Seitens des Zielanschlusses ist durch eine geeignete Konfiguration sicherzustellen, dass eine Rufumleitung zu anderen Anschlüssen verhindert wird. Zu beachten ist, dass mit dem automatischen Rückruf auch die Kosten der Datenübertragung übernommen werden.

– Deaktivieren nicht benötigter ISDN-Funktionalitäten

  In den Anschlusskomponenten vorhandene, für die Anbindung jedoch nicht benötigte Funktionen sollten deaktiviert werden. Dies betrifft vor allem die für die Datenkommunikation nicht erforderlichen ISDN-Dienstekennungen. Soweit die Anbindung über eine ISDN-Nebenstellenanlage realisiert ist, ist der jeweilige Anschluss entsprechend zu konfigurieren.

– Filterung von Steuerinformationen

  Neben den Kanälen für die Übertragung der Inhalte wird im ISDN-Dienst der D-Kanal für die Übertragung von Steuerinformationen genutzt. Da diese für den Auf- und Abbau der Verbindung sowie die Steuerung des Ablaufs der Kommunikation erforderlich sind, werden sie im Regelfall nicht verschlüsselt. Über Manipulationen der Steuerinformationen können der ordnungsgemäße Betrieb oder die Vertraulichkeit personenbezogener Daten beeinträchtigt werden. Soweit es nach Art der gespeicherten Daten erforderlich ist, sollte daher der Einsatz so genannter „D-Kanal-Filter“ in Betracht gezogen werden.

– Protokollierung der ISDN-Verbindungen

  Von Bedeutung ist hier vor allem die Nachvollziehbarkeit von Verbindungen mit den Angaben Datum, Uhrzeit, Anschlussnummer, Benutzer, Authentisierungsverfahren und -ergebnis. Die Protokollierung ist in regelmäßigen Abständen auf sicherheitsrelevante Vorkommnisse hin auszuwerten (z. B. fehlgeschlagene Verbindungsversuche im Rahmen einer PAP/CHAP-Authentisierung, Verbindungen zu unüblichen Zeiten, Verstöße gegen Zugriffsrechte).

– Dokumentation der ISDN-Konfiguration

  Die Konfigurationseinstellungen der verwendeten Anschlusskomponenten (ISDN-Karte, Router) wie Anschlussnummern und Adressen, eingestellte Leistungsmerkmale, Authentisierungsverfahren, verwendete Protokolle u. Ä. sind zu dokumentieren.

– Verschlüsselung der Kommunikation

  Da bei Wählverbindungen die Datenübertragung in der Regel über Vermittlungseinrichtungen des Providers erfolgt, besteht das Risiko einer bewussten oder zufälligen Kenntnisnahme der Kommunikationsinhalte durch Dritte. Neben den eigentlichen Nutzdaten betrifft dies auch die für die Identifikation und Authentisierung der Teilnehmer im Klartext übertragenen Angaben (Benutzerkennung, Passwörter). Soweit sensible personenbezogene Daten betroffen sind, sollte daher ergänzend eine Verschlüsselung der übertragenen Daten vorgesehen werden.

Die datenschutzrechtliche Verpflichtung, die erforderlichen technisch-organisatorischen Maßnahmen zu treffen, obliegt den einzelnen Verwaltungen (§ 9 Abs. 1 LDSG). Neben den genannten Aspekten ist dabei insbesondere die Konfiguration der betroffenen IT-Systeme, hier vor allem die ordnungsgemäße Verwaltung der über die Wählverbindung zugelassenen Benutzer und die Vergabe von Zugriffsrechten von Bedeutung.

21.3.4 Fernwartung durch nichtöffentliche Stellen

Für verschiedene in der Landesverwaltung eingesetzte Systeme wurden bislang vom DIZ erbrachte Betreuungsleistungen einem privaten Unternehmen übertragen. Betroffen waren insbesondere Systeme im Bereich der Kommunen und der Bezirksregierungen.

Die einschlägigen Leistungen (Pflege der Systemsoftware, Störungsbeseitigung, Fernwartung) sind, wenn sie nicht von den speichernden Stellen selbst erbracht werden, rechtlich als Datenverarbeitung im Auftrag einzuordnen (vgl. hierzu 15. Tb., Tz. 21.6.1). Daraus ergeben sich nach § 4 LDSG bzw. spezialgesetzlichen Vorschriften (z. B. § 80 SGB X) bestimmte Anforderungen an die Vertragsgestaltung und die technisch-organisatorische Durchführung. Soweit Datenverarbeitungsaufträge an nichtöffentliche Stellen vergeben werden, können sich, insbesondere soweit besondere Berufs- und Amtsgeheimnisse betroffen sind, Einschränkungen der Zulässigkeit ergeben. Dies ist vor allem bei im Krankenhausbereich eingesetzten Systemen von Bedeutung.

Bei der Einleitung und Durchführung von Fernwartungsverfahren sind die Empfehlungen des LfD zu den technisch-organisatorischen Maßnahmen im 15. Tb., Tz. 21.6.2 zugrunde zu legen. Für die Vertragsgestaltung hat der LfD vor allem folgende Empfehlungen ausgesprochen:

Soweit es sich beim Auftragnehmer um eine nichtöffentliche Stelle handelt, finden die Vorschriften des LDSG keine unmittelbare Anwendung. Gemäß der Vorgabe aus § 4 Abs. 1 Satz 3 LDSG sollte daher eine Verpflichtung aufgenommen werden, wonach die Bestimmungen des LDSG vom Auftragnehmer zu beachten sind. Eine Beschränkung auf die Beachtung des Datengeheimnisses nach § 8 LDSG ist insoweit nicht ausreichend. Weiterhin ist eine Vereinbarung vorzusehen, nach der sich der Auftragnehmer der Kontrolle des LfD unterwirft. In diesem Zusammenhang sollten auch die Kontrollrechte des Auftraggebers genannt werden.

Um eine ordnungsgemäße Beachtung der sich aus § 8 LDLSLG ergebenden Verpflichtungen zu gewährleisten, sollte mit der auftragnehmenden Stelle vereinbart werden, dass die mit der Durchführung von Wartungsaufgaben betrauten Personen ihrerseits auf die Wahrung des Datengeheimnisses verpflichtet werden. Im Hinblick auf § 8 Abs. 1 Satz 2 LDSG ist dabei deutlich zu machen, dass die Verpflichtung über das Vertragsende hinaus besteht. Nach § 4 Abs. 2 Satz 2 LDSG sind die technischen und organisatorischen Maßnahmen des Datenschutzes, insbesondere bei der Durchführung der Fernwartung, schriftlich festzulegen. Auch aus Gründen der Transparenz sollten die durch den Auftragnehmer sicherzustellenden Maßnahmen im Vertrag dokumentiert und Änderungen nur mit Zustimmung des Auftraggebers zugelassen sein.

Unterauftragsverhältnisse sind nach § 4 Abs. 2 Satz 2 LDSG grundsätzlich zugelassen, soweit sie vertraglich festgelegt sind. Soweit dies beabsichtigt ist, sollte danach eine Vereinbarung getroffen werden, dass der Abschluss weiterer oder die Änderung bestehender Unterauftragsverhältnisse nur mit Zustimmung des Auftragnehmers möglich sind. Dies gilt insbesondere auch für die Beschäftigung sog. „freier Mitarbeiter“.

Die Entwicklung im Bereich der Informationsverarbeitung führt möglicherweise zu Änderungen bei der Art und Weise, in der die vereinbarten Vertragsleistungen technisch erbracht werden. Der Vertrag sollte daher eine Formulierung enthalten, die für den Fall, dass datenschutzrechtlich relevante Sachverhalte betroffen sind, eine gegenseitige Unterrichtung und Abstimmung vorsieht.

Die betroffenen Firmen sind den Empfehlungen des LfD gefolgt und haben entsprechende Vertragsergänzungen vorgenommen.

21.3.5 Gestaltung von Internet-Zugängen und Angeboten

Das Internet hat sich zum globalen Informations- und Kommunikationsmedium entwickelt und dabei auch vor den öffentlichen Verwaltungen nicht Halt gemacht. Zunehmend verfügen öffentliche Stellen über einen Internet-Zugang, sowohl zur Informationsgewinnung als auch zur Bereitstellung eigener Informationen. Mit einem Anschluss an das Internet sind Risiken für den Datenschutz und die Datensicherheit verbunden. Die Rechner und Übertragungswege des Netzes sind durch die Nutzer nicht kontrollierbar, welchen Weg eine Nachricht nimmt oder in welchem Vermittlungsrechner die Nachricht bearbeitet wird, ist nicht transparent. Sicherheitslücken existieren in den Protokollen für die Datenübertragung, in den Implementierungen und Installationen der Programme für die Internet-Dienste und in den angeschlossenen Rechnersystemen.

So stellt das zugrunde liegende TCP/IP-Protokoll bislang keine sicheren Mechanismen zur Identifikation und Authentisierung bereit. Bei vielen gängigen Diensten werden die Inhaltsdaten im Klartext übertragen. Mit speziellen Programmen kann der Datenverkehr im Netz bzw. auf den Netzknoten abgehört, mitgeschnitten und nach relevanten Informationen durchsucht werden. Datenpakete können nicht nur abgehört, sondern auch manipuliert werden. So lassen sich die IP-Adressen von Sender und Empfänger fälschen, die TCP-Sequence Number von Paketen kann häufig vorhergesagt werden, und der Übertragungsweg ist bei dynamischem Routing modifizierbar. Pakete können abgefangen werden, so dass sie nicht an ihrem Ziel ankommen; ein Angreifer kann sie durch eigene Pakete ersetzen. Weiterhin lässt sich die Kommunikation eines autorisierten Nutzers mitschneiden und später wiedereinspielen (Replay Attack), wodurch sich der Angreifer u. U. die Rechte des Nutzers verschaffen kann. Mit verschiedenen „Denial of service"-Attacken können Rechner blockiert oder in ihrer Funktionsfähigkeit beeinträchtigt werden. Neben diesen protokoll- und dienstespezifischen Risiken können sich Sicherheitsprobleme aus über das Internet wirkenden Programmen mit Schadensfunktionen (z. B. Viren, Trojanische Pferde) oder aktiven Komponenten in Angeboten des Word Wide Web (ActiveX, Java-Scripts) ergeben.

Bei Anschluss an das Internet muss daher die Sicherheit bis auf Anwendungsebene beachtet werden. Wenn keine Schutzmaßnahmen ergriffen wurden, kann sich ein Angreifer, oft mit wenig Aufwand, unter Ausnutzung der Sicherheitslücken unberechtigten Zugang zu fremden Rechnern verschaffen und dort Daten ausspähen, manipulieren oder zerstören. Angesichts der Millionen von Internet-Nutzern ist die Zahl potentieller Angreifer groß. Hinzu kommt, dass zunehmend weniger persönliches Know-how für Angriffe erforderlich ist, da die Beschreibungen der Sicherheitslücken, das für Angriffe erforderliche Instrumentarium sowie Handlungsanweisungen ebenfalls im Internet zur Verfügung stehen. Ein Anschluss an das Internet ist angesichts dieser Gefährdungslage aus Datenschutzsicht daher nur vertretbar, wenn zuvor eine Analyse und Bewertung der damit verbundenen Risiken erfolgt ist und den Gefahren durch technische und organisatorische Maßnahmen (Firewall) hinreichend begegnet wird. Die Datenschutzbeauftragten des Bundes und der Länder haben hierzu eine entsprechende Orientierungshilfe herausgegeben (siehe Anlage 23).

Im Zusammenhang mit der Bereitstellung von Informationen im Internet durch die Verwaltung gewinnen für diese auch die medienrechtlichen Regelungen des Informations- und Kommunikationsdienstegesetzes bzw. des Mediendienste-Staatsvertrages an Bedeutung. Internet-Angebote öffentlicher Stellen sind regelmäßig als Teledienste im Sinne des Teledienstegesetzes bzw. Mediendienste nach dem Mediendienste-Staatsvertrag einzuordnen. Aus beiden Rechtsgrundlagen folgen nicht zuletzt technische Anforderungen zur Gewährleistung des Datenschutzes der Nutzer. Hier handelt es sich insbesondere um Kennzeichnungs-, Informations- und Löschungspflichten. Der LfD hat hierzu eine Orientierungshilfe erstellt, die die wesentlichen Anforderungen an die Gestaltung von Internet-Zugängen und -Angeboten zusammenfasst (siehe Anlage 22, Orientierungshilfe zu datenschutzrechtlichen Anforderungen an die Gestaltung von Internet-Zugängen und -Angeboten öffentlicher Stellen in Rheinland-Pfalz).

21.3.6 Gestaltung von Schulverwaltungsprogrammen

Der Einsatz der Informationstechnik hat innerhalb der letzten beiden Jahre an den Schulen des Landes deutlich zugenommen. Neben dem Lehrbereich sind davon vor allem die im Zusammenhang mit der Schulverwaltung anfallenden Arbeiten betroffen, z. B. die Verarbeitung von Schüler- und Lehrerdaten, die Zeugniserstellung oder Schriftverkehr mit Gremien, Verwaltungen und Eltern.

Die datenschutzrelevanten Gesichtspunkte beim Einsatz der Informationstechnik sind in den hierzu ergangenen Vorschriften des Ministeriums für Bildung, Wissenschaft und Weiterbildung näher geregelt (Muster einer Dienstanweisung über den Datenschutz und die Datensicherheit in Schulen, Studienseminaren, Kollegs und im Staatl. Studienkolleg – GMBl. Nr. 11/1997, S. 526 ff. ; Datenschutz und Datensicherheit in der Verwaltung der Schulen bei der Verarbeitung personenbezogener Daten mit Arbeitsplatzrechner [PC] oder in Akten – GMBl. Nr. 9/1996, S. 349 ff.).
Um einen datenschutzgerechten Einsatz zu unterstützen, sollten jedoch bereits die eingesetzten Programme über geeignete Funktionen verfügen. Mehrere Hersteller haben sich in diesem Zusammenhang mit der Bitte um Beratung an den LfD gewandt. Dieser hat dabei folgende generelle Empfehlungen für die Gestaltung von Schulverwaltungsprogrammen ausgesprochen:

– Zugriffskontrolle

  Für den Fall, dass mehrere Anwendergruppen wie Schulleitung, Schulsekretariat, Kollegium usw. vorgesehen sind, ist gemäß § 9 Abs. 2 Nr. 5 LDSG eine differenzierte Zugriffskontrolle in Form unterschiedlicher Benutzerprofile sicherzustellen.

– Betriebssystemzugriff

Ein generell eröffneter Betriebssystemzugriff ist hinsichtlich der Zugriffskontrolle grundsätzlich problematisch, da auf diesem Weg bestehende Zugriffsregelungen ggf. umgangen werden können. Auf einen Betriebssystemzugang aus der Anwendung heraus sollte daher verzichtet werden.

– Datenaustausch

Für den Datenaustausch mit dem Statistischen Landesamt Bad Ems und den Bezirksregierungen sowie für die Übernahme von Daten anderer Anwendungen sollten entsprechende Funktionen zur Verfügung stehen, die einen Zugriff auf Systemebene verzichtbar machen. Gleiches gilt für die zur Abwicklung eines Diskettenaustauschs erforderlichen Dienstprogramme (Exportfunktion, Diskettenformatierung, Datensicherung, Verschlüsselung, Erstellung von Begleitscheinen/Etiketten).

– Protokollierung

Die im Rahmen der Übermittlungs- und Eingabekontrolle nach § 9 Abs. 2 Nr. 6 und 7 LDSG gestellten Anforderungen müssen umgesetzt werden. Die Nutzung des Schulverwaltungsprogramms muss angemessen nachvollziehbar sein. Darüber hinaus sollte die Protokollierung sicherheitsrelevante Ereignisse wie erfolglose Anmeldeversuche und Verstöße gegen Zugriffsbeschränkungen erfassen.

– Löschung

Die Löschung von Datensätzen sollte einzeln oder klassenweise möglich sein, ebenso die Reduzierung der Datensätze auf die für einen Aktennachweis benötigten Angaben. Beides sollte als Menüpunkt zur Verfügung stehen. Die Einhaltung der Löschungszeitpunkte ist möglichst automatisiert zu überwachen, d. h. die Datensätze sollten bereits bei der Anlage mit einem Datum versehen werden können, nach dessen Erreichen eine Prüfung der weiteren Speicherung erfolgen muss.

21.3.7 Protokollierung der Internet-Nutzung

Im Zusammenhang mit der Einrichtung und dem Betrieb von Internet-Zugängen wurde die Frage des zulässigen Umfangs einer Protokollierung von Benutzeraktivitäten an den LfD herangetragen.

Die Protokollierung von Benutzeraktivitäten stellt, wenn diese bestimmten oder bestimmbaren natürlichen Personen zugeordnet werden können, eine Verarbeitung personenbezogener Daten i. S. des LDSG dar. Dies gilt nicht für lediglich statistische Auswertungen ohne Personenbezug.

Soweit eine schriftliche Einwilligung der Betroffenen nach § 5 LDSG nicht vorliegt, ist die Verarbeitung nur aufgrund einer Rechtsvorschrift und nach Maßgabe des LDSG zulässig. Dieses enthält konkrete Regelungen zur Protokollierung in § 7 Abs. 4 sowie § 9 Abs. 2 Nr. 6 und 7 LDSG. Darüber hinaus ist die Speicherung nach § 13 LDSG zulässig, wenn sie zur rechtmäßigen Erfüllung der in der Zuständigkeit der Daten verarbeitenden Stelle liegenden Aufgaben erforderlich ist. Im Hinblick auf Protokolldaten zählt hierzu vor allem die Speicherung für Zwecke der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung des ordnungsgemäßen Betriebs. Dabei steht vor allem die Dokumentation sicherheitsrelevanter, auffälliger oder von allgemeinen Vorgaben abweichender Vorgänge im Vordergrund.

Bezüglich ihrer Nutzung unterliegen Protokolldaten einer engen Zweckbindung. Sie dürfen grundsätzlich nur für die oben genannten Zwecke gespeichert werden. Eine anderweitige Nutzung ist lediglich zur Abwehr erheblicher Gefährdungen der öffentlichen Sicherheit zulässig. Ausdrücklich untersagt ist die Nutzung zu Zwecken der Verhaltens- oder Leistungskontrolle.

In diesem Zusammenhang ist darauf hinweisen, dass die automatisierte Verarbeitung von Bedienstetendaten der Mitbestimmung der Personalvertretung unterliegt. Eine umfassende Information der Nutzer über den Umfang der Protokollierung ist daher wünschenswert.

Für die Überwachung der ordnungsgemäßen dienstlichen Nutzung des Internet-Zugangs durch Angehörige öffentlicher Stellen kommt z. B. die Protokollierung

– der Zugriffe auf aus Sicherheitsgesichtspunkten oder inhaltlichen Gründen untersagte Internet-Adressen,
– der Downloads von bestimmten Servern oder außerhalb eines festgelegten Umfangs,
– des Versandes oder Empfangs von Spam-Mail,
– von Online-Sitzungen, welche einen bestimmten Zeitrahmen überschreiten,
– des Empfangs sicherheitskritischer Inhalte (z. B. bestimmter E-Mail-Attachements)

in Betracht. Für die Protokollierung der Zugriffe von außerhalb sind andere Gesichtspunkte maßgebend.

Eine vollständige Aufzeichnung aller benutzerspezifischen Aktivitäten durch die Systembetreuung, insbesondere die grundsätzliche Speicherung der Inhalte elektronischer Post oder der Äußerungen in Chat-Foren, ist im Allgemeinen nicht erforderlich. Bestimmte Vorkommnisse können es jedoch erfordern, den Umfang der Protokollierung – ggf. vorübergehend – zu erweitern; die Entscheidung hierüber sollte dabei an der Häufigkeit und Bedeutung der aufzuklärenden Umstände orientiert werden.

Inwieweit eine Protokollierung datenschutzrechtlichen Anforderungen entspricht, bemisst sich weiterhin nach der Dauer der Aufbewahrung der Protokolldaten und den bestehenden Zugriffs- und Auswertungsmöglichkeiten. Sie ist Teil der nach § 9 LDSG erforderlichen technisch-organisatorischen Maßnahmen; ihr erforderlicher Umfang orientiert sich damit auch an den übrigen getroffenen Sicherungsmaßnahmen.

Zur privaten Nutzung eines dienstlich bereitgestellten Internet-Zugangs siehe Tz. 20.1.2.

21.3.8 Löschen und Vernichten von Datenträgern

Papier ist in der Verwaltung nach wie vor ein wesentlicher Informationsträger. Daneben kommen magnetische und zunehmend auch optische Datenträger zum Einsatz. Alle Datenträger mit personenbezogenen Daten sind, wenn sie nicht mehr benötigt werden, ordnungsgemäß zu vernichten. Für die Aktenvernichtung sind in der DIN 32757 (01/1995) je nach Sensitivitätsgrad des zu vernichtenden Materials unterschiedliche Sicherheitsstufen und Grenzwerte für Zustand, Form und Größe der nach der Vernichtung verbleibenden Materialteilchen festgelegt.

Den Sicherheitsstufen entsprechen unterschiedliche Stufen der Sensitivität bzw. Vertraulichkeit von Informationsträgern und unterschiedlichem Aufwand für eine etwaige Reproduktion der auf ihnen wiedergegebenen Informationen:

Bei Informationsträgern mit personenbezogenen Daten sollte grundsätzlich eine Vernichtung mindestens nach Stufe 3 der Norm erfolgen, bei welcher eine Reproduktion nur unter erheblichem Aufwand möglich ist. Für besonders sensible personenbezogene Daten (z. B. Sozialdaten, medizinische Daten) ist mindestens die Stufe 4 zugrunde zu legen. Eine Reproduktion ist dabei nur unter Verwendung gewerbeunüblicher Einrichtungen bzw. Sonderkonstruktionen möglich. Bei der Beschaffung entsprechender Geräte ist auf die Erfüllung der DIN-Anforderungen zu achten bzw. bei der Beauftragung entsprechender Unternehmen vertraglich sicherzustellen. Die genannten Anforderungen gelten sinngemäß für die Vernichtung von magnetischem Datenträgermaterial.

Für die Löschung magnetischer Datenträger werden durch die DIN 33 858 (04/1993) vergleichbare Anforderungsstufen festgelegt. Soweit keine Vernichtung der Datenträger erfolgt, ist bei der Löschung von Datenträgern mit personenbezogenen Daten grundsätzlich die Anforderungsstufe B mit einer Löschdämpfung von mind. 90 dB vorzusehen. Alternativ kommen Programme in Betracht, die durch mehrmaliges Überschreiben mit binären Nullen und Einsen eine verlässliche physikalische Löschung sicherstellen.

Bei nur einmalig beschreibbaren optischen Datenträgern, z. B. CD-ROM, WORM, kann keine Löschung erfolgen. In Betracht kommt hier neben dem Schreddern analog zur DIN 32757 das Ätzen, Einschmelzen oder Verbrennen.

21.3.9 Raum- und Gebäudesicherung

Im Berichtszeitraum wurde der LfD im Zusammenhang mit dem Neu- oder Umbau von Verwaltungsgebäuden mehrfach um Beratung hinsichtlich der Absicherung von Räumlichkeiten mit besonderer Bedeutung für den Einsatz der Informationstechnik gebeten. Hierunter fallen insbesondere Räume mit zentralen Komponenten der Informations- und Kommunikationstechnik (z. B. Server-, Verteiler- und TK/DFÜ-Räume), Datenträgerarchive sowie die Arbeitsräume der Mitarbeiter der Systemverwaltung und -betreuung. Im Vergleich zu normalen Büroräumen besteht für die genannten Bereiche ein erhöhter Schutzbedarf.

21.3.9.1 Anforderungen an die Absicherung von Räumen und Gebäuden

Die grundlegenden datenschutzrechtlichen Anforderungen an die Raumsicherung ergeben sich aus § 9 Abs. 2 Nr. 1 (Zugangskontrolle), Nr. 2 (Datenträgerkontrolle) und Nr. 10 (Organisationskontrolle) LDSG. Hierbei spielen insbesondere die Gefährdungen

- unbefugtes Eindringen in Gebäude,
- unbefugter Zutritt zu Räumen,
- unbefugter Zutritt zu IT-Komponenten,
- Entwendung von Datenträgern oder Geräten der Informationstechnik und
- vorsätzliche Manipulationen an IT-Komponenten

eine Rolle. Über vorbeugende Maßnahmen sollte auf der Grundlage einer entsprechenden Schutzbedarfsanalyse entschieden werden. Aus Sicht des Datenschutzes sind für die Absicherung von IT-Bereichen vor allem die folgenden Maßnahmen von Bedeutung:

Gefahrenmeldeanlage

Ist eine Gefahrenmeldeanlage für Einbruch oder Brand vorhanden, ist zu prüfen, inwieweit mit vertretbarem Aufwand die Kernbereiche der IT (Serverräume, Datenträgerarchive, Räume für technische Infrastruktur u. Ä.) in die Überwachung einbezogen werden können. Ist keine Gefahrenmeldeanlage vorhanden oder lässt sich die vorhandene nicht nutzen, kommen ggf. lokale Melder in Betracht. Diese arbeiten selbständig, ohne Anschluss an eine Zentrale. Die Alarmierung erfolgt vor Ort oder über Telefonleitung an anderer Stelle.

Einbruchsschutz

Die gängigen Maßnahmen zum Einbruchsschutz sollten den örtlichen Gegebenheiten entsprechend angepasst werden. Dazu gehören:

- Rollladensicherungen bei einstiegsgefährdeten Türen und Fenstern,
- besondere Schließzylinder, Zusatzschlösser und Riegel,
- Sicherung von Kellerlichtschächten,
- Verschluss von nicht benutzten Nebeneingängen,
- einbruchgesicherte Notausgänge.

Soweit Server- und Verteilerräume nicht ebenerdig zur Gebäudeaußenseite gelegen sind, ist eine darüber hinausgehende Außenhautsicherung im Regelfall nicht erforderlich. Zur Durchwurfhemmung empfiehlt sich die Verwendung von bruchsicherem Glas oder das Anbringen einer Sicherheitsfolie auf der Innenseite. Bei ebenerdig gelegenen IT-Bereichen sollte nach Möglichkeit eine verstärkte Rahmenausführung der Fenster sowie grundsätzlich einbruchhemmendes Glas verwendet werden.

Sicherheitstüren

Sicherheitstüren nach DIN 18 103 oder Schutzklasse T90 nach DIN 4102 bieten aufgrund ihrer Stabilität Schutz gegen Einbruch und verzögern in der Ausführung als selbstschließende feuerhemmende Tür (FH-Tür T30, DIN 18 082) die Ausbreitung eines Brandes. Soweit nicht besondere Umstände vorliegen, wird den datenschutzrechtlichen Anforderungen mit dem Einbau von Sicherheitstüren, Schließhilfen sowie einem Türknauf statt Klinke auf der Außenseite entsprochen. Bei Schließanlagen sollte für den IT-Bereich ein gesonderter Schlüsselkreis gewählt werden.

Lagehinweise auf schützenswerte Gebäudeteile

Schützenswerte Gebäudeteile wie Serverräume, Datenträgerarchiv, TK-Verteilerraum usw. sollten in Bereichen mit Publikumsverkehr keinen Hinweis auf ihre Nutzung tragen, um potentiellen Missbrauchstätern die Vorbereitung von Manipulationen zu erschweren. Stattdessen sollte eine Lageübersicht der Räume in der Brandmeldezentrale vorgehalten werden.

Anordnung schützenswerter Räume

Räume mit zentralen IT-Komponenten sollten nicht in exponierten Bereichen untergebracht sein (z. B. Publikumszonen, Empfangsbereich). Räume zu öffentlichen Verkehrsflächen hin sind durch Anschlag, Vandalismus, schlecht einsehbare Bereiche durch Einbruch gefährdet. Unter Sicherheitsgesichtspunkten sollten schützenswerte Bereiche im Zentrum eines Gebäudes und nicht in ebenerdigen Räumen untergebracht sein.

Datensicherungsschränke

Für die Aufbewahrung von Datenträgern kommen Datensicherungsschränke nach VDMA 24991 in Betracht. Diese bieten je nach Spezifikation ausreichenden Einbruchsschutz bzw. Schutz von Datenträgern im Brandfall.

21.3.9.2 Empfehlungen des Gemeindeversicherungsverbandes zur Schadensminderung bei Einbrüchen

Zur Schadensminderung bei Einbrüchen hat der Versicherungsverband für Gemeinden und Gemeindeverbände (GVV) empfohlen, Innenräume und Mobiliar nach Dienstschluss grundsätzlich nicht zu verschließen. Die Empfehlung des Versicherungsverbandes ist angesichts der häufigen Schäden nachvollziehbar, die Entscheidung hierüber kann jedoch nicht allein unter dem Gesichtspunkt der Schadensminderung getroffen werden, da von ihr unmittelbar datenschutzrechtliche Belange berührt sind. Aus Sicht des LfD ist für Räume mit zentralen IT-Komponenten ein im Vergleich zu sonstigen Büroräumen höherer Schutz zu fordern. In seiner Stellungnahme gegenüber dem Versicherungsverband hat der LfD daher auf Folgendes hingewiesen:

§ 9 Abs. 4 LDSG verpflichtet die öffentlichen Stellen, Maßnahmen zu treffen, die verhindern, dass bei der Aufbewahrung von Akten Unbefugte zugreifen können. Ähnliches gilt nach § 9 Abs. 2 Nr. 2 LDSG für Datenträger. Demzufolge sind die Bediensteten in vielen Fällen angewiesen, bei Abwesenheit die Diensträume zu verschließen. Hintergrund ist dabei weniger die Absicht, Einbrüche auszuschließen, als vielmehr eine unbefugte Kenntnisnahme, z. B. durch Besucher, Reinigungskräfte oder auch durch andere Bedienstete der Verwaltung, zu verhindern. Durch einen generellen Verzicht auf das Verschließen von Räumen und Mobiliar würde dem nicht entsprochen.

Das Gebot wirtschaftlichen Handelns erfordert es andererseits zu prüfen, inwieweit zu einer Schadensminderung beigetragen werden kann. Dabei sollte nicht unberücksichtigt bleiben, dass Diebstähle nicht ausschließlich auf Einbrüche zurückzuführen sind und, insbesondere bei Behörden mit Publikumsverkehr, somit gerade der Verschluss von Räumen und Mobiliar Schäden vermeidet. Aus datenschutzrechtlicher Sicht sollten bei der Entscheidung folgende Punkte Beachtung finden:

- Für Räume, in denen eine Verarbeitung personenbezogener Daten nicht erfolgt, besteht keine Notwendigkeit, diese zu verschließen (z. B. Aufenthaltsräume, Besprechungszimmer, u. U. Bibliothek, Kopierräume usw.). Gleiches gilt für Mobiliar, in welchem keine Akten oder Datenträger mit personenbezogenen Daten aufbewahrt werden.

- Sonstige Räume brauchen dann nicht verschlossen zu werden, wenn keine Akten mit personenbezogenen Daten im Zugriff stehen. Damit könnte nach Dienstschluss auf das Verschließen von Innentüren verzichtet werden, wenn durch organisatorische Maßnahmen sichergestellt ist, dass Akten z. B. in gesonderten Registraturen oder geeigneten Schränken unter Verschluss aufbewahrt werden. Das Verschließen von Diensträumen oder Büromobiliar kann damit auf das erforderliche Maß beschränkt werden.

- Soweit das Verschließen der Diensträume der Absicherung des Zugangs zu Datenverarbeitungsgeräten dient, kommen ersatzweise auch andere und zum Teil geeignetere Möglichkeiten in Betracht (Verriegelung der Geräte, Tastatur- und Bildschirmsperre, Zugriffskontrolle über Benutzerkennung und Passwort usw.). Wenn die unbefugte Inbetriebnahme, Nutzung oder Entwendung von Datenverarbeitungsgeräten durch alternative Maßnahmen ausgeschlossen wird, kann auf das Verschließen der Räume verzichtet werden.

- Räume mit zentralen Komponenten der Informationstechnik (Netzwerk-Server, Datenfernübertragungsanschlüsse usw.) sind unter Datenschutzgesichtspunkten regelmäßig unter Verschluss zu halten. Die besondere Bedeutung dieser Bereiche für den ordnungsgemäßen Betrieb der eingesetzten Verfahren erfordert eine im Vergleich zu sonstigen Diensträumen stärkere Absicherung.

- Datenträger mit personenbezogenen Daten sollten am Arbeitsplatz nur aufbewahrt werden, wenn hierfür geeignete Behältnisse (z. B. Datensicherungsschränke) zur Verfügung stehen. Auch der Versicherungsverband geht im Hinblick auf Wertgegenstände in seinen Hinweisen von der Schaffung entsprechender zusätzlicher Sicherungsmöglichkeiten aus. Schreibtische oder normale Büroschränke sind für die Aufbewahrung von Datenträgern ohnehin nur bedingt geeignet, da ein ausreichender Schutz z. B. im Brandfall nicht gewährleistet ist.

Damit ist in vielen Bereichen die Möglichkeit gegeben, den Empfehlungen des Versicherungsverbandes zu folgen und gleichzeitig datenschutzrechtlichen Anforderungen zu entsprechen.

21.3.10 Empfehlungen zum Einsatz von Verschlüsselungsverfahren

Der Einsatz kryptografischer Verfahren wird vom LfD bei besonderer Sensibilität der betroffenen Daten empfohlen, beispielsweise dann, wenn besondere Berufs- und Amtsgeheimnisse nach § 203 StGB berührt sind, was vorrangig bei Gesundheits- und Sozialdaten der Fall ist. Die Verschlüsselung spielt vor allem dann eine Rolle, wenn Daten auf öffentlichen Übertragungswegen bzw. auf Kommunikationsstrecken, die nicht unter der Kontrolle der beteiligten öffentlichen Stellen stehen, übertragen werden.

In technischer Hinsicht sind dabei als sicher anerkannte Verfahren mit ausreichender Schlüssellänge zu verwenden. Lösungen, die auf einer einfachen DES-Verschlüsselung oder einer effektiven Schlüssellänge von lediglich 40 Bit beruhen, genügen dem im Allgemeinen nicht. Geeignete Algorithmen sind z. B. Triple DES mit 112 Bit, IDEA mit 64 Bit Schlüssellänge oder größer. Für asymmetrische Verfahren wie RSA wird ein Schlüssel von 1 024 Bit oder mehr empfohlen. Sonstige Lösungen kommen in Betracht, wenn diese nachweislich eine vergleichbare Sicherheit bieten. Die Entscheidung sollte sich jedoch nicht ausschließlich auf die verwendeten Algorithmen und Schlüssellängen stützen. Für die Beurteilung des mit einer bestimmten Lösung verbundenen Sicherheitsniveaus sind weitere Faktoren wie Schlüsselerzeugung, -verteilung und -management, organisatorische Regelungen oder die Verwendung zertifizierter Produkte von Bedeutung. Soweit z. B. im Rahmen einer Leitungsverschlüsselung ein regelmäßiger Wechsel von Session-Keys erfolgt, kann auch bei kürzerer Schlüssellänge ein ausreichendes Maß an Datensicherheit gewährleistet sein.

21.3.11 E-Mail in der Verwaltung

Die elektronische Post hat sich als Form des Austauschs und der Übertragung von Informationen in den Verwaltungen etabliert. Sie wird für die interne Kommunikation genutzt, für Mitteilungen an andere Behörden und im Verkehr mit dem Bürger; vielfach dient dabei das Internet als Kommunikationsmedium.

Aufgrund der technischen Gegebenheiten im Internet ist ein angemessener Schutz personenbezogener Daten häufig nicht gewährleistet. Die Vertraulichkeit der übertragenen Daten, ihre Vollständigkeit, der Schutz vor unerlaubten Veränderungen (Integrität) sowie die verlässliche Zurechenbarkeit zu einem bestimmten Absender (Authentizität) müssen gegebenenfalls durch zusätzliche Maßnahmen sichergestellt werden.

Die datenschutzrechtlichen Anforderungen ergeben sich u. a. aus § 9 Abs. 2 Nr. 9 LDSG. Danach sind bei der Übertragung personenbezogener Daten via E-Mail Maßnahmen zu treffen, die gewährleisten, dass Nachrichten nicht unbefugt gelesen, kopiert, verändert oder gelöscht werden können. Weitere datenschutzrechtliche Gesichtspunkte sind die Löschung von Nachrichten und die Protokollierung der E-Mail-Nutzung.

Der LfD hat die für die Erstellung einer Dienstanweisung nach § 9 Abs. 5 LDSG relevanten Gesichtspunkte in einer Orientierungshilfe zusammengefasst (siehe Anlage 21, Hinweise zur datenschutzgerechten Gestaltung und Nutzung von E-Mail-Diensten durch öffentliche Stellen).

21.4 Entwicklung des Datenschutzregisters

Verfahren, in denen personenbezogene Daten automatisiert verarbeitet werden, sind beim LfD zur Eintragung in das dort geführte Datenschutzregister anzumelden (§ 27 LDSG). Für den LfD bilden diese Eintragungen eine wichtige Grundlage der Kontrollarbeit. Auch die behördlichen Datenschutzbeauftragten können aus den Anmeldungen die Informationen entnehmen, die sie für die Wahrnehmung ihrer Aufgaben nach § 11 LDSG benötigen.

Häufig werden datenschutzrechtliche Defizite, wie z. B. das Fehlen von Löschungsfristen oder Speicherungen nicht erforderlicher personenbezogener Merkmale in automatisierten Verfahren nur aufgrund von Anmeldungen zum Datenschutzregister bekannt. Fernerhin gab es in der Vergangenheit auf Grund der Anmeldungen häufig Veranlassung, örtliche Feststellungen durchzuführen und datenschutzrechtliche Verbesserungen anzuregen.

Die Bedeutung des Datenschutzregisters für die Datenschutzkontrolle wird auch aus der zahlenmäßigen Entwicklung der Anmeldungen erkennbar. Bei der Umstellung im Jahre 1986 waren im Datenschutzregister ca. 3 200 Anwendungen gespeichert, heute sind es bereits über 7 600 (vgl. Anlage 24).

In der Vergangenheit wurden im Durchschnitt ca. 200 Verfahren pro Jahr neu angemeldet. 1998 lag die Zahl der Anmeldungen bereits bei 490 und 1999 wurden bis September ca. 380 Verfahren neu angemeldet. Nicht zu vernachlässigen ist in diesem Zusammenhang auch, dass dem LfD immer häufiger Änderungsmeldungen zu bereits angemeldeten Verfahren vorgelegt werden.

Der LfD ist bemüht, den mit dem Anmeldeverfahren verbundenen Verwaltungsaufwand so gering wie möglich zu halten. Neben der Möglichkeit, zentral entwickelte Verfahren verkürzt anzumelden, hat er auch das von ihm entwickelte Anmeldeformular auf Diskette zur Verfügung gestellt. Derzeit werden Überlegungen angestellt, dieses Formular auch im Internet bereitzustellen.

22. Datenverarbeitung bei Sparkassen

22.1 SIS West

Nach der Verschmelzung der Sparkassen-Informatik-Gesellschaft Rheinland-Pfalz mbH, Mainz, mit dem Sparkassen-Rechenzentrum Rheinland GmbH ab 1. Januar 1998 wurde die Sparkassen-Informatik-Systeme West GmbH (SIS West), Duisburg, mit der Datenverarbeitung durch Sparkassen in Rheinland-Pfalz beauftragt. Sie betreibt Rechenzentren in Duisburg und in Köln.

Die SIS West unterliegt generell als öffentlich-rechtliches Wettbewerbsunternehmen der Kontrolle der Landesbeauftragten für den Datenschutz in Nordrhein-Westfalen. Bei der Verarbeitung der Daten für die rheinland-pfälzischen Sparkassen durch die SIS West handelt es sich um Datenverarbeitung im Auftrag gem. § 4 LDSG. Verantwortlich für die Einhaltung des Datenschutzes bleiben damit die jeweiligen Sparkassen als Auftraggeber. Der Auftragnehmer hat sich gem. § 4 Abs. 1 Satz 3 LDSG der Kontrolle des LfD zu unterwerfen. Diese Kontrollkompetenz beschränkt sich jedoch auf die Auftragsdatenverarbeitung. Aufgrund der Überwachungstätigkeit der Landesbeauftragten für den Datenschutz Nordrhein-Westfalen sah der LfD bisher noch nicht die Notwendigkeit, von dieser Kompetenz Gebrauch zu machen.

22.2 Datenübermittlung durch eine Sparkasse an das Arbeitsamt

Dem LfD wurde vorgetragen, dass eine Sparkasse Auskünfte über das Girokonto und das Sparkonto eines Kunden gegenüber dem Arbeitsamt gegeben habe. Der Petent sah sich dadurch in seinen Rechten verletzt.

Aufgrund der Neufassung des § 144 AFG (jetzt § 315 Abs. 2 SGB III) besteht die gesetzliche Verpflichtung, im Rahmen der Bedürftigkeitsprüfung bei der Arbeitslosenhilfe Auskunft über Guthaben und Vermögensgegenstände des Arbeitslosen, seines Ehegatten oder Partners einer eheähnlichen Gemeinschaft an das zuständige Arbeitsamt zu erteilen.

Folglich war die Datenübermittlung nicht zu beanstanden.

22.3 Datenübermittlung durch eine Sparkasse an den Schlichter des Sparkassen- und Giroverbandes

Im Rahmen einer Eingabe hatte sich der LfD mit folgendem Sachverhalt zu befassen:

Der Kunde einer Sparkasse hatte sein Girokonto bei diesem Kreditinstitut gekündigt und bei einer anderen Bank ein neues eröffnet. Die neue Bankverbindung teilte er der Sparkasse mit, damit diese von dort die Raten für einen bestehenden Kredit abbuchen konnte. Als das Girokonto bei der Sparkasse aufgelöst wurde, war eine Abwicklungsgebühr fällig, die die Sparkasse vom neuen Girokonto des Petenten abbuchte. Als dieser sich wegen der geschilderten Vorgehensweise beim Vorstand der Sparkasse beschwerte und dabei auch den bestehenden Kredit erwähnte, leitete der Vorstand den Vorgang dem Schlichter des Sparkassen- und Giroverbandes zu. Dieser wiederum bat die Sparkasse um Stellungnahme zu dem Vorgang, wobei auch die Höhe des bestehenden Kredits genannt wurde. Der Petent vertrat die Auffassung, dass der bestehende Kredit nichts mit dem Beschwerdegegenstand zu tun gehabt hätte und daher dem Schlichter auch nicht zur Kenntnis hätte gebracht werden dürfen.

Aus datenschutzrechtlicher Sicht hat der LfD die Angelegenheit wie folgt beurteilt:

Die Schlichtungsstelle des Sparkassen- und Giroverbandes wird aufgrund der Schlichtungsordnung der rheinland-pfälzischen Sparkassenorganisation sowohl für die Sparkassen wie für ihre Kunden tätig. Im Vermittlungsfall besteht ein besonderes Schlichtungsverhältnis zwischen diesen drei Stellen. Für die in diesem Zusammenhang erfolgenden Datenübermittlungen ist § 28 Abs. 1 BDSG maßgeblich: Danach ist das Übermitteln personenbezogener Daten als Mittel für die Erfüllung eigener Geschäftszwecke zulässig, wenn dies im Rahmen der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen liegt.

Datenübermittlungen zwischen den drei im Rahmen eines Schlichtungsverhältnisses beteiligten Stellen sind also dann zulässig, wenn sie im Rahmen der Zweckbestimmung des Schlichtungsverhältnisses liegen. Damit ist keine strikte Erforderlichkeitsprüfung anzustellen: Es reicht aus, dass die fraglichen Daten zum Zweck der Durchführung der Schlichtung übermittelt werden. Diese Voraussetzung lag auch bei der Datenübermittlung durch die Sparkasse an den Schlichter bezüglich der Höhe des in Anspruch genommenen Kredites vor.

Zwar hätte es für die Beurteilung des der Schlichtung unterworfenen Sachverhaltes dieser Information nicht unabdingbar bedurft. Doch konnte die Information über die näheren Modalitäten der zwischen dem Petenten und der Sparkasse bestehenden Geschäftsverbindung durchaus auch im Rahmen der Schlichtung bedeutsam sein. Es war jedenfalls nicht festzustellen, dass die hier zu beurteilende Datenübermittlung außerhalb des Zwecks der Schlichtung gelegen hätte.

Es kommt hinzu, dass der Schlichter gem. Nr. 4 lit. c der Schlichtungsordnung der rheinland-pfälzischen Sparkassenorganisation zur Verschwiegenheit über alle den Kunden oder die Sparkasse betreffenden Tatsachen und Wertungen verpflichtet ist, von denen er im Rahmen des Schlichtungsverfahrens Kenntnis erlangt.

Damit war aus Sicht des LfD ein zu beanstandendes Verhalten der Sparkasse im vorliegenden Zusammenhang nicht festzustellen.

22.4 Personalausweiskopie als Voraussetzung einer Vollmachtserteilung

Der LfD hatte sich mit der Vorgehensweise einer Sparkasse bei einer Vollmachtserteilung zu befassen: Ein Ehepaar beabsichtigte, seinen Kindern für den Fall seines Todes eine Bankvollmacht zu erteilen. Dazu verlangte die Sparkasse das Ausfüllen eines dafür vorgesehenen Formulars sowie die beglaubigten Unterschriften der Kinder. Zusätzlich sollten Kopien der Personalausweise der Kinder vorgelegt werden.

Der LfD hat die Sparkasse darauf hingewiesen, dass aus seiner Sicht Bedenken bestehen, ob im vorliegenden Fall die Forderung nach Personalausweiskopien der bevollmächtigten Personen mit den datenschutzrechtlichen Vorschriften (hier: § 28 Abs. 1 Nr. 1 i. V. m. Satz 2 BDSG) übereinstimmt. Aus seiner Sicht war in diesem Zusammenhang die Aufnahme von Ausweiskopien in die Unterlagen der Bank nur aufgrund der Einwilligung der Betroffenen zulässig. Eine Forderung, solche Kopien der Bank zu übergeben, ohne Hinweis auf die Freiwilligkeit, vielmehr mit der Behauptung, das angestrebte Rechtsgeschäft sei ohne diese Datenpreisgabe unwirksam, verstieß jedenfalls auch gegen den Grundsatz des § 28 Abs. 1 Satz 2 BDSG, wonach die Daten nach Treu und Glauben und auf rechtmäßige Weise erhoben werden müssen.

Die Sparkasse hat sich dieser Auffassung angeschlossen und die Mitarbeiter nochmals auf eine auch unter datenschutzrechtlichen Gesichtspunkten ordnungsgemäße Sachbearbeitung hingewiesen.

22.5 Schufa-Anfragen durch öffentliche Stellen

Werden Gemeindekassen als Vollstreckungsbehörden tätig, holen sie Auskünfte über Schuldner häufig bei der Schufa ein. Dies führte zu einer Anfrage der Schufa beim LfD, ob eine solche Vorgehensweise überhaupt zulässig sei.

Im Bereich der Vollstreckung gemeindlicher Abgaben gelten gem. § 3 Abs. 1 Nr. 3 KAG für die Sachverhaltsaufklärung auch im Vollstreckungsverfahren die §§ 88 ff. AO, ergänzend das Landesverwaltungsvollstreckungsgesetz. Danach ermitteln die Vollstreckungsbehörden den Sachverhalt von Amts wegen und bestimmen Art und Umfang der Ermittlungen. Für die Vollstreckung sonstiger gemeindlicher Ansprüche gilt daneben insbesondere für die Datenerhebung bei Dritten das Verwaltungsverfahrensgesetz, ergänzend die §§ 12 ff. LDSG (gem. § 2 Abs. 8 LDSG).

Insbesondere war zu klären, ob nicht vorrangig die Abnahme einer eidesstattlichen Versicherung in Betracht kommt, bevor sich die Vollstreckungsbehörde an die Schufa wendet. Einen generellen Vorrang der eidesstattlichen Versicherung vor einer Schufa-Anfrage sieht der LfD nicht. Vielmehr vertritt er die Auffassung, dass das Ermittlungsverfahren in Zusammenhang mit der Vollstreckung nicht durch die Abgabe einer eidesstattlichen Versicherung nach § 284 AO beeinflusst wird. Die Vollstreckungsbehörde muss bei Ausübung ihres Ermessens, ob sie den Sachverhalt gem. §§ 88 ff. AO (bzw. den o. g. Vorschriften des LVwVG und des LDSG) ermittelt oder ob sie die Abgabe der eidesstattlichen Versicherung einleitet, das für den Vollstreckungsschuldner jeweils am wenigsten belastende Mittel wählen. Die eidesstattliche Versicherung soll erst dann verlangt werden, wenn die sonstigen Ermittlungen nicht zum Erfolg führen oder mit deren Misserfolg sicher zu rechnen ist. Die Auffassung, dass umgekehrt zunächst die eidesstattliche Versicherung verlangt werden sollte und sonstige Ermittlungshandlungen erst nachrangig durchzuführen wären, ist aus Sicht des LfD unzutreffend.

Aus datenschutzrechtlicher Sicht ist die Datenerhebung bei der Schufa eine von den gesetzlichen Vorschriften grundsätzlich gedeckte Form der Datenerhebung; sie geht im Ergebnis nicht zu Lasten des Datenschutzes, denn sie entlastet den Schuldner von anderen Ermittlungsmaßnahmen der Vollstreckungsbehörden, die diesen möglicherweise sehr viel intensiver beeinträchtigen würden, wie etwa die Nachfrage bei den örtlichen Kreditinstituten.

23. Sonstiges

23.1 Das nachkartende Katasteramt

Zur Sachverhaltsaufklärung im Zusammenhang mit der Bearbeitung von Eingaben ist es häufig unerlässlich, gegenüber den betroffenen öffentlichen Stellen die Namen der Petenten zu nennen. Es entspricht der ständigen Praxis des LfD, solche personenbezogenen Recherchen nur mit Einwilligung der Betroffenen vorzunehmen.

Ein anschauliches Beispiel dafür, wie verärgert Behörden gelegentlich reagieren, wenn Bürger ihre Datenschutzrechte wahrnehmen, ist das Schreiben eines Katasteramtes mit folgendem auszugsweise wiedergegebenen Text:

> „Wir sehen Veranlassung auf die von Ihnen ausgelösten, höchst unerfreulichen Vorgänge – hoffentlich abschließend – zurückzukommen. ... Es ist häufiger versucht worden, Ihnen den simplen Sachverhalt schriftlich ausführlich darzulegen. ... Bei solch hoffnungsloser Verstocktheit verbietet sich natürlich jedweder Versuch weiter gehender Sachverhaltserläuterung. ... Ihrem von Energie, Ausdauer und unnachahmlicher Aufsässigkeit durchdrungenen einschlägigen Weiterwirken endlich wenigstens einen Achtungserfolg wünschend verbleiben wir mit freundlichen Grüßen ...“

Der LfD hielt in Übereinstimmung mit dem Betroffenen eine Überprüfung des Schreibens durch die zuständige Aufsichtsbehörde für angezeigt.

23.2 Einsichtnahme in Bauakten durch Dritte

Für eine Verbandsgemeindeverwaltung stellte sich die Frage, unter welchen Voraussetzungen Dritte Einsicht in Bauakten anderer nehmen können.

Der LfD hat diese Frage wie folgt beurteilt:

Nach § 29 Abs. 1 Satz 1 VwVfG hat die Behörde den Beteiligten Einsicht in die das Verfahren betreffenden Akten zu gestatten. Die Beteiligtenfähigkeit ist in § 13 VwVfG geregelt. Dritte, die nicht gem. § 13 Abs. 1 VwVfG Beteiligte sind, können von Amts wegen oder auf Antrag als Beteiligte gem. § 13 Abs. 2 VwVfG hinzugezogen werden, wenn deren rechtliche Interessen durch den Ausgang des Verfahrens berührt werden können. Ein noch unbeteiligter Dritter, der Akteneinsicht begehrt, könnte demnach beantragen, als Beteiligter hinzugezogen zu werden. Dies setzt voraus, dass der Antragsteller die mögliche Berührung seiner rechtlichen Interessen geltend macht und die Behörde dies prüft. Sollte ein Antrag auf Hinzuziehung als Beteiligter nicht gestellt werden, könnte der Antrag auf Akteneinsicht in diesem Sinne ausgelegt werden.

Auch wenn das Verfahren bereits für die Beteiligten abgeschlossen sein sollte, hat die Hinzuziehung eines Dritten als Beteiligten gerade in Hinsicht auf das Recht auf Akteneinsicht und die Entscheidung über eine Rechtsmitteleinlegung bis zu dem Zeitpunkt praktische Bedeutung, bis zu dem von Dritten noch Rechtsmittel eingelegt werden könnten. Ein Dritter wird des Öfteren erst nach Abschluss eines Verwaltungsverfahrens Kenntnis von dem zugrunde liegenden Sachverhalt erhalten und muss auch dann noch über die Möglichkeit verfügen können, seine Rechte zu wahren. Eine Hinzuziehung als Beteiligter ist daher nach Ansicht des LfD bis zum Zeitpunkt des bestandskräftigen Abschlusses des Verwaltungsverfahrens zulässig.

Wenn ein Akteneinsichtsrecht nach Verwaltungsverfahrensgesetz nicht besteht, könnte ein solches nach § 16 Abs. 1 Nr. 3 LDSG gegeben sein. Das setzt neben der Glaubhaftmachung eines rechtlichen Interesses auch voraus, dass überwiegende schutzwürdige Interessen des Betroffenen nicht entgegenstehen. Hier ist also zusätzlich eine Interessenabwägung durch die entscheidende Behörde vorzunehmen.

Außerdem könnte ein Akteneinsichtsrecht nach dem Umweltinformationsgesetz bestehen. Nach § 4 UIG hat jeder Anspruch auf freien Zugang zu Informationen über die Umwelt, die bei einer Behörde vorhanden sind. Dieser Anspruch besteht gem. § 8 Abs. 1 Nr. 1 UIG dann nicht, soweit durch Bekanntwerden der Informationen personenbezogene Daten offenbart und dadurch schutzwürdige Interessen der Betroffenen beeinträchtigt werden. Danach wäre auch hier stets eine Interessenabwägung bei der Entscheidung über die Akteneinsicht vorzunehmen.

24. Schlussbemerkung

24.1 Zur Situation der Geschäftsstelle

Im Berichtszeitraum ist der langjährige Stellvertreter des LfD in den Ruhestand getreten. Insbesondere in den Bereichen der polizeilichen Datenverarbeitung und der Datenverarbeitung durch den Verfassungsschutz hat er sich durch die Herstellung intensiver Kontakte zu den von ihm zu kontrollierenden Bereichen verdient gemacht. Aufgrund der geschäftsstelleninternen Nachfolgeregelung wurde eine Beamtenstelle frei, die zeitnah besetzt werden konnte. Durch eine Änderung der internen Struktur der Geschäftsstelle, die Schaffung von vier Referaten, wurden Tätigkeitsfelder gebündelt und effizienter organisiert.

Bereits im 16. Tb. (Tz. 24.1) hat der LfD zum Ausdruck gebracht, dass er in Bezug auf die Personalausstattung im Bereich des technischen Datenschutzes eine Verstärkung mittelfristig für unabdingbar halte. Die Notwendigkeit, auch angesichts der immer dramatischer werdenden Haushaltslage des Landes die Geschäftsstelle in diesem Sektor zu vergrößern, hat sich bestätigt. Für die anstehende Aufstellung des Doppelhaushalts 2000/2001 hat der LfD deshalb für das Referat „technisch-organisatorischer Datenschutz“ eine zusätzliche Stelle beantragt. Als Begründung hat er in erster Linie angeführt, dass sich der Kontroll- und Beratungsaufwand in seiner Dienststelle wegen der flächendeckenden Einführung von IT-Lösungen in den letzten Jahren quantitativ und qualitativ erheblich erhöht hat. Ein Indiz für die zunehmende Bedeutung des technischen Kontroll- und Beratungsaufwands lässt sich aus der Steigerung der Zahl der neu angemeldeten automatisierten Verfahren ablesen: Im Jahr 1998 wurden 490 Verfahren neu angemeldet (im Vergleich dazu: im Jahre 1994 waren es noch 200 Verfahren).

Auch die verstärkte Nutzung der digitalen Kommunikationsnetze begründet einen verstärkten datenschutzrechtlich orientierten technischen Beratungsbedarf. Es kommt hinzu, dass die Dezentralisierung der Informationsverarbeitung (die zu einem Bedeutungsverlust der Rechenzentren und zu einer Verlagerung der DV-Kapazitäten zu den Kommunen führt), die Vernetzung innerhalb und zwischen Behörden, der Einsatz von Chipkarten, die Nutzung des Internets sowie die Einführung neuer Arbeitsformen wie der Telearbeit die Anforderungen an die technische Beratung beim LfD verstärken.

Mit nur 1,5 Stellen im Bereich des technischen und organisatorischen Datenschutzes bildet die Personalausstattung des rheinland-pfälzischen Datenschutzbeauftragten (zusammen mit dem Saarland) das Schlusslicht unter allen Datenschutzbeauftragten des Bundes und der Länder. Nach Einwohnern und Fläche kleinere Länder haben in diesem Bereich beispielsweise bis zu neun Bedienstete; selbst das kleinste Bundesland verfügt im Technikbereich über erheblich mehr Personal als Rheinland-Pfalz.

Diese Situation ist aus der Sicht des LfD nicht mehr länger akzeptabel. Die Entwicklung der Informationstechnologie, die auch auf der Ebene des Landes zu Recht im Allgemeininteresse durch den Staat mit erheblichen Mitteln gefördert wird, verläuft stürmisch und verursacht einen wesentlichen Strukturwandel hin zur Informationsgesellschaft. Es ist erforderlich, dass die Bürger bei dieser Entwicklung darin unterstützt werden, Eigenvorsorge zu treffen und dass auch für die öffentlichen Stellen ein unabhängiger und kompetenter Berater und Kontrolleur zur Verfügung steht. Die komplexeren Aufgaben, vor die jeder Einzelne, aber auch die öffentlichen Stellen des Landes gestellt werden, dürfen nicht ohne Orientierung durch den Staat bleiben. In diesem Zusammenhang hat der LfD eine wichtige Funktion, deren Erfüllung ihm durch eine angemessene – wenn schon nicht optimale, so doch ausreichende – Personalausstattung zu ermöglichen ist. Nur dann kann er seinen gesetzlichen Auftrag erfüllen.

Die Realisierungschancen dieses Anliegens des LfD sind derzeit noch nicht abschließend abschätzbar.

Die Unterstützung durch die Landtagsverwaltung (z. B. Druckerei, Personalabteilung, Poststelle etc.) und ihre Leitung bei der Wahrnehmung der Verwaltungsaufgaben des LfD hat sich im Berichtszeitraum wiederum bewährt. Dadurch konnten die vorhandenen Personalressourcen optimal für die Erfüllung seiner sachlichen Aufgaben eingesetzt werden. Ein Umzug konnte trotz der neuen Raumsituation der Landtagsverwaltung vermieden werden. Dadurch konnten Haushaltsmittel in durchaus nennenswerter Höhe eingespart und Störungen des Arbeitsablaufs vermieden werden. Auch dafür gebührt der Landtagsverwaltung, insbesondere deren Direktor, Dank.

Den Mitarbeiterinnen und Mitarbeitern der Dienststelle des LfD, die ihre Aufgaben engagiert und umsichtig erfüllt haben, gebührt dafür Anerkennung und Dank. Besonders zu danken ist dem früheren stellvertretenden LfD, Herrn LMR Dr. Reiner von Dietel, der bis zum Eintritt in den Ruhestand zum 31. August 1998 dem Datenschutz nahezu 20 Jahre mit seinem herausragenden Fachwissen und Energie erfolgreich gedient hat.

24.2 Veröffentlichungen der Dienststelle

In der Schriftenreihe „Informationen zum Datenschutz“ des LfD sind die Hefte zum technischen und organisatorischen Datenschutz (Heft 2) sowie zum Datenschutz im Krankenhaus (Heft 4; vgl. Tz. 10.8.2) überarbeitet worden. Sie sind in der Neuauflage erneut auf eine große Nachfrage gestoßen.

Die Verwaltungen nutzen in erheblichem Maß die Möglichkeit, datenschutzrechtliche Orientierungshilfen auf einer Diskette zu beziehen und sie auf diesem Wege auszuwerten.

Der LfD ist auch als Anbieter von Informationen im Internet vertreten: Unter „http://www.datenschutz.rlp.de“ können grundlegende und auch aktuelle Informationen zu Datenschutzfragen abgerufen werden. Neben den bereichsbezogen gegliederten Auszügen aus den Tätigkeitsberichten stehen dort u. a. die Hefte der Schriftenreihe zum Datenschutz sowie Hinweise und Orientierungshilfen zu technisch-organisatorischen Fragen zur Verfügung. Der LfD ist bemüht, dieses Angebot ständig technisch und inhaltlich zu verbessern. Zu betonen ist, dass ihm dies bislang mit minimalen Haushaltsmitteln (in einer Größenordnung von insgesamt bislang ca. 2 000,– DM zuzüglich eigener Arbeitsleistungen) gelungen ist.

Anlässlich des 25-jährigen Jubiläums des Datenschutzrechts in Rheinland-Pfalz wird der LfD eine CD-ROM herausgeben, auf der unter anderem die im Internet verfügbaren Informationen enthalten sein werden.

24.3 Zusammenarbeit mit anderen Datenschutzinstitutionen

Die bewährte Abstimmung mit den Datenschutzbeauftragten der anderen Länder und dem des Bundes erfolgte wiederum in Arbeitskreisen und den beiden jährlichen Gesamtkonferenzen. Der LfD hat die Entschließungen, an deren Zustandekommen er regelmäßig beteiligt war, in der Anlage abgedruckt. Aus der großen Zahl der gemeinsamen Standpunkte wird deutlich, dass trotz gelegentlicher Unterschiede in der Betonung von datenschutzrechtlichen Aspekten ein großer Vorrat an Gemeinsamkeiten besteht. Der LfD hofft, dass dies auch künftig so bleibt, denn die Erfolgschancen in der Sache sind umso größer, je geschlossener die Institutionen auftreten, die die Wahrung des Datenschutzes als Auftrag zu erfüllen haben. Wie in den Vorjahren bestand ein besonders enger Kontakt zum hessischen Datenschutzbeauftragten und seinen Mitarbeiterinnen und Mitarbeitern.

Die Kommission beim LfD hat im Berichtszeitraum wiederum ihre gesetzliche Aufgabe, den LfD bei der Wahrnehmung seiner Aufgaben zu unterstützen und den Tätigkeitsbericht vorzubereiten, engagiert wahrgenommen. Der LfD dankt an dieser Stelle erneut den Mitgliedern der Kommission für ihre Arbeit und gibt der Hoffnung Ausdruck, dass die datenschutzrechtlichen Anliegen auch künftig auf das Interesse und die Unterstützung des Landtags stoßen.

24.4 Resümee und Ausblick

In letzter Zeit hat sich der Schwerpunkt der Bedrohung des Datenschutzes auf die Auswirkungen der „Informationsgesellschaft“ verlagert; Begriffe wie „Multimedia“, „Data-Warehouses“, Unkontrollierbarkeit des Internets, Chipkartentechnik, Zusammenwachsen von Medien, Kommunikation und Computertechnologie spielen hier die wichtigste Rolle. Es wird von der Unmöglichkeit des Datenschutzes oder zumindest von der Notwendigkeit eines Paradigmenwechsels, einer grundsätzlichen Neuorientierung datenschutzrechtlicher Grundstrukturen, gesprochen. Es werden grundsätzlich zwei unterschiedliche neue Bedrohungsszenarien für realistisch gehalten:

Einmal die Entwicklung, dass durch Privatisierung und Ausweitung der informationsgesellschaftlichen Möglichkeiten und der Kommunikationstechnologie viele private Stellen sensibelste Bürgerdaten speichern und eine unangemessene Macht erhalten mit der Folge, dass nur noch zahlungskräftige Mitbürger an wesentlichen Errungenschaften der Zivilisation teilhaben können. Eine andere Zukunftsvision ist die alte, aber immer noch aktuelle vom „Großen Bruder“ Staat, wobei dem Einsatz fortgeschrittener multimedialer Informations- und Kommunikationstechnologie durch die Behörden eine besondere Bedeutung zugemessen wird. Dabei spielt besonders die Zusammenschaltbarkeit und der intensive Einsatz von Techniken zur zentralen Auswertung unterschiedlicher Datenbanken mittels Data-Ware -Housing- und Data-Mining-Technologien eine wesentliche Rolle. Die europäische Zentralisierung durch Einführung einer gemeinsamen Währung, der Ausbau der sog. „Dritten Säule“ in Europa nach dem Vertrag von Amsterdam (also der Ausbau der Zusammenarbeit im Bereich Justiz und Innere Sicherheit innerhalb der EU) verstärken diese Tendenzen (Stichwort Europol). Hinzu kommt die Möglichkeit der Europäischen Union, auch auf diesen Gebieten durch Verordnungen und Richtlinien den nationalen Gesetzgeber zu binden.

Abwegig sind beide Vorstellungen nicht. Zu berücksichtigen ist auch, dass das Internet insbesondere in Bezug auf die Aktivitäten privater Anbieter nur sehr schwer kontrollierbar ist: Grenzüberschreitende Kontrollen durch Datenschutzbeauftragte oder Strafverfolgungsbehörden sind nur schwer realisierbar. Die Datenmacht privater Datenverarbeiter gerät grundsätzlich zu Recht verstärkt ins Blickfeld besorgter Bürger und auch der Datenschützer.

Dennoch kann den Gefahren aus der Sicht des LfD jedenfalls grundsätzlich mit den bewährten Mitteln des Datenschutzes weitgehend entgegengewirkt werden. Dabei sind Modernisierungen und Anpassungen des Rechts sicher notwendig: Betonung des Prinzips der Datenvermeidung auch bei geschäftlichen, privatrechtlichen Aktivitäten, Erweiterung der Information und der Einflussmöglichkeiten des Einzelnen (Stichwort „Selbstdatenschutz“), „Datenschutz-Audit“ und Technikfolgenabschätzung sind Gesichtspunkte, über deren gesetzliche Verstärkung bzw. Verankerung nachzudenken ist. Auch eine auf bestimmte Bereiche zielende gesetzliche Betonung des staatlichen Schutzes vor dem Machtmissbrauch Privater, die ihren Einfluss mit Hilfe von Datensammlungen unangemessen steigern könnten, ist geboten und im besonders bedeutsamen Medienbereich erfolgt (Mediendienste-Staatsvertrag, Teledienstegesetz, Teledienstedatenschutzgesetz). Dies alles führt aber keinesfalls zu einer grundsätzlichen Veränderung des Datenschutzrechts. Soweit eine solche diskutiert wird (Stichworte „Datenverkehrsordnung“ und „Informationsgesetzbuch“), könnte dies gefährliche Auswirkungen haben: Dies könnte zu einer Verwässerung des freiheitssichernden Grundanliegens des Datenschutzes und damit zu einer Verschlechterung der Position des Einzelnen führen.

Gegenüber dem Staat hat der Einzelne Abwehrrechte, die relativ eindeutig sind. Wenn man die Datenspeicherung als Eingriff versteht, ist der Staat begründungspflichtig, warum er diese Daten speichern will. Wenn der Einzelne aber als Teil eines sozialen und informationellen Geflechts verstanden wird, in dem er Informationen gleichermaßen erhält und preiszugeben hat, wird seine Abwehrposition gegen staatliche Datenspeicherungen insoweit unklar und tendenziell aufgehoben.

In Richtung auf eine Unterstützung des Datenschutzes weist auch folgende Erfahrung: Die Privatwirtschaft ist ihrerseits durchaus kooperativ und sieht ein, dass Datenschutz für die Akzeptanz von Produkten der Informations- und Kommunikationstechnik und Dienstleistungen durch die Gesellschaft und den Verbraucher eine wichtige Rolle spielt. Insbesondere bei elektronischen Dienstleistungen im Internet ist dies zurzeit aktuell. Das Prinzip der Datenvermeidung kann zum ökonomischen Erfolg bestimmter Produkte beitragen. Es gibt inzwischen eine Reihe von Beispielen dafür, dass mangelhafter Datenschutz dazu führt, dass Produkte auf dem Markt keinen Erfolg haben.
Auch die Befürchtung, dass Informationszugänge verstopft werden und nur noch zahlungskräftige Bürger angemessene Informationen erhalten können, ist derzeit wenig realistisch; die aussagekräftigsten und zuverlässigsten Informationsangebote, die derzeit im Internet angeboten werden, sind häufig diejenigen von öffentlichen Stellen, die sich im Internet präsentieren und die dies als einen wesentlichen Teil ihrer gesetzlichen Aufgabenerfüllung ansehen.

Ein weiterer wesentlicher Gesichtspunkt kommt hinzu: Die rechtlichen Regelungen und die Marktmechanismen werden ergänzt durch eine neue Kategorie von Technologie, der sog. datenschutzfreundlichen Technologie. Hierzu gehören beispielsweise blinde digitale Signaturen, verschlüsselte biometrische Daten, digitale Pseudonyme. Der Schlüsselbegriff hierfür ist PET, privacy enhancing technologies. Diese Technologie soll dazu beitragen, dass auch bei der Nutzung elektronischer Zahlungs-, Dienstleistungs- und Informationssysteme dem Konsumenten die vertraute und übliche Anonymität erhalten bleibt.

Letztlich bleibt natürlich der Blick in die Zukunft ungewiss: Was die Informationsgesellschaft tatsächlich für Folgen haben wird, kann im Moment niemand exakt vorhersagen. Allerdings lassen die Erfahrungen aus der Vergangenheit, wie sie auch in diesem Tätigkeitsbericht ihren Niederschlag gefunden haben, den Schluss zu, dass der Schutz der Privatsphäre für die Gesellschaft eine wichtige Rolle spielt und dass dies auch von den Entscheidungsträgern in Staat und Gesellschaft erkannt und anerkannt wird. Aus der Sicht des LfD ist deshalb auch unter den neuen Bedingungen der Informationsgesellschaft ein gewisser Optimismus gerechtfertigt, der allerdings von misstrauischer Wachsamkeit begleitet bleiben muss. Ein grundlegend neuer Datenschutz mit gänzlich neuen Regelungsansätzen aber ist verfehlt und tendenziell unter dem Aspekt des Individualrechtsschutzes eher gefährlich.

Anlage 1

Entschließung
der 54. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
vom 23./24. Oktober 1997
Novellierung des Bundesdatenschutzgesetzes und Modernisierung des Datenschutzrechts

Die fristgerechte Harmonisierung des Datenschutzes entsprechend den Vorgaben der europäischen Datenschutzrichtlinie vom 24. Oktober 1995 droht zu scheitern. Die von dieser Richtlinie gesetzte Dreijahresfrist wird heute in einem Jahr ablaufen. Eine gründliche Beratung im Deutschen Bundestag wird durch den baldigen Ablauf der Legislaturperiode in Frage gestellt.

Noch immer gibt es keinen Kabinettsbeschluss; die Bundesregierung hat bisher noch nicht einmal einen abgestimmten Referentenentwurf vorgelegt. Sie gefährdet dadurch die rechtzeitige Umsetzung der Richtlinie und riskiert ein Vertragsverletzungsverfahren vor dem Europäischen Gerichtshof.

Für die Entwicklung des Datenschutzes ist diese Lage höchst nachteilig:

- Verbesserungen des Datenschutzes der Bürger, z. B. durch genauere Information über die Verarbeitung ihrer Daten, verzögern sich;
- dem Datenschutzrecht droht Zersplitterung, weil den Ländern eine Orientierung für die Anpassung der Landesdatenschutzgesetze fehlt.

Die Datenschutzbeauftragten des Bundes und der Länder appellieren daher an die Bundesregierung, für eine fristgerechte Umsetzung der Richtlinie Sorge zu tragen.

Zur Harmonisierung des europäischen Datenschutzrechts empfehlen die Datenschutzbeauftragten der Bundesregierung und dem Gesetzgeber folgende Grundsatzentscheidungen:

- weitgehende Gleichbehandlung des öffentlichen und des privaten Bereichs bei gleichzeitiger Verbesserung der Datenschutzkontrolle, insbesondere durch generell anlassunabhängige Kontrolle und durch die ausdrückliche Festlegung der völligen Unabhängigkeit der Aufsichtsbehörden und die Erweiterung ihrer Eingriffsbefugnisse;
- Bestellung weisungsfreier Datenschutzbeauftragter auch bei öffentlichen Stellen mit dem Recht, sich jederzeit an den Bundes- oder Landesbeauftragten für den Datenschutz zu wenden;
- Bürgerfreundlichkeit durch einfache und verständliche Formulierung des BDSG, z. B. durch einen einheitlichen Begriff der Verarbeitung personenbezogener Daten entsprechend der Richtlinie;
- Gewährleistung eines einheitlichen, hohen Datenschutzniveaus durch Beibehaltung der Funktion des BDSG und der Landesdatenschutzgesetze als Querschnittsgesetze sowie durch Vermeidung eines Gefälles zwischen den Bereichen, die der EG-Datenschutzrichtlinie unterfallen, und den übrigen Gebieten, deren Datenschutzregelungen nicht verschlechtert werden dürfen;
- Sonderregelungen für Presse und Rundfunk nur, soweit zur Sicherung der Meinungsfreiheit notwendig.

Als ebenso vordringlich betrachten die Datenschutzbeauftragten eine Anpassung der noch von der Großrechnertechnologie der siebziger Jahre bestimmten gesetzlichen Regelungen an die heutige Informationstechnologie und an die Verhältnisse der modernen Informationsgesellschaft. Dazu gehören insbesondere folgende Punkte:

- verbindliche Grundsätze für die datenschutzfreundliche Gestaltung von Informationssystemen und -techniken, so zur Datensparsamkeit, zur Anonymisierung und Pseudonymisierung, zur Verschlüsselung und zur Risikoanalyse;
- mehr Transparenz für die Verbraucher und mehr Eigenständigkeit für die Anbieter durch Einführung eines Datenschutz-Audits;
- Erweiterung des Schutzbereichs bei Bild- und Tonaufzeichnungen, Regelung der Video-Überwachung;
- Sonderregelungen für besonders empfindliche Bereiche, wie den Umgang mit Arbeitnehmerdaten, Gesundheitsdaten und Informationen aus gerichtlichen Verfahren;
- Einführung einer Vorabkontrolle für besonders risikoreiche Datenverarbeitung, namentlich bei Verarbeitung sensitiver Daten;
- Regelungen für Chipkarten-Anwendungen;

- Verstärkung des Schutzes gegenüber Adressenhandel und Direktmarketing, unter anderem auch mindestens durch die Festlegung von Hinweispflichten hinsichtlich der Möglichkeit des Widerspruchs; vorzuziehen ist in jedem Fall eine Einwilligungsregelung;
- Verstärkung des Schutzes gegenüber der Einholung von Selbstauskünften vor Abschluss von Miet-, Arbeits- und ähnlich existenzwichtigen Verträgen;
- Datenexport nach Inlandsgrundsätzen nur bei angemessenem Schutzniveau im Empfängerstaat; Festlegung, unter welchen Voraussetzungen ein Mitgliedstaat Daten, die dieser im Anwendungsbereich der Richtlinie (also nach Inlandsgrundsätzen) erhalten hat, außerhalb ihres Anwendungsbereichs verwenden darf;
- möglichst weit gehende Ersetzung der Anmeldung von Dateien bei der Aufsichtsbehörde durch Bestellung weisungsfreier Datenschutzbeauftragter; Beibehaltung des internen Datenschutzbeauftragten auch bei Sicherheitsbehörden;
- Stärkung der Kontrollrechte des Bundesbeauftragten und der Landesbeauftragten für den Datenschutz durch uneingeschränkte Kontrollbefugnis bei der Verarbeitung personenbezogener Daten in Akten einschließlich solcher über Sicherheitsüberprüfungen.

Die Konferenz weist ferner auf die Rechtspflicht der Länder hin, ihr Datenschutzrecht ebenfalls der EG-Richtlinie fristgerecht anzupassen.

Anlage 2

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) in einem umfassenderen Bedeutungs- und Funktionszusammenhang 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 Überlegungen, 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 und der Länder fordern wirksame Vorkehrungen zum Schutz des Persönlichkeitsrechts bei Verwendung von Bild-Ton-Aufzeichnungen im Strafverfahren. Unabhängig von der Frage, welche Zielsetzung 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 Verfahrensbeteiligte zulässt, müssen jedenfalls wirksame Vorkehrungen gegen Missbrauch gewährleistet sein, z. B. sichtbare Signierung und strafbewehrte Regelungen über Zweckbindungen und Löschungsfristen.

4. Eine Verwertung der Aufzeichnungen 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 Aufzeichnungen zulässt, müssen Voraussetzungen, Umfang und Fristen der weiteren Aufbewahrung klar und eng geregelt werden.

Anlage 3

E n t s c h l i e ß u n g
der 54. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
vom 23./24. Oktober 1997
Erforderlichkeit datenschutzfreundlicher Technologien

Moderne Informations- und Telekommunikationstechnik (IuK-Technik) gewinnt in allen Lebensbereichen zunehmende Bedeutung. Die Nutzer wenden diese Technik z. B. in Computernetzen, Chipkartensystemen oder elektronischen Medien in vielfältiger Weise an und hinterlassen dabei zumeist umfangreiche elektronische Spuren. Dabei fällt in der Regel eine Fülle von Einzeldaten an, die geeignet sind, persönliche Verhaltensprofile zu bilden.

Den Erfordernissen des Datenschutzes wird nicht in ausreichendem Maße Rechnung getragen, wenn sich der Schutz der Privatheit des Einzelnen lediglich auf eine Beschränkung des Zugangs zu bereits erhobenen, gespeicherten und verarbeiteten personenbezogenen Daten reduziert. Daher ist es erforderlich, bereits vor der Erhebung und Speicherung die zu speichernde Datenmenge wesentlich zu reduzieren.

Datensparsamkeit bis hin zur Datenvermeidung, z. B. durch Nutzung von Anonymisierung und Pseudonymisierung personenbezogener Daten, spielen in den unterschiedlichen Anwendungsbereichen der IuK-Technik, wie elektronischen Zahlungsverfahren, Gesundheits- oder Verkehrswesen, bisher noch eine untergeordnete Rolle. Eine datenschutzfreundliche Technologie lässt sich aber nur dann wirksam realisieren, wenn das Bemühen um Datensparsamkeit die Entwicklung und den Betrieb von IuK-Systemen ebenso stark beeinflusst wie die Forderung nach Datensicherheit.

Die Datenschutzbeauftragten des Bundes und der Länder wollen in Zusammenarbeit mit Herstellern und Anbietern auf datenschutzgerechte Lösungen hinarbeiten. Die dafür erforderlichen Techniken stehen weitgehend schon zur Verfügung. Moderne kryptographische Verfahren zur Verschlüsselung und Signatur ermöglichen die Anonymisierung oder Pseudonymisierung in vielen Fällen, ohne dass die Verbindlichkeit und Ordnungsmäßigkeit der Datenverarbeitung beeinträchtigt werden. Diese Möglichkeiten der modernen Datenschutztechnologie, die mit dem Begriff „Privacy enhancing technology (PET)“ eine Philosophie der Datensparsamkeit beschreibt und ein ganzes System technischer Maßnahmen umfasst, sollten genutzt werden.

Vom Gesetzgeber erwarten die Datenschutzbeauftragten des Bundes und der Länder, dass er die Verwendung datenschutzfreundlicher Technologien durch Schaffung rechtlicher Rahmenbedingungen forciert. Sie begrüßen, dass sowohl der Mediendienste-Staatsvertrag der Länder als auch das Teledienstedatenschutzgesetz des Bundes bereits den Grundsatz der Datenvermeidung normieren. Der in den Datenschutzgesetzen des Bundes und der Länder festgeschriebene Grundsatz der Erforderlichkeit lässt sich in Zukunft insbesondere durch Berücksichtigung des Prinzips der Datensparsamkeit und der Verpflichtung zur Bereitstellung anonymer Nutzungsformen verwirklichen. Die Datenschutzbeauftragten des Bundes und der Länder bitten darüber hinaus die Bundesregierung, sich im europäischen Bereich dafür einzusetzen, dass die Förderung datenschutzfreundlicher Technologien entsprechend dem Vorschlag der Kommission in das 5. Rahmenprogramm „Forschung und Entwicklung“ aufgenommen wird.

Neben Anbietern von Tele- und Mediendiensten sollten auch die Hersteller und Anbieter von IuK-Technik bei der Ausgestaltung und Auswahl technischer Einrichtungen dafür gewonnen werden, sich am Grundsatz der Datenvermeidung zu orientieren und auf eine konsequente Minimierung gespeicherter personenbezogener Daten achten.

Anlage 4

Entschließung
der 55. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
vom 19./20. März 1998
Datenschutz beim digitalen Fernsehen

Die Datenschutzbeauftragten des Bundes und der Länder machen darauf aufmerksam, dass bei elektronischen Diensten immer umfangreichere Datenspuren über das Verhalten der Einzelnen entstehen. Mit der Digitalisierung der Fernseh- und Hörfunkübertragung entsteht die technische Infrastruktur dafür, dass erstmals auch das individuelle Mediennutzungsverhalten registriert werden kann. Sie bekräftigen deshalb ihre Forderung, dass auch bei der Vermittlung und Abrechnung digitaler Fernsehsendungen eine flächendeckende Registrierung des individuellen Fernsehkonsums vermieden wird. Im digitalen Fernsehen („Free-TV“ und „Pay-TV“) muss die unbeobachtete Nutzung des Mediums ohne Nachteile möglich bleiben.

Die Datenschutzbeauftragten begrüßen es deshalb, dass die Staats- und Senatskanzleien Vorschläge für die Änderung des Rundfunkstaatsvertrages vorgelegt haben, mit denen Belangen des Datenschutzes Rechnung getragen werden soll. Besonders hervorzuheben sind folgende Punkte:

– Die Gestaltung technischer Einrichtungen muss sich an dem Ziel ausrichten, dass so wenige personenbezogene Daten wie möglich erhoben, verarbeitet und genutzt werden;

– die Rundfunkveranstalter müssen die Nutzung und Bezahlung von Rundfunkangeboten anonym oder unter Pseudonym ermöglichen, soweit dies technisch möglich und zumutbar ist;

– personenbezogene Daten über die Inanspruchnahme einzelner Sendungen dürfen für Abrechnungszwecke nur gespeichert werden, wenn ein Einzelnachweis verlangt wird;

– wie bereits im Mediendienste-Staatsvertrag enthält auch der Entwurf des Rundfunkstaatsvertrags eine Vorschrift zum Datenschutz-Audit, d. h. Veranstalter können ihr Datenschutzkonzept und ihre technischen Einrichtungen von unabhängigen Gutachtern prüfen und das Prüfungsergebnis veröffentlichen lassen.

Die Datenschutzbeauftragten halten diese Grundsätze für geeignet, eine datenschutzgerechte Nutzung digitaler Fernsehangebote zu ermöglichen. Die technischen Möglichkeiten, diesen datenschutzrechtlichen Vorgaben zu entsprechen, sind gegeben. Die Datenschutzbeauftragten konnten sich bereits 1996 hiervon praktisch überzeugen. Die Systementscheidung von Veranstaltern für einen Decodertyp, der möglicherweise weniger geeignet ist, die Datenschutzanforderungen zu erfüllen, kann kein Maßstab für die Angemessenheit dieser Anforderungen sein, wenn zugleich andere Geräte ihnen ohne Probleme genügen.

Der Forderung von Inhabern von Verwertungsrechten, einen Nachweis über die Inanspruchnahme von Pay-per-View-Angeboten vorzulegen, kann ohne Personenbezug – etwa durch zertifizierte Zähleinrichtungen oder den Einsatz von Pseudonymen – entsprochen werden.

Die Datenschutzbeauftragten bitten deshalb die Ministerpräsidentin und die Ministerpräsidenten der Länder, an den datenschutzrechtlichen Regelungen des Entwurfs festzuhalten. Damit würden das bisherige Datenschutzniveau für die Fernsehnutzung im digitalen Zeitalter abgesichert und zugleich die Vorschriften für den Bereich des Rundfunks und der Mediendienste harmonisiert.

Die Datenschutzbeauftragten fordern die Rundfunkveranstalter und Hersteller auf, den Datenschutz bei der Gestaltung von digitalen Angeboten schon jetzt zu berücksichtigen.

Anlage 5

E n t s c h l i e ß u n g
der 55. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
vom 19./20. März 1998
Datenschutzprobleme der Geldkarte

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder wiederholt ihre Forderung aus ihrer Entschließung vom 13. Oktober 1995 nach einem anonymen elektronischen Zahlungsverfahren bei elektronischen Geldbörsen. Dies gilt insbesondere für die Geldkarte des deutschen Kreditwesens, bei der in kartenbezogenen „Schattenkonten“ der Evidenzzentralen nicht nur der Kaufbetrag und ein identifizierbarer Händlerschlüssel, sondern auch der Kaufzeitpunkt gespeichert werden. Mit diesen Daten können sämtliche mit der Geldkarte getätigten Kaufvorgänge jahrelang nachvollzogen werden, wenn die Daten mit den persönlichen Kundendaten zusammengeführt werden. Diese Geldkarte erfüllt nicht die Forderungen der Datenschutzbeauftragten.

Außerdem werden die Kundinnen und Kunden über diese „Schattenkonten“ noch nicht einmal informiert. Die Herausgeber solcher Karten bzw. die Kreditinstitute haben aber die Pflicht, ihre Kundinnen und Kunden über Art und Umfang der im Hintergrund laufenden Verarbeitungsvorgänge zu informieren.

Unabhängig davon müssen bei der Geldkarte des deutschen Kreditwesens sämtliche Umsatzdaten in den Evidenzzentralen und auch bei den Händlern nach Abschluss der Verrechnung (Clearing) gelöscht oder zumindest anonymisiert werden.

Die Datenschutzbeauftragten fordern die Kartenherausgeber und die Kreditwirtschaft erneut dazu auf, vorzugsweise kartengestützte Zahlungssysteme ohne personenbezogene Daten – sog. White Cards – anzubieten. Die Anwendung ist so zu gestalten, dass ein karten- und damit personenbezogenes Clearing nicht erfolgt.

Der Gesetzgeber bleibt aufgerufen sicherzustellen, dass auch in Zukunft die Möglichkeit besteht, im wirtschaftlichen Leben im gleichen Umfang wie bisher bei Bargeldzahlung anonym zu bleiben.

Anlage 6

Entschließung
der 56. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 5./6. Oktober 1998
Fehlende bereichsspezifische Regelungen bei der Justiz

Derzeit werden in allen Bereichen der Justiz bei Staatsanwaltschaften, Gerichten und Gerichtsvollziehern im Zuge von Modernisierungsvorhaben umfassende Systeme der automatisierten Datenverarbeitung eingeführt mit der Folge, dass sensible personenbezogene Daten auch hier in viel stärkerem Maße verfügbar werden als bisher. Sogar die Beauftragung Privater mit der Verarbeitung sensibler Justizdaten wird erwogen. Gerade vor dem Hintergrund dieser vollkommen neuen Qualität der Datenverarbeitung in der Justiz wird deutlich, dass die Rechtsprechung des Bundesverfassungsgerichts zum so genannten Übergangsbonus hier keine tragfähige Grundlage für Eingriffe in die informationelle Selbstbestimmung mehr darstellen kann. Vielmehr müssen die Entscheidungen des Gesetzgebers den Maßstab für die weitere technische Ausgestaltung der Datenverarbeitung innerhalb der Justiz bilden und nicht umgekehrt. Dabei ist nicht nur für formell ausreichende Rechtsgrundlagen Sorge zu tragen. Auch Fragen der Datensicherheit und der Ordnungsmäßigkeit der Datenverarbeitung bedürfen der Regelung.

Seit dem Volkszählungsurteil des Bundesverfassungsgerichts sind 15 Jahre vergangen. Dennoch werden ausgerechnet im Bereich der Justiz sensible personenbezogene Daten nach wie vor ohne die vom Bundesverfassungsgericht geforderten bereichsspezifischen gesetzlichen Grundlagen erhoben und verarbeitet.

Die Datenschutzbeauftragten des Bundes und der Länder bekräftigen deshalb im Anschluss an ihren Beschluss der 48. Konferenz vom 26./27. September 1994 in Potsdam ihre wiederholten Forderungen zu bereichsspezifischen Regelungen bei der Justiz.

Zwar hat der Gesetzgeber in der abgelaufenen Legislaturperiode zumindest Regelungen über Datenerhebung, -verarbeitung und -nutzung im Strafvollzug sowie über die Datenübermittlung von Amts wegen durch Gerichte und Staatsanwaltschaften an Gerichte, Behörden und sonstige öffentlichen Stellen geschaffen.

Trotzdem sind in wichtigen Bereichen gesetzliche Regelungen weiterhin überfällig. Ausreichende gesetzliche Regelungen fehlen vor allem für

- weite Bereiche der Datenverarbeitung im Strafverfahren, insbesondere in automatisierten Dateien namentlich die
  - Übermittlung von Strafverfahrensdaten an nicht am Strafverfahren beteiligte dritte Stellen;
  - Rechte der Betroffenen (nicht nur der Beschuldigten, sondern auch von Zeugen und sonstigen Personen, deren Daten gespeichert werden) in Bezug auf Daten, die im Zusammenhang mit einem Strafverfahren gespeichert werden.
- Aufbewahrung von Akten, Karteien und sonstigen Unterlagen sowie die Dauer der Speicherung in automatisierten Dateien;
  - Datenübermittlung zu wissenschaftlichen Zwecken;
  - Datenverarbeitung in der Zwangsvollstreckung;
  - Datenverarbeitung im Jugendstrafvollzug;
  - Datenverarbeitung im Vollzug der Untersuchungshaft.

Der Gesetzgeber sollte daher in der kommenden Legislaturperiode zügig die notwendigen Novellierungen, für die zum Teil ja schon erhebliche Vorarbeiten geleistet worden sind, aufgreifen. Dabei ist nicht die jeweils geübte Praxis zu legalisieren, sondern es muss vorab unter datenschutzrechtlichen Gesichtspunkten geprüft werden, welche Form der Datenerhebung und -verarbeitung in welchem Umfang erforderlich ist. Ferner hat der Gesetzgeber jeweils bereichsspezifisch zu prüfen, inwieweit Aufgaben der Justiz und damit verbundene Datenverarbeitungen Privaten übertragen werden dürfen.

Der Entwurf für ein „StVÄG 1996“ erfüllt diese Voraussetzungen nicht, im Gegenteil fällt er teilweise hinter den bereits erreichten Standard der allgemeinen Datenschutzgesetze und anderer bereichsspezifischer Regelungen (wie z. B. dem Bundeszentralregistergesetz und den Polizeigesetzen der Länder) zurück. Zu kritisieren sind vor allem:

- Mangelnde Bestimmtheit der Voraussetzungen für Maßnahmen der Öffentlichkeitsfahndung.
- Unangemessen weite Auskunfts- und Akteneinsichtsmöglichkeiten für nicht Verfahrensbeteiligte.
- Unzureichende Regelungen über Inhalt, Ausmaß und Umfang von staatsanwaltlichen Dateien und Informationssystemen.

Die Datenschutzbeauftragten halten es deshalb zum Schutz des Rechts des Einzelnen auf informationelle Selbstbestimmung für geboten, wegen der mit der Datenerhebung, Verarbeitung und Nutzung verbundenen Rechtseingriffe unverzüglich in der neuen Legislaturperiode bereichsspezifische Regelungen der materiellen Voraussetzungen sowie der organisatorischen und verfahrensrechtlichen Vorkehrungen zu schaffen, welche der Gefahr einer Verletzung des Persönlichkeitsrechtes der Bürgerinnen und Bürger entgegenwirken.

Anlage 7

Entschließung
der Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 5./6. Oktober 1998
Dringlichkeit der Datenschutzmodernisierung

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt und unterstützt grundsätzlich die vom 62. Deutschen Juristentag (DJT) im September 1998 in Bremen gefassten Beschlüsse zum Umgang mit Informationen einschließlich personenbezogener Daten. Von den gesetzgebenden Körperschaften erhofft sich die Konferenz die Berücksichtigung dieser Beschlüsse bei der nunmehr dringend erforderlichen Umsetzung der EG-Datenschutzrichtlinie in Bundes- und Landesrecht.

Insbesondere betont die Konferenz folgende Punkte:

- Die materiellen Anforderungen des Datenschutzrechts sind angesichts der wachsenden Datenmacht in privater Hand auf hohem Niveau grundsätzlich einheitlich für den öffentlichen wie für den privaten Bereich zu gestalten.
- Die anlassfreie Aufsicht für die Einhaltung des Datenschutzes im privaten Bereich muss in gleicher Weise unabhängig und weisungsfrei ausgestaltet werden wie die Datenschutzkontrolle bei öffentlichen Stellen.
- Die Rechte der Bürgerinnen und Bürger sind zu stärken; als Voraussetzung für die Ausübung des Rechts auf informationelle Selbstbestimmung der Betroffenen sind die Verpflichtungen zu ihrer Information, Aufklärung und ihren Wahlmöglichkeiten ohne faktische Zwänge auszuweiten.
- Ein modernisiertes Datenschutzrecht hat die Grundsätze der Datenvermeidung, des Datenschutzes durch Technik, der Zweckbindung der Daten und ihres Verwendungszusammenhangs in den Mittelpunkt zu stellen.

Zur Sicherstellung vertraulicher und unverfälschter elektronischer Kommunikation ist die staatliche Förderung von Verschlüsselungsverfahren geboten, nicht eine Reglementierung der Kryptographie.

Anlage 8

Entschließung
der Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 5./6. Oktober 1998
Entwicklungen im Sicherheitsbereich

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder stellt fest, dass die Sicherheitsbehörden in den vergangenen Jahren umfangreiche zusätzliche Eingriffsbefugnisse erhalten haben. Demgegenüber fehlen in weiten Teilen Erkenntnisse über die Wirksamkeit und Grundrechtsverträglichkeit der Anwendung dieser Instrumente, wie z. B. bei der Schleppnetzfahndung und der Ausweitung der Telefonüberwachung.

Die Datenschutzbeauftragten des Bundes und der Länder erwarten vom Bundesgesetzgeber und der Bundesregierung, dass die Erforderlichkeit und die Wirksamkeit aller Eingriffsbefugnisse anhand objektiver Kriterien überprüft werden (Evaluierung).

Anlage 9

Entschließung
der 56. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 5./6. Oktober 1998
Weitergabe von Meldedaten an Adressbuchverlage und Parteien

Bei den Datenschutzbeauftragten des Bundes und der Länder gehen viele Beschwerden ein, in denen deutlicher Unmut über veröffentlichte Daten in Adressbüchern und unverlangt erhaltene Werbesendungen geäußert wird. Vor Wahlen nehmen die Beschwerden noch zu. Überrascht stellten Betroffene fest, dass sie persönlich adressierte Wahlwerbung der Parteien bekommmen. Ihnen ist unerklärlich, wie Adressbuchverlage und Parteien an ihre Adressen gekommen sind. Sie erhalten auf Anforderung Daten aus den kommunalen Melderegistern. Damit sind die Adressbuchverlage und Parteien gegenüber anderen gesellschaftlichen Gruppen privilegiert.

Dieser Umgang mit Meldedaten ist weder transparent noch angemessen. Die Konferenz tritt dafür ein, die Rechte der Bürgerinnen und Bürger zu verbessern. Die Information über die Widerspruchsmöglichkeit erreicht die Menschen häufig nicht. Vorzuziehen ist deshalb eine Einwilligungslösung. Sie würde das Grundrecht auf informationelle Selbstbestimmung konsequent umsetzen – erst fragen, dann handeln. Nach der Einwilligungslösung ist eine Erklärung informierter Bürgerinnen und Bürger gegenüber dem Meldeamt nötig, ob sie mit den Datenweitergaben an die genannten Empfänger einverstanden sind oder nicht.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder empfiehlt den gesetzgebenden Körperschaften, künftig die Einwilligungslösung vorzusehen.

Anlage 10

Entschließung
der 56. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
vom 5./6. Oktober 1998
Prüfungskompetenz der Datenschutzbeauftragten bei den Gerichten

Die Datenschutzbeauftragten des Bundes und der Länder stellen fest, dass in der Praxis die Abgrenzung ihrer Zuständigkeiten bei den Gerichten immer wieder Anlass von Unsicherheiten ist. Sie weisen daher darauf hin, dass die Beschränkung der Prüfkompetenz bei den Gerichten einzig und allein den Zweck hat, den grundgesetzlich besonders geschützten Bereich der richterlichen Unabhängigkeit von Kontrollen freizuhalten.

Deshalb erstreckt sich die Kontrolle der Datenschutzbeauftragten bei den Gerichten u. a. auch darauf, ob die erforderlichen technischen und organisatorischen Maßnahmen zur Datensicherung getroffen und eingehalten werden, insbesondere bei automatisierter Datenverarbeitung.

Die Datenschutzbeauftragten des Bundes und der Länder halten eine gesetzliche Klarstellung für hilfreich, dass Gerichte der Kontrolle des Bundesbeauftragten bzw. der Landesbeauftragten für den Datenschutz unterliegen, soweit sie nicht in richterlicher Unabhängigkeit tätig werden.

Anlage 11

Entschließung
der 56. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder am 5./.6. Oktober 1998
Verweigerung der Auskunft durch das Bundesamt für Finanzen
auf Anfragen Betroffener über ihre Freistellungsaufträge

Die Datenschutzbeauftragten des Bundes und der Länder betonen das Recht der Bürgerinnen und Bürger auf Auskunft über ihre Daten auch gegenüber der Finanzverwaltung (§ 19 BDSG). Die Betroffenen haben Anspruch, von dem Bundesamt für Finanzen Auskunft über die Freistellungsaufträge zu erhalten, die sie ihrer Bank im Zusammenhang mit dem steuerlichen Abzug von Zinsen erteilt haben.

Der Bundesbeauftragte für den Datenschutz hat die Verweigerung der Auskünfte gegenüber dem Bundesministerium der Finanzen beanstandet und dieses aufgefordert, den entsprechenden Erlass an das Bundesamt aufzuheben. Bisher hat das Ministerium in der Sache allerdings nicht eingelenkt.

Für die Betroffenen ergibt sich hierdurch ein unhaltbarer Zustand. Ihnen wird die Auskunft zu Unrecht vorenthalten.

Die Datenschutzbeauftragten der Länder unterstützen mit Nachdruck die Forderung des Bundesbeauftragten für den Datenschutz gegenüber dem Bundesministerium der Finanzen, seinen Erlass an das Bundesamt für Finanzen aufzuheben und dieses anzuweisen, dem Auskunftsanspruch der Auftraggeber von Freistellungsaufträgen nachzukommen.

Anlage 12

Entschließung
der 57. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder vom 25./26. März 1999
Modernisierung des Datenschutzes – umfassende Novellierung des BDSG nicht aufschieben

Die deutschen Datenschutzbeauftragten haben bereits früh gefordert, die Novellierung des BDSG zur Umsetzung der EG-Datenschutzrichtlinie zu einer gründlichen Modernisierung des veralteten deutschen Datenschutzrechts zu nutzen. Da die dreijährige Anpassungsfrist im Oktober 1998 verstrichen ist, besteht jetzt ein erheblicher Zeitdruck. Für die Neuregelung, die derzeit in der Bundesregierung und in Koalitionsgremien vorbereitet wird, ist daher ein „Zwei-Stufen-Konzept“ vorgesehen. Einem ersten, in Kürze vorzulegenden Novellierungsgesetz soll zu einem späteren Zeitpunkt eine zweite Änderung folgen, die weitere Verbesserungen enthalten soll. Die Konferenz geht davon aus, dass das Zweistufenkonzept von dem festen politischen Willen getragen wird, die zweite Stufe nach Einbindung des ersten Gesetzentwurfes zügig in Angriff zu nehmen und noch in dieser Legislaturperiode abzuschließen. Auch der in dieser Stufe bestehende Handlungsbedarf duldet keinen Aufschub.

Die Konferenz begrüßt, dass jetzt mit Hochdruck an der BDSG-Novellierung gearbeitet wird und Verantwortliche in Regierung und Fraktionen zugesagt haben, die erste Stufe der Neuregelung werde sich nicht auf das von der Richtlinie geforderte Minimum beschränken. Sie unterstützt die Vorschläge, Regelungen zur Videoüberwachung, zu Chipkarten und zum Datenschutz-Audit aufzunehmen. Gleiches gilt für die Übernahme der zukunftsweisenden Bestimmungen zur Datenvermeidung sowie zur anonymen bzw. pseudonymen Nutzung von Telediensten aus dem Multimediarecht. Diese sind wichtige und dringend notwendige Regelungen zur Modernisierung des Datenschutzrechts. Die Konferenz drückt daher ihre Erwartung darüber aus, dass diese Vorschriften in der ersten Stufe des Gesetzgebungsverfahrens zügig verabschiedet werden.

Zu den Punkten, die keinen Aufschub dulden, gehört auch die Verbesserung der Voraussetzungen für eine effektive Datenschutzkontrolle. Die völlig unabhängige Gestaltung der Kontrolle im nicht öffentlichen Bereich muss institutionell sichergestellt und durch eine sachgerechte finanzielle und personelle Ausstattung unterstützt werden. Gegenwärtig noch bestehende Einschränkungen der Kontrollkompetenzen im öffentlichen Bereich müssen abgebaut, den Aufsichtsbehörden müssen wirksamere Befugnisse an die Hand gegeben werden.

Zum Schutz der Bürgerinnen und Bürger sind bei massenhaften Datenerhebungen mit unkalkulierbaren Datenverarbeitungsrisiken oder ungeklärter Zweckbestimmung klare materielle Grenzen durch den Gesetzgeber zu ziehen.

Die bereichsspezifischen Gesetze, z. B. die Sicherheitsgesetze, dürfen nicht vom Bundesdatenschutzgesetz mit den dort zu erwartenden substantiellen Fortschritten für die Bürgerinnen und Bürger, wie beispielsweise einem verbesserten Auskunftsrecht, abgekoppelt werden.

Notwendig ist nach Auffassung der Konferenz, dass das Datenschutzrecht auch in Zukunft bürgerfreundlich und gut lesbar formuliert ist. Dies ist eine unverzichtbare Akzeptanzvoraussetzung für den Datenschutz bei Bürgern, Wirtschaft und Verwaltung.

Anlage 13

E n t s c h l i e ß u n g
der 57. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder vom 25./26. März 1999
Entschließung zur geplanten erweiterten Speicherung von Verbindungsdaten in der Telekommunikation

Die Bundesregierung und der Bundesrat werden demnächst über den Erlass der seit längerem überfälligen Rechtsverordnung zum Datenschutz in der Telekommunikation auf Grund des Telekommunikationsgesetzes zu entscheiden haben.

Im Gegensatz zur früheren analogen Vermittlungstechnik erzeugt und verarbeitet das digitalisierte Telekommunikationsnetz (ISDN-Netz) in großem Umfang personenbezogene Verbindungsdaten. Dies zwingt zu begrenzenden, am Grundsatz der Datensparsamkeit orientierten Regelungen, um das Fernmeldegeheimnis und das Grundrecht der Telefonkundinnen und -kunden auf unbeobachtete Kommunikation zu garantieren.

Die bisher geltende Telekommunikationsdienstunternehmen-Datenschutzverordnung von 1996 sieht vor, dass die Verbindungsdaten unter Kürzung der Zielrufnummer regelmäßig bis zu 80 Tagen nach Versendung der Rechnung gespeichert werden dürfen. Über diese Frist hinaus dürfen Verbindungsdaten nur gespeichert bleiben, wenn Streit zwischen dem Telekommunikationsunternehmen und den Kunden über die Richtigkeit der Abrechnung entsteht.

Demgegenüber gibt es Überlegungen für eine neue Telekommunikations-Datenschutzverordnung, dass alle Verbindungsdaten in der Regel selbst bei unbestrittenen oder bezahlten Rechnungen zwei Jahre lang nach Ende der Verbindung gespeichert bleiben können. Da die Speicherungsfrist erst am Ende des Jahres beginnen soll, in dem die Verbindung stattfand, kann dies in Einzelfällen dazu führen, dass die Daten bis zu drei Jahre lang vorgehalten werden.

Hiergegen wenden sich die Datenschutzbeauftragten des Bundes und der Länder mit Entschiedenheit. Sie sehen darin einen unverhältnismäßigen Eingriff in das Grundrecht der Telefonkundinnen und -kunden auf unbeobachtete Kommunikation. Auch das Telekommunikationsgesetz hebt die Grundsätze der Verhältnismäßigkeit und der Zweckbindung ausdrücklich hervor. Personenbezogene Daten, die für Zwecke der Telekommunikation erhoben und verarbeitet werden, dürfen nur so lange gespeichert bleiben, wie es zu diesen Zwecken erforderlich ist. Auch die vom Gesetz geforderte Höchstfrist für die Speicherung von Verbindungsdaten muss sich am Grundsatz der Datensparsamkeit orientieren, solange sich die Kundin und der Kunde nicht ausdrücklich für eine längere Speicherung entscheiden.

Die Dauer einer zivilrechtlichen Verjährungsfrist kann ebenfalls kein rechtfertigender Anlass für eine solche Datenspeicherung sein. Jedenfalls müssen die Daten unverzüglich gelöscht werden, wenn die Rechnung beglichen und unbestritten ist und damit der vertragliche Speicherzweck erledigt ist.

Da eine telekommunikations- oder zivilrechtlich bedingte Notwendigkeit für eine derart lange Speicherfrist der Verbindungsdaten somit nicht ersichtlich ist, würde sie eine unzulässige Datenspeicherung auf Vorrat zu unbestimmten Zwecken darstellen.

Diese Speicherung von Kommunikationsdaten wäre auch nicht mit der Überlegung zu rechtfertigen, dass diese Daten zum Zwecke eventueller künftiger Strafverfolgung benötigt werden könnten. Die mit einer solchen Speicherung verbundene vorsorgliche Überwachung unverdächtiger Bürgerinnen und Bürger wäre unzulässig.

Anlage 14

Entschließung
der 57. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder vom 25./26. März 1999
Transparente Hard- und Software

Die Datenschutzbeauftragten des Bundes und der Länder haben sich wiederholt für die Nutzung datenschutzfreundlicher Technologien eingesetzt. Sie sehen jedoch mit Sorge die Entwicklung im Bereich der Informationstechnik, die zu neuen Industriestandards und Produkten führt, die für die Benutzerinnen und Benutzer kaum durchschaubar und selbst für Fachleute nur noch eingeschränkt revisionsfähig sind.

Beispielsweise sind seit kurzem mit dem Intel Pentium III-Prozessor bestückte PCs auf dem Markt, deren Prozessor bei der Herstellung mit einer eindeutigen Nummer (Processor Serial Number – PSN) versehen wurde. Intel sieht vor, das Auslesen der PSN durch die Nutzerinnen und Nutzer kontrollieren zu lassen. Die mittlerweile bekannt gewordenen Manipulationsmöglichkeiten der dafür erforderlichen Software machen deutlich, dass die Existenz einer solchen eindeutigen Kennung kaum kontrollierbare Nutzungsmöglichkeiten eröffnet, die dem Datenschutz diametral zuwiderlaufen.

Die durch den Intel Pentium III initiierte Debatte um eindeutige Kennungen brachte ans Tageslicht, dass Softwarehersteller Nutzern neuerer Office-Produkte ohne deren Wissen eindeutige Kennungen zuordnen. Diese Kennungen können in Dokumenten versteckt sein und bei der Nutzung des Internets von Softwareherstellern verdeckt abgefragt werden.

Werden Daten der Nutzerinnen und Nutzer übermittelt, ohne dass sie dies bemerken, kann deren missbräuchliche Verwendung die Anonymität der Anwender von Informationstechnik weiter aushöhlen. Den Erfordernissen des Datenschutzes wird aber nur dann ausreichend Rechnung getragen, wenn zum Schutz der Privatheit transparente und von den Nutzerinnen und Nutzern in eigener Verantwortung bedienbare Sicherheitsfunktionen zur Verfügung stehen.

Deshalb erwarten die Datenschutzbeauftragten des Bundes und der Länder von Herstellern von Informations- und Kommunikationstechnik, Hard- und Software so zu entwickeln und herzustellen, dass Anwender und unabhängige Dritte sich jederzeit von der Wirksamkeit von Sicherheitsvorkehrungen überzeugen können.

Den Anwendern moderner Technik empfehlen die Datenschutzbeauftragten, nur solche Produkte einzusetzen, welche auch eine Transparenz der Verfahrensabläufe gewährleisten.

Anlage 15

Entschließung
der 57. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder vom 25./26. März 1999
Entwurf einer Ratsentschließung zur Überwachung der Telekommunikation
(ENFOPOL '98)

Die Konferenz der Datenschutzbeauftragten hält es für inakzeptabel, dass der entsprechende Entwurf bisher geheim gehalten und ohne Einbeziehung der Datenschutzbeauftragten beraten wird.

Sie fordert die Bundesregierung auf, der Schaffung gemeinsamer Standards zur grenzüberschreitenden Überwachung der Telekommunikation nur insoweit zuzustimmen, als damit nicht zusätzliche Eingriffe in das Grundrecht auf unbeobachtete Kommunikation und das Fernmeldegeheimnis verbunden sind und die Nutzung datenschutzfreundlicher Technologien (z. B. prepaid cards) nicht konterkariert wird.

Anlage 16

E n t s c h l i e ß u n g
der Datenschutzbeauftragten
des Bundes und der Länder vom 17. Juni 1998
Parlamentarische Kontrolle von Lauschangriffen in den Bundesländern

Bei der Einführung der Befugnis zum „Großen Lauschangriff“ hat der Gesetzgeber im Grundgesetz ein Verfahren zur parlamentarischen Kontrolle weitreichender Eingriffe in das Grundrecht auf Unverletzlichkeit der Wohnung verankert (Artikel 13 Abs. 6 GG). Dieses Verfahren dient nach dem Willen des Gesetzgebers der parlamentarischen Kontrolle der Normeffizienz. Auch wenn es die Überprüfung von Lauschangriffen durch die Gerichte und Datenschutzbeauftragten nicht ersetzt, hat es gleichwohl eine grundrechtssichernde Bedeutung. Jetzt ist jedoch bekannt geworden, dass einige Landesjustizverwaltungen der Ansicht sind, Art. 13 Abs. 6 GG sehe eine Berichtspflicht über Lauschangriffe zu Strafverfolgungszwecken gegenüber den Landesparlamenten nicht vor.

Im Gegensatz dazu vertritt die Konferenz der Datenschutzbeauftragten des Bundes und der Länder die Auffassung, dass die Verfassung eine effektive parlamentarische Kontrolle von Lauschangriffen auf Landesebene vorschreibt, die der Kontrolle auf Bundesebene gleichwertig sein muss. Bei Maßnahmen zur Strafverfolgung durch Landesbehörden besteht die parlamentarische Verantwortlichkeit gegenüber den Landesparlamenten. Die Landtage müssen die Möglichkeit haben, die ihnen in anonymisierter Form übermittelten Berichte der Landesregierungen öffentlich zu erörtern. Die Landesparlamente sollten deshalb durch Gesetz eine regelmäßige Berichtspflicht der Landesregierung für präventiv-polizeiliche und repressive Lauschangriffe vorsehen. Nur auf diese Weise ist eine wirksame parlamentarische Kontrolle der Ausübung dieser einschneidenden Überwachungsbefugnisse gewährleistet.

Wird durch eine solche Kontrolle deutlich, dass die akustische Wohnraumüberwachung für Zwecke der Strafverfolgung in der Praxis nicht die vom Gesetzgeber angestrebte Effizienz im Verhältnis zur Häufigkeit und Intensität der Grundrechtseingriffe zeigt, können Landesregierungen, die das Bundesrecht in eigener Verantwortung auszuführen haben, über den Bundesrat darauf hinwirken, die Befugnis für eine derartige Überwachung wieder aufzuheben oder zumindest zu modifizieren.

Anlage 17

E n t s c h l i e ß u n g
der Datenschutzbeauftragten
des Bundes und der Länder vom 16. August 1999
Angemessener Datenschutz auch für Untersuchungsgefangene

Die Datenschutzbeauftragten des Bundes und der Länder begrüßen, dass die Bundesregierung den Entwurf eines Gesetzes zur Regelung des Vollzuges der Untersuchungshaft vorgelegt hat. Damit wird die seit Jahren erhobene Forderung der Datenschutzbeauftragten nach einer bereichsspezifischen gesetzlichen Regelung aufgegriffen.
Diese Regelung muss das Strafverfolgungs- und Sicherheitsinteresse des Staates im Rahmen des gesetzlichen Zwecks der Untersuchungshaft berücksichtigen. Gleichzeitig sind jedoch das Persönlichkeitsrecht der Gefangenen sowie die Unschuldsvermutung und der Anspruch auf wirksame Verteidigung im Strafverfahren angemessen zur Geltung zu bringen.

Der Gesetzentwurf der Bundesregierung trägt diesem Anliegen durch differenzierende Vorschriften teilweise Rechnung, lässt allerdings noch Raum für datenschutzrechtliche Verbesserungen. Die Stellungnahme des Bundesrates betont demgegenüber einseitig das staatliche Vollzugsinteresse und entfernt sich damit deutlich vom Ziel einer sorgfältigen Güterabwägung.

Nach Auffassung der Datenschutzbeauftragten des Bundes und der Länder muss die gesetzliche Regelung insbesondere folgenden Anforderungen genügen:

– Entgegen dem Vorschlag des Bundesrates, von einer inhaltlichen Überwachung nur ausnahmsweise nach dem Ermessen des Gerichts abzusehen, sollte im weiteren Gesetzgebungsverfahren an der Konzeption der Bundesregierung festgehalten werden. Der Gesetzentwurf der Bundesregierung differenziert bei der Überwachung der Unterhaltung mit Besucherinnen und Besuchern sowie bei der Kontrolle des Textes von Schriftstücken sachgerecht nach Haftgründen. Nur im Falle der Untersuchungshaft wegen Verdunkelungsgefahr sollten diese Maßnahmen unmittelbar und generell durch Gesetz vorgeschrieben werden, während sie bei Vorliegen anderer Haftgründe (z. B. Fluchtgefahr) nur im Einzelfall aufgrund richterlicher Anordnung erfolgen dürfen.

  Darüber hinaus sollte im weiteren Gesetzgebungsverfahren die Möglichkeit unüberwachter Kontakte der Gefangenen zu nahen Angehörigen mit Zustimmung der Staatsanwaltschaft auch in Fällen der Untersuchungshaft wegen Verdunkelungsgefahr erwogen werden. Stichprobenartige Überprüfungen von Schriftstücken durch die Vollzugsanstalt anstelle einer Textkontrolle sollten nicht den gesamten Schriftverkehr einzelner Gefangener umfassen. Dies könnte sich im Ergebnis als verdachtsunabhängige Totalkontrolle ohne richterliche Entscheidung auswirken.

– Das Recht auf ungehinderten und unüberwachten telefonischen Kontakt zwischen Verteidigung und Beschuldigten muss auch in der Untersuchungshaft gewährleistet sein. Mit dem rechtsstaatlichen Gebot wirksamer Strafverteidigung wäre es nicht vereinbar, diesen Kontakt von einer besonderen Erlaubnis des Gerichts abhängig zu machen, wie vom Bundesrat befürwortet.

– Bei Datenübermittlungen an öffentliche Stellen außerhalb der Vollzugsanstalt (z. B. Sozialleistungsträger, Ausländerbehörden) und an Forschungseinrichtungen müssen die schutzwürdigen Interessen der Betroffenen im Rahmen einer Abwägung berücksichtigt werden. Auch die Erteilung von Auskünften an die Verletzten der Straftat sollte der Gesetzgeber unter Beachtung der Unschuldsvermutung regeln.

– Die vom Bundesrat vorgeschlagene erhebliche Einschränkung des Auskunfts- und Akteneinsichtsrechts von Gefangenen im Hinblick auf den Zweck der Untersuchungshaft würde wesentliche Datenschutzrechte in einem besonders sensiblen Bereich weitgehend entwerten und ist daher abzulehnen.

Anlage 18

E n t s c h l i e ß u n g
der Datenschutzbeauftragten
des Bundes und der Länder vom 25. August 1999
„Gesundheitsreform 2000“

Die Datenschutzbeauftragten von Bund und Ländern erklären zu dem Entwurf eines Gesetzes „Gesundheitsreform 2000“:

Die Datenschutzbeauftragten haben großes Verständnis für die Bemühungen, die Kosten im Gesundheitswesen zu begrenzen und eine gute Versorgung der Patientinnen und Patienten sicherzustellen. Bei der Wahl der Mittel ist es aber Aufgabe des Gesetzgebers, beim Eingriff in das Recht auf informationelle Selbstbestimmung das Prinzip der Erforderlichkeit und der Verhältnismäßigkeit zu wahren.

Der Entwurf lässt jede Begründung vermissen, warum die bisherigen Kontrollmechanismen, die das Entstehen umfangreicher medizinischer Patientendatenbestände bei den Krankenkassen vermeiden, ungeeignet sein sollen, die Wirtschaftlichkeit und Qualität ärztlicher Leistungserbringung sicherzustellen.

Der Entwurf gibt das bisherige Konzept der Datenverarbeitung in der gesetzlichen Krankenversicherung auf. Insbesondere standen bisher aus dem ambulanten Bereich personenbezogene Abrechnungsdaten mit medizinischen Inhalten und Diagnosedaten den Krankenkassen nur ausnahmsweise zu Prüfzwecken zur Verfügung, künftig sollen diese Informationen den Krankenkassen dagegen generell versichertenbezogen übermittelt werden. Damit entstehen bei den gesetzlichen Krankenkassen vollständige personenbezogene medizinische Datenbestände der gesetzlich Versicherten mit der Möglichkeit, für jede einzelne Person umfassende Darstellungen ihres Gesundheitszustandes zu bilden. Bei den Kassen entstehen gläserne Patientinnen und Patienten. Das Patientengeheimnis wird ausgehöhlt.

Die Datenschutzbeauftragten richten an den Gesetzgeber die dringende Bitte, die bisher versäumte eingehende Prüfung von Erforderlichkeit und Verhältnismäßigkeit der weiter reichenden Datenverarbeitungsbestimmungen nachzuholen. Der Bundesbeauftragte für den Datenschutz, mit dem der Entwurf entgegen anders lautenden Äußerungen von Regierungsvertretern in der Sache bisher in keiner Weise abgestimmt wurde, sowie die Datenschutzbeauftragten der Länder stehen hierfür zur Diskussion zur Verfügung.

Insbesondere klärungsbedürftig sind folgende Punkte:

– Der Entwurf erweitert die Aufgaben der Krankenkassen auch auf eine steuernde und durch die Patientinnen und Patienten nicht geforderte Beratung über Gesundheitserhaltungsmaßnahmen und auf eine Prüfung der u. a. durch die Ärztinnen und Ärzte erbrachten Leistungen. Er sieht dafür umfangreiche Datenerhebungs- und -verarbeitungsbefugnisse vor.

  Der Wortlaut des Entwurfes beschreibt diese Aufgabe allerdings nur vage. Er lässt nicht erkennen, was auf die Patientinnen und Patienten zukommt. Weder ist klar geregelt, wie weit die Beratung reichen darf, noch mit welchen Rechtsfolgen die oder der Einzelne rechnen muss. Es ist zu befürchten, dass diese Beratung dazu dienen wird, die Patientinnen und Patienten, Ärztinnen und Ärzte und die sonstigen Leistungserbringer zu kontrollieren und zu beeinflussen und dass hierdurch das Arzt-Patienten-Vertrauensverhältnis belastet wird.

  Wegen der vagen Aufgabenbeschreibung sind auch die damit verbundenen Datenverarbeitungs- und -zusammenführungsbefugnisse in gleicher Weise unklar und verschwommen. Eine Präzisierung und Eingrenzung ist dringend erforderlich.

– Der Entwurf sieht im Gegensatz zum bisherigen System vor, dass Abrechnungsdaten und Diagnosen aus der ambulanten ärztlichen Behandlung generell patientenbezogen an die Krankenkassen übermittelt werden. Dadurch entstehen bei den Kassen umfangreiche sensible Datenbestände, aus denen sich für jede einzelne Patientin und jeden einzelnen Patienten ein vollständiges Gesundheitsprofil erstellen lässt. Wegen der Verpflichtung, die Diagnosen nach dem international gültigen ICD-10-Schlüssel zu codieren, sind diese medizinischen Informationen z. B. im Bereich der Psychotherapie auch hochdifferenziert.

  Die zur Begründung besonders angeführten Punkte *„Unterrichtung der Versicherten über die in Anspruch genommenen Leistungen, Kontrolle der Einhaltung der zweijährigen Gewährleistungspflicht bei den Zahnärzten, Unterstützung der Versicherten bei Behandlungsfehlern“* vermögen insoweit nicht zu überzeugen. Bereits jetzt können die Versicherten über die beanspruchten Leistungen und deren Kosten informiert werden und von ihrer Krankenkasse auch im Übrigen Unterstützung erbitten, so dass keine Notwendigkeit für die Anlegung derart sensibler, umfangreicher und zentraler Datenbestände ersichtlich ist.

  Der Eingriff in die Rechte der Patientinnen und Patienten steht damit in keinem Verhältnis zu den angegebenen Zwecken.

– Die beabsichtigte Einführung von zentralen Datenannahme- und -verteilstellen, bei denen nicht einmal klar ist, in welcher Rechtsform (öffentlich oder privat) sie betrieben werden sollen, hat eine weitere, diesmal Krankenkassen übergreifende zentrale Sammlung medizinischer personenbezogener Patientendaten zur Folge. Wegen des hohen weiteren Gefährdungspotentials von derart umfassenden Datenbeständen müsste der Entwurf im Einzelnen begründen, warum eine konsequente Umsetzung der schon bisher möglichen Kontrollmechanismen nicht ausreicht.

  Die angesprochenen Punkte stellen besonders gewichtige, aber keineswegs die einzigen Probleme dar. Zu nennen sind hier nur beispielsweise

– die Verlängerung der Speicherdauer von Patientendaten beim Medizinischen Dienst der Krankenversicherung (MDK) von fünf auf zehn Jahre,

– unzureichende Regelungen bei den Speicherfristen, bei Umfang, Zweckbindung und Freiwilligkeit der Datenerhebung beim Hausarztmodell, der integrierten Versorgung und den Bonus-Modellen sowie

– unzureichende Pseudonymisierung bei den Arbeitsgemeinschaften.

Abzulehnen ist auch die völlig mangelhafte Zweckbindung der Daten bei den Krankenkassen.

Anlage 19

Schreiben der Konferenz der Datenschutzbeauftragten des Bundes und der Länder an den Vorsitzenden der Innenministerkonferenz Molekulargenetische Untersuchung von Körperzellen aufgrund einer Einwilligung

Sehr geehrter Herr Minister,

die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat sich schon frühzeitig damit befasst, unter welchen Voraussetzungen molekulargenetische Untersuchungen zum Zwecke der Identitätsfeststellung in künftigen Strafverfahren zulässig sind. Die Entschließung der 53. Konferenz vom 17./18. April 1997 über „Genetische Informationen in Datenbanken der Polizei für erkennungsdienstliche Zwecke“ füge ich zu Ihrer Information bei.

Die Datenschutzbeauftragten weisen darauf hin, dass molekulargenetische Untersuchungen in einigen Ländern zum Zwecke der Identitätsfeststellung in künftigen Strafverfahren auch aufgrund von Einwilligungen erfolgen. Diese Praxis halten sie für unzulässig. Gem. § 81 g i. V. m. § 81 f StPO erfolgt die Untersuchung zum Zwecke der Identitätsfeststellung in künftigen Strafverfahren auf Anordnung des Richters. Dieser entscheidet auf der Grundlage einer von ihm zu treffenden Prognose. § 81 Abs. 1 StPO setzt voraus, dass wegen Art oder Ausführung der Tat, wegen der Persönlichkeit des Beschuldigten oder sonstigen Erkenntnissen Grund zu der Annahme besteht, dass gegen ihn künftig erneut Strafverfahren wegen einer in § 81 g genannten Straftat zu führen sind. Diese gesetzlich vorgeschriebene Prognoseentscheidung fehlt, wenn die molekulargenetische Untersuchung aufgrund einer Einwilligung des Betroffenen durchgeführt wird. Eine solche Praxis beseitigt gesetzlich vorgesehene Schutzmechanismen und führt damit zu einer erheblichen Schlechterstellung derjenigen Personen, die „freiwillig“ eine Speichelprobe abgeben.

Darüber hinaus halten die Datenschutzbeauftragten des Bundes und der Länder insbesondere das von Strafgefangenen erteilte „Einverständnis“ für äußerst problematisch. Sie haben insoweit erhebliche Zweifel an der „Freiwilligkeit“ der Erklärung. Gerade bei einem Strafgefangenen, der Vollzugslockerungen begehrt, von deren Gewährung wiederum eine vorzeitige Entlassung abhängen kann, kann nicht von der Freiwilligkeit seiner Zustimmung zu einer molekulargenetischen Untersuchung ausgegangen werden. Dies gilt nicht nur dann, wenn er sich der Konsequenzen für die Gewährung der Vollzugslockerungen bewusst ist, sondern auch, wenn er solche nur befürchtet. In einer solchen Lage kann von einer freien Entscheidung keine Rede sein.

Ich wäre Ihnen dankbar, wenn Sie dieses Anliegen in der Innenministerkonferenz zur Sprache bringen würden.

Mit freundlichen Grüßen

Dr. Werner Kessel

Anlage 20

Datenschutz und Telefax

I. Datenschutzrechtliche Aspekte der Telefax-Nutzung

Die Besonderheiten der Telefaxkommunikation, insbesondere die Gefährdungen, die sich für das Post- und Fernmeldegeheimnis (Art. 10 GG) ergeben können, erfordern es, in den nachfolgenden Bereichen Maßnahmen zu treffen. Da die Rechtslage nicht allgemein bekannt ist, sollten die Bediensteten im Rahmen der allgemeinen Dienstanweisung nach § 9 LDSG auf die genannten Anforderungen hingewiesen werden.

Sende-/Empfangsprotokoll

Telefaxgeräte erzeugen automatisch oder auf Wunsch Sende-/Empfangsprotokolle, die bezüglich jedes Vorganges u. a. Zeitpunkt der Sendung bzw. des Empfangs und die Anschlusskennung der anderen Station enthalten. Diese Daten unterliegen dem besonderen Schutz des Fernmeldegeheimnisses. Die Sende- und Empfangsprotokolle müssen daher entsprechend sorgfältig behandelt werden. Kenntnisnahme und Ausdruck dürfen nur hierzu befugten Mitarbeitern erlaubt sein, für Unbefugte ist dies, soweit möglich, technisch zu verhindern; weiterhin sollte die Einsichtnahme geregelt werden. Die Protokolle sind sorgfältig und gesichert aufzubewahren.

Kenntnisnahme durch Unbefugte

Telefaxsendungen kommen – soweit nicht durch besondere Vorkehrungen eine Verschlüsselung oder Passwortsicherung erfolgt – beim Empfänger offen an, bei der Versendung ist daher besondere Sorgfalt geboten. Vor der Absendung muss die Richtigkeit der angegebenen Anschlussnummer gewährleistet sein. Dabei ist stets zu berücksichtigen, dass eine Telefaxsendung ebenso wie ein Telefongespräch u. U. von Unbefugten „abgehört“ werden kann.

Beim Einsatz PC-gestützter Fax-Systeme können sich aufgrund der Speicherung zu übertragender bzw. empfangener Sendungen zusätzliche Risiken ergeben. In diesen Fällen ist insbesondere durch Maßnahmen der Zugriffskontrolle eine Kenntnisnahme durch Unbefugte auszuschließen.

Anschlusskennung des Empfängers

Durch Falschwahl sowohl beim Absender als auch im Übertragungsnetz der Deutschen Bundespost kann es dazu kommen, dass ein anderer als der gewünschte Anschluss erreicht wird. Bei jeder Sendung ist zu überprüfen, ob auch tatsächlich der richtige Anschluss und der richtige Empfänger erreicht wird:

Nahezu jedes Gerät sendet – wenn es von einem anderen Gerät aus angewählt wird – die eigene Anschlusskennung an dieses zurück. Sie besteht in der Regel aus einem numerischen Teil und einem Textteil. Bei Absendung eines Telefax sollte daher stets die Rücksendung der Kennung des angewählten Gerätes abgewartet und diese überprüft werden. Bei fehlender Übereinstimmung muss im Zweifelsfall die Sendung sofort abgebrochen werden.

Zeitversetzte Sendungen

Bei Sendungen ins Ausland ist die Ortszeit im Empfängerland zu berücksichtigen. Bei Sendungen mit schutzwürdigem Inhalt ist sicherzustellen, dass ein Telefax dort nicht außerhalb der Dienstzeit ankommt und somit durch Unbefugte Einsicht genommen werden könnte. Dieser Gesichtspunkt ist auch im Inland dann zu beachten, wenn ein Telefax nicht sofort abgesandt, sondern von der Möglichkeit der zeitversetzten Sendung Gebrauch gemacht wird.

Anrufumleitung

Für Telefaxgeräte, die in Nebenstellenanlagen (Telefonanlagen) eingebunden sind, kann – soweit vorhanden – die Möglichkeit der Anrufumleitung und -weiterschaltung genutzt werden. Dies kann dazu führen, dass eine Sendung bei einem (anderen als dem angewählten) Empfangsgerät ankommt, das in einem fachlich unzuständigen Bereich aufgestellt ist. Dadurch könnte es zu einer datenschutzrechtlich unzulässigen Übermittlung kommen. Dieses Risiko kann nur durch Überprüfung der rückgesendeten Kennung ausgeschlossen werden.

Besonders schutzbedürftige Daten

Wegen der bestehenden Risiken sollten besonders schutzbedürftige Daten, insbesondere solche, die sich auf

- strafbare Handlungen, Ordnungswidrigkeiten,
- Sachverhalte, die einer besonderen gesetzlichen Geheimhaltungspflicht unterliegen (z. B. Steuergeheimnis, Sozialgeheimnis, Arztgeheimnis, Statistikgeheimnis),
- religiöse oder politische Anschauungen sowie
- arbeitsrechtliche (dienstrechtliche) Rechtsverhältnisse (bei Übermittlung durch den Arbeitgeber/Dienstherrn)

beziehen, nur dann per Telefax übermittelt werden, wenn dies von der Eilbedürftigkeit her geboten und durch besondere Vor-

kehrungen sichergestellt ist, dass die Sendung (nur) dem gewünschten Empfänger zugeht. Neben der Beachtung dieser Hinweise ist es bei besonders schutzwürdigen Daten geboten, unmittelbar vor der Sendung eine telefonische Vereinbarung möglichst auch über die persönliche Entgegennahme der Sendung zu treffen.

Dokumentation, Vollständigkeit

Jeder Sendung sollte ein Vorblatt vorangefügt werden, welches den Absender, dessen Telefax- und Telefonnummer (für Rückrufe) sowie die Gesamtzahl der gesendeten Seiten ausweist. Es sollte möglichst für jede einzelne Sendung ein Sendeprotokoll erzeugt und dem Vorgang beigefügt werden. Soweit das Gerät eine Kennzeichnung gesendeter Seiten durch einen Verifikationsstempel unterstützt, sollte diese Funktion eingestellt sein.

Bei Ausfall der Netzstromversorgung können die Speicherinhalte des Gerätes gelöscht werden. Davon können – sofern vorhanden – auch Seitenspeicher (für Gruppensendungen usw.) oder Ziel- und Gruppenwahlnummern betroffen sein. Die Gültigkeit der Anschlussnummern ist von Zeit zu Zeit, bei bekannt gewordenem Netzausfall in jedem Fall zu überprüfen.

Räumliche Unterbringung

Telefaxgeräte sollten in geeigneten Räumen untergebracht werden. Insbesondere muss sichergestellt sein, dass eine Telefaxsendung nicht, auch wenn sie unbeobachtet ankommt, von Unbefugten entnommen oder eingesehen werden kann.

Grundsätzlich ist beim Telefax-Einsatz zwischen konventionellen Faxgeräten und der Einbindung von Faxlösungen in Bürokommunikationssysteme zu unterscheiden:

II. Konventionelle Telefaxgeräte

Telefaxgeräte sind Daten verarbeitende Geräte, mit denen auch personenbezogene Daten automatisiert übertragen werden können. Sie werden eingesetzt, um bei einfacher Handhabung schnell Informationen zu übermitteln. Das Telefax ist nach dem Telefon inzwischen zum wichtigsten Kommunikationsverfahren geworden. Nicht alle Nutzer von Telefaxgeräten sind sich darüber im Klaren, welche Risiken für die Vertraulichkeit der per Telefax übermittelten Informationen bestehen.

Die besonderen Gefahren sind:

- Die Informationen werden grundsätzlich „offen“ (unverschlüsselt) übertragen und der Empfänger erhält sie – vergleichbar mit einer Postkarte – in unverschlossener Form.
- Der Telefaxverkehr ist wie ein Telefongespräch abhörbar.
- Die Adressierung erfolgt durch eine Zahlenfolge (Telefaxnummer) und nicht durch eine mehrgliedrige Anschrift. Dadurch sind Adressierungsfehler wahrscheinlicher, und Übertragungen an den falschen Adressaten werden nicht oder erst nachträglich bemerkt.
- Bei Telefaxgeräten neueren Typs kann der Hersteller Fernwartungen durchführen, ohne dass der Besitzer diesen Zugriff wahrnimmt. Unter bestimmten Umständen kann er dabei auf die im Telefaxgerät gespeicherten Daten zugreifen (z. B. Lesen der Seitenspeicher sowie Lesen und Beschreiben der Rufnummern- und Parameterspeicher).

Diese Gefahren werden von Anbietern der Telekommunikationsnetze und -dienste nicht abgefangen. Deshalb ist insbesondere die absendende Stelle für die ordnungsgemäße Übertragung und die richtige Einstellung der technischen Parameter am Telefaxgerät verantwortlich.

Die Datenschutzbeauftragten des Bundes und der Länder haben sich mit den Risiken vertraulicher Kommunikation beim Einsatz von Telefaxgeräten befasst. Sie geben die folgenden Empfehlungen, um einen datenschutzgerechten Umgang mit Telefaxgeräten zu gewährleisten.

1. Aufgrund der gegebenen Gefährdungen darf die Übertragung sensibler personenbezogener Daten per Telefax nicht zum Regelfall werden, sondern darf nur im Ausnahmefall unter Einhaltung zusätzlicher Sicherheitsvorkehrungen erfolgen.
2. Was am Telefon aus Gründen der Geheimhaltung nicht gesagt wird, darf auch nicht ohne besondere Sicherheitsvorkehrungen (z. B. Verschlüsselungsgeräte) gefaxt werden. Das gilt insbesondere für sensible, personenbezogene Daten, beispielsweise solche, die einem besonderen Berufs- oder Amtsgeheimnis unterliegen (Sozial-, Steuer-, Personal- und medizinische Daten).
3. Bei der Übertragung sensibler personenbezogener Daten ist zusätzlich zu hier genannten Maßnahmen mit dem Empfänger ein Sendezeitpunkt abzustimmen, damit Unbefugte keinen Einblick nehmen können. So kann auch eine Fehlleitung durch z. B. veraltete Anschlussnummern oder beim Empfänger aktivierte Anrufumleitungen bzw. -weiterleitungen vermieden werden.

4. Telefaxgeräte sollten nur auf der Grundlage schriftlicher Dienstanweisungen eingesetzt werden. Die Bedienung darf nur durch eingewiesenes Personal erfolgen.

5. Das Telefaxgerät ist so aufzustellen, dass Unbefugte keine Kenntnis vom Inhalt eingehender oder übertragener Schreiben erhalten können.

6. Alle vom Gerät angebotenen Sicherheitsmaßnahmen (z. B. Anzeige der störungsfreien Übertragung, gesicherte Zwischenspeicherung, Abruf nach Passwort, Fernwartungsmöglichkeit sperren) sollten genutzt werden.

7. Die vom Gerät auf der Gegenseite vor dem eigentlichen Sendevorgang abgegebene Kennung ist sofort zu überprüfen, damit bei eventuellen Wählfehlern die Übertragung unverzüglich abgebrochen werden kann.

8. Bei Telefaxgeräten, die an Nebenstellenanlagen angeschlossen sind, ist das Risiko einer Fehladressierung besonders groß, da vor der Nummer des Teilnehmers zusätzlich Zeichen zur Steuerung der Anlage eingegeben werden müssen. Beim Umgang mit derartigen Geräten ist deshalb besondere Sorgfalt geboten. Sofern technisch möglich, sollte die Nebenstellenanlage so eingerichtet werden, dass sie eine Verbindung ins öffentliche Netz nicht nach Eingabe einer „0“, sondern nach Eingabe eines Zeichens oder einer Zeichenfolge bereitstellt, die in „normalen“ Telefaxnummern nicht vorkommen können (beispielsweise „*“ oder „#“).

9. Die Dokumentationspflichten müssen eingehalten werden (z. B. Vorblatt oder entsprechend aussagekräftige Aufkleber verwenden, Zahl der Seiten angeben, Protokolle aufbewahren), Sende- und Empfangsprotokolle sind vertraulich abzulegen, da sie dem Fernmeldegeheimnis unterliegen.

10. Vor Verkauf, Weitergabe oder Aussortieren von Telefaxgeräten ist zu beachten, dass alle im Gerät gespeicherten Daten (Textinhalte, Verbindungsdaten, Kurzwahlziele usw.) gelöscht werden.

11. Die am Telefaxgerät eingestellten technischen Parameter und Speicherinhalte sind regelmäßig zu überprüfen, damit Veränderungen frühzeitig erkannt werden.

12. Verfügt das Telefaxgerät über eine Fernwartungsfunktion, sollte sie grundsätzlich durch den Nutzer deaktiviert werden. Nur für notwendige Wartungsarbeiten ist diese Funktion freizugeben. Nach Abschluss der Wartungsarbeiten sollten die eingestellten Parameter und Speicherinhalte kontrolliert werden.

III. Telefax in Bürokommunikationslösungen

Rechner mit Standard- oder Bürokommunikationssoftware können um Hard- und Softwarekomponenten erweitert werden, mit deren Hilfe Telefaxe gesendet und empfangen werden können (integrierte Telefaxlösungen). Lösungen für den Faxbetrieb werden sowohl für Einzelplatzrechner als auch für Rechnernetze angeboten.

Der Betrieb (Installation, Konfiguration, Bedienung und Wartung) integrierter Telefaxlösungen birgt gegenüber dem konventionellen Telefaxgerät zusätzliche Gefahren, da beispielsweise die verwendeten Faxmodems bzw. -karten oft nicht nur für Telefaxsendung und -empfang geeignet sind, sondern auch andere Formen der Datenübertragung und des Zugriffes ermöglichen.

Daher sollten die folgenden Empfehlungen beim Umgang mit integrierten Telefaxlösungen zusätzlich zu den bereits genannten beachtet werden.

1. Das verwendete Rechnersystem muss sorgfältig konfiguriert und gesichert sein. Die IT-Sicherheit des verwendeten Rechners bzw. Netzes ist Voraussetzung für einen datenschutzgerechten Betrieb der Faxlösung. Dazu gehört unter anderem, dass kein Unbefugter Zugang oder Zugriff zu den benutzten Rechnern und Netzwerken hat.

2. Beim Absenden ist auf die korrekte Angabe der Empfänger zu achten. Dazu sind die durch die Faxsoftware bereitgestellten Hilfsmittel wie Faxanschlusslisten, in denen Empfänger und Verteiler mit aussagekräftigen Bezeichnungen versehen werden können, zu benutzen.

3. Die vielfältigen Nutzungsmöglichkeiten integrierter Faxlösugen erfordern die regelmäßige und besonders sorgfältige Überprüfung der in der Faxsoftware gespeicherten technischen Parameter, Anschlusslisten und Protokolle.

4. Der Einsatz kryptographischer Verfahren ist bei integrierten Faxlösungen möglich, sofern beide Seiten kompatible Produkte einsetzen. Deshalb sollten personenbezogene Daten verschlüsselt und digital signiert übertragen werden, um das Abhören zu verhindern und um den Absender sicher ermitteln und Manipulationen erkennen zu können.

5. Schon bei der Beschaffung integrierter Telefaxlösungen sollte darauf geachtet werden, dass ausreichende Konfigurationsmöglichkeiten vorhanden sind, um die dringend notwendige Anpassung an die datenschutzrechtlichen Erfordernisse des Nutzer zu gewährleisten.

Zehn Hinweise zum Datenschutz bei Telefax

1. Sie tragen die Verantwortung für die durch Sie übermittelten personenbezogenen Daten; prüfen Sie daher genau deren Sensibilität.
2. Beachten Sie die für Ihre Behörde/Dienststelle geltenden Anweisungen für die Nutzung des Telefax-Dienstes.
3. Nutzen Sie nach Möglichkeit alle der Sicherheit dienenden Einrichtungen des Gerätes, insbesondere die Anzeige des erreichten Gerätes.
4. Vergewissern Sie sich vor einer Sendung, ob der Adressat noch unter der Ihnen bekannten Anschlussnummer erreichbar ist.
5. Verständigen Sie sich vor der Absendung besonders sensibler Daten mit dem Adressaten über den konkreten Zeitpunkt der Übermittlung.
6. Gewährleisten Sie – möglichst durch persönliche Anwesenheit am Gerät – während der Übertragung von Dokumenten mit personenbezogenen Daten, dass kein Unbefugter in diese Einsicht nehmen kann.
7. Verständigen Sie sich nach Empfang einer Sendung mit Ihrem Partner über aufgetretene Mängel und ggf. deren Behebung.
8. Erleichtern Sie sich und Ihren Partnern die Nachweisführung:
   - Vorblatt/Aufkleber der Dienststelle benutzen,
   - Blattnummerierung der Kopien,
   - Originale mit Verifikationsstempel versehen,
   - Journalfunktion nutzen.
9. Faxübertragungen sind „abhörbar“: Was am Telefon nicht gesagt werden darf, darf auch nicht gefaxt werden.
10. Beachten Sie bei der Nutzung von Fernkopierern auf PC-Basis (z. B. Fax-Karten) auch die damit verbundenen Risiken; verständigen Sie sich darüber mit Ihrem Datenschutzbeauftragten.

Anlage 21

Hinweise
zur datenschutzgerechten Gestaltung und Nutzung von E-Mail-Diensten durch öffentliche Stellen

Die elektronische Post (E-Mail) hat sich als Form des Austauschs und der Übertragung von Informationen in den Verwaltungen etabliert. Sie wird für die interne Kommunikation genutzt, für Mitteilungen an andere Behörden und im Verkehr mit dem Bürger; vielfach dient dabei das Internet als Kommunikationsmedium.

Aufgrund der technischen Gegebenheiten im Internet ist ein angemessener Schutz personenbezogener Daten häufig nicht gewährleistet. Die Vertraulichkeit der übertragenen Daten, ihre Vollständigkeit, der Schutz vor unerlaubten Veränderungen (Integrität) sowie die verlässliche Zurechenbarkeit zu einem bestimmten Absender (Authentizität) müssen gegebenenfalls durch zusätzliche Maßnahmen sichergestellt werden.

Die datenschutzrechtlichen Anforderungen ergeben sich u. a. aus § 9 Abs. 2 Nr. 9 Landesdatenschutzgesetz (LDSG). Danach sind bei der Übetragung personenbezogener Daten via E-Mail-Maßnahmen zu treffen, die gewährleisten, dass Nachrichten nicht unbefugt gelesen, kopiert, verändert oder gelöscht werden können. Weitere datenschutzrechtliche Gesichtspunkte sind die Löschung von Nachrichten und die Protokollierung der E-Mail-Nutzung.

Die Datenschutzmaßnahmen sind in einer Dienstanweisung darzustellen (§ 9 Abs. 5 LDSG). Aus technisch-organisatorischer Sicht sind bei der Einführung von E-Mail-Verfahren die nachfolgenden Punkte zu berücksichtigen.[1)]

1. Organisatorische Festlegungen

Vor der Freigabe von E-Mail-Verfahren ist zu klären, in welchem Umfang die dienstliche Nutzung der elektronischen Post zugelassen wird. Ausschlaggebend sind die bestehenden Anforderungen an die Vertraulichkeit der Information, an deren Schutz vor unbefugter Veränderung und an die Verbindlichkeit einer Mitteilung (vgl. Nr. 3). Dabei ist festzulegen, in welchen Bereichen die elektronische Post ergänzend oder an Stelle der Schriftform genutzt werden kann und in welchen Fällen Ausdrucke zu fertigen und zu den Akten zu nehmen sind. Ebenso wie für schriftliche Eingänge sind Vetretungsregelungen zu treffen (siehe Nr. 6).

Mailprogramme erlauben es meist, Absenderangaben wie Organisationsbezeichnung, Anschrift, Telefonnummer automatisch an das Ende einer E-Mail anzufügen. Soweit kein besonderer E-Mail-Briefkopf verwendet wird, sollte diese Möglichkeit genutzt werden, um die Zurechenbarkeit einer Nachricht zu unterstützen.

Die Adressierung beim Versand elektronischer Nachrichten muss so eindeutig erfolgen, dass fehlerhafte Zustellungen vermieden werden. Elektronische Nachrichten, die lediglich innerhalb einer öffentlichen Stelle versandt werden sollen, dürfen das interne Netz nicht verlassen. Hierauf ist insbesondere bei der Gestaltung Aufbau elektronischer Verteilerlisten zu achten.

2. Beschränkung auf die erforderlichen Komponenten und Dienste

Soweit lediglich die E-Mail-Funktionalität benötigt wird, sind ausschließlich die hierfür benötigten Komponenten bereitzustellen. Dies kann dadurch erfolgen, dass ein- und ausgehende Verbindungen über filternde Komponenten (z. B. Router) geleitet werden, die unzulässige Protokoll- und Diensteanforderungen zurückweisen. Falls die E-Mail-Anbindung im Rahmen eines mehrere Dienste umfassenden Internet-Zugangs realisiert wird, sind die Empfehlungen des LfD zum Anschluss von Netzen der öffentlichen Verwaltung an das Internet zu berücksichtigen.[2)]

3. Verschlüsselung der Inhalte, digitale Signatur

Nachrichten der elektronischen Post werden, wenn keine besonderen Vorkehrungen zur Sicherung der Vertraulichkeit getroffen wurden, im Klartext übertragen. Sie können damit auf allen Systemen, über welche die Daten geleitet werden, mitgelesen oder verändert werden. Der Übertragungsweg und seine Eigenschaften sind dem Absender und dem Empfänger, vielfach auch dem Provider, beim E-Mail-Versand in der Regel weder bekannt noch durch sie beeinflussbar, eine Vertrauenswürdigkeit des Transportwegs ist damit nicht gegeben. Kryptographische Verfahren wie Verschlüsselung und digitale Signatur sind hier geeignet, Verletzungen des Datenschutzes bei der Übetragung schutzwürdiger Daten zu verhindern. Mit ihrer Hilfe lassen sich Manipulationen und Übertragungsfehler erkennen und die unberechtigte Kenntnisnahme unterbinden. Verschlüsselungs- und Signaturlösungen sind Stand der Technik und können mit vertretbarem Aufwand eingesetzt werden.

1) Vgl. – Bundesamt für Sicherheit in der Informationstechnik, IT-Grundschutzhandbuch
– Entschließung der 49. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 9./10. März 1995 zum Datenschutz bei elektronischen Mitteilungssystemen
– Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 9. Mai 1996 zur sicheren Übertragung personenbezogener Daten

2) Orientierungshilfe „Anschluss von Netzen der öffentlichen Verwaltung an das Internet“ des Arbeitskreises Technik der Datenschutzbeauftragten des Bundes und der Länder

Entsprechend der Sensibilität der übermittelten Daten ist daher bei der Nutzung öffentlicher Übertragungswege eine Verschlüsselung vorzusehen. Aus datenschutzrechtlicher Sicht gilt dies insbesondere für Fälle, in denen besondere Berufs- und Amtsgeheimnisse berührt sind (§ 203 Strafgesetzbuch). Hierbei sind als sicher anerkannte Verfahren mit ausreichender Schlüssellänge zu verwenden. Lösungen, die auf einer einfachen DES-Verschlüsselung oder einer effektiven Schlüssellänge von lediglich 40 Bit beruhen, genügen dem nicht. Geeignete Algorithmen sind z. B. Triple DES mit 112 Bit oder IDEA mit 64 bzw. 128 Bit Schlüssellänge. Für asymmetrische Verfahren wie RSA wird ein Schlüssel von 1 024 Bit oder mehr empfohlen. Andere Lösungen kommen alternativ in Betracht, wenn diese nachweislich eine vergleichbare Sicherheit bieten. Bei personenbezogenen Daten geringer Sensibilität ist zumindest ein Schutz vor zufälliger Kenntnisnahme vorzusehen.

Für Verschlusssachen gelten die Regelungen der Verschlusssachenanweisung (VSA, MinBl. 1996 S. 66). Danach sind Verschlusssachen bei der Übertragung über technische Kommunikationsverbindungen mit zugelassenen Verfahren zu kryptieren bzw. durch andere zugelassene Maßnahmen zu sichern (VSA Nr. 47.1).

Für die verlässliche Zurechenbarkeit von Nachrichten und den Schutz vor unbefugten Veränderungen sollte daher auf digitale Signaturverfahren zurückgegriffen werden. Das in dieser Hinsicht mit einer zertifizierten Lösung nach dem Signaturgesetz (SigG) verbundene Schutzniveau kommt in der Regel nur dort in Betracht, wo besondere Anforderungen an Authentizität und Integrität elektronischer Daten bestehen und ein grundsätzlich offener Teilnehmerkreis vorliegt. Wenn regelmäßig ausschließlich festgelegte Stellen miteinander kommunizieren oder geringere Anforderungen an die Zurechenbarkeit und Unversehrtheit der Daten gestellt werden, sind aus Sicht des Datenschutzes auch andere Verfahren im Sinne des § 1 Abs. 2 SigG ausreichend.

Neben der Auswahl geeigneter Algorithmen ist beim Einsatz der Verfahren darauf zu achten, dass kein unbefugter Zugriff auf die verwendeten Schlüssel erfolgen kann. Soweit diese auf Festplatten oder Disketten gespeichert werden, sind sie durch geeignete Maßnahmen (z. B. Passphrase) entsprechend zu schützen.

4. Prüfung auf Schadensfunktionen in E-Mail-Anhängen

Nachrichten sind häufig Anlagen in Form von Dateien beliebigen Inhalts beigefügt. Diese können, vor allem, wenn es sich um lauffähige Programme, selbstextrahierende Dateien oder Dateien mit Makrofunktionen handelt, Schadensfunktionen enthalten. Vor der weiteren Verarbeitung sind daher die E-Mail-Eingänge mit aktuellen Prüfprogrammen regelmäßig auf sicherheitsrelevante Inhalte hin (Programm und Makroviren, Trojanische Pferde, ActiveX/Java-Komponenten usw.) zu untersuchen. Die Anwender sind darauf hinzuweisen, dass der Aufruf von E-Mail-Anhängen, deren Schadensfreiheit nicht kontrolliert wurde, zu Problemen führen kann und unterbleiben soll.

5. Löschen von Nachrichten

Personenbezogene Nachrichten sind nach § 19 Abs. 2 LDSG zu löschen, wenn ihre Kenntnis zur Aufgabenerfüllung nicht mehr erforderlich ist. Für die Speicherung verschickter und empfangener Nachrichten in den elektronischen Postfächern der Benutzer sowie auf dem Mail-Server der speichernden Stelle sind daher Regelungen über die Dauer der Speicherung zu treffen. Die daraus folgende Löschung nach Ablauf der festgelegten Speicherungsfrist sollte möglichst durch technische Maßnahmen unterstützt werden.

Die eingesetzten Programme für die E-Mail-Nutzung sind so zu konfigurieren, dass erfolgreich empfangene Nachrichten auf dem Mailserver des Providers gelöscht werden.
Im Hinblick auf die nach § 6 Abs. 2 Teledienstedatenschutzgesetz (TDDSG) vorgeschriebene Löschung von Nutzungs- und Abrechnungsdaten durch den Provider sollte im Rahmen des Vertragsschlusses eine entsprechende Bestätigung eingeholt werden.

6. Administration und Konfiguration der Mail-Systeme

Im Zusammenhang mit der o. g. Filterung von E-Mail-Verbindungen und der Prüfung auf sicherheitsrelevante Inhalte empfiehlt sich die Installation des lokalen Mail- bzw. Kommunikationsservers auf einem separaten Rechner. Die Verwaltung des Mail-Systems (postmaster) sollte aus Sicherheitsgründen von der Netzwerkverwaltung getrennt werden.

Der Verbindungsaufbau darf ausschließlich von der öffentlichen Stelle aus zum jeweiligen Provider möglich sein (Dial-up). Vorhandene Sicherheitsfunktionen der Anschlusskomponenten sind zu nutzen (vgl. Hinweise des LfD zur Einrichtung von ISDN-Wählverbindungen). Der Zugang zu den Postfächern der einzelnen Mitarbeiter oder Sachbereiche ist im Rahmen der Speicher- und Zugriffskontrolle nach § 9 Abs. 2 Nr. 3 und 5 LDSG durch geeignete Maßnahmen wie Benutzerpassworte oder vergleichbare Lösungen (z. B. Chipkarte, Token) zu sichern.

Dies gilt auch für die lediglich vorübergehend benötigten Zugriffe im Vertretungsfall. Die Weiterleitung von Nachrichten im Vertretungsfall sollte nach Möglichkeit durch die Eingabe eines Abwesenheitszeitraums durch den Vertretenen und die damit verbundene automatische Zustellung an die jeweilige Vertretung erfolgen. Bei Inanspruchnahme der Vertretungsberechtigung muss im Rahmen der Eingabekontrolle erkennbar sein, dass nicht der eigentlich zuständige Bearbeiter, sondern die Vertretung zugegriffen hat.

7. Protokollierung der E-Mail-Nutzung

Nach § 9 Abs. 2 Nr. 6 LDSG ist im Rahmen der Übermittlungskontrolle zu gewährleisten, dass festgestellt werden kann, an wen welche personenbezogenen Daten durch Einrichtungen zur Datenübertragung übermittelt werden können und dies einschließlich des Zeitpunktes stichprobenweise überprüft werden kann. Darüber hinaus kann eine Protokollierung für Zwecke der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung des ordnungsgemäßen Betriebs erfolgen. Hinsichtlich der Überwachung der ordnungsgemäßen Nutzung eines dienstlich bereitgestellten E-Mail-Zugangs bestehen gegen die Protokollierung

- des Versands von Nachrichten an gesperrte Empfängeradressen,
- des Versands/Empfangs von Nachrichten, die einen festgelegten Umfang überschreiten,
- des Versands/Empfangs von Massensendungen (Spam-Mail),
- des Empfangs von Nachrichten mit Schadensfunktionen (s. Nr. 4) sowie
- von Fehlermeldungen

keine Bedenken. Im Vordergrund steht dabei vor allem die Dokumentation sicherheitsrelevanter, auffälliger oder von allgemeinen Vorgaben abweichender Vorgänge. Bezüglich ihrer Nutzung unterliegen Protokolldaten einer engen Zweckbindung (§ 13 Abs. 5 LDSG). Ausdrücklich untersagt ist die Nutzung zu Zwecken der Verhaltens- oder Leistungskontrolle (§ 31 Abs. 5 LDSG). Eine vollständige Aufzeichnung aller benutzerspezifischen Aktivitäten durch die Systembetreuung, insbesondere die grundsätzliche Speicherung der Inhalte elektronischer Post ist im Allgemeinen nicht erforderlich. Beim Verdacht auf eine missbräuchliche Nutzung des E-Mail-Dienstes kann es notwendig werden, den Umfang der Protokollierung vorübergehend zu erweitern. Die Entscheidung hierüber sollte an der Häufigkeit und Bedeutung der aufzuklärenden Umstände orientiert und unter Beteiligung der Personalvertretung getroffen werden.

Inwieweit eine Protokollierung datenschutzrechtlichen Anforderungen entspricht, bemisst sich weiterhin nach der Dauer der Aufbewahrung der Protokolldaten und den bestehenden Zugriffs- und Auswertungsmöglichkeiten. Nach den Empfehlungen des LfD sollte die Aufbewahrungsdauer von Protokolldaten den Zeitraum eines Jahres nicht überschreiten. Soweit Protokolle zum Zweck gezielter Kontrollen angefertigt werden, ist eine kürzere Speicherungsdauer vorzusehen; in der Regel reicht dabei eine Aufbewahrung bis zur tatsächlichen Kontrolle aus.

8. Veröffentlichung der E-Mail-Adressen der Angehörigen öffentlicher Stellen

Angaben über die elektronische Erreichbarkeit (Name, Amts- und Funktionsbezeichnung, dienstliche E-Mail-Adresse, öffentlicher Kryptografieschlüssel) unterliegen bei Angehörigen öffentlicher Stellen als Amtsträgerdaten nicht dem informationellen Selbstbestimmungsrecht. Gegen die Veröffentlichung dienstlicher E-Mail-Adressen bestehen daher aus datenschutzrechtlicher Sicht keine Bedenken. Dies beschränkt sich jedoch grundsätzlich auf Funktionsträger, die im Rahmen ihrer Aufgabenerfüllung nach außen hin tätig werden. Fürsorgegesichtspunkte können auch in diesen Fällen eine Beschränkung oder neutrale Fassung der Angaben erforderlich machen.

9. Private Nutzung

Gestattet der Dienstherr allgemein die private Nutzung eines vorhandenen E-Mail-Dienstes, wird er medienrechtlich zum Anbieter eines Teledienstes nach § 2 Abs. 2 Nr. 1 TDG und unterliegt den besonderen Anforderungen des Medienrechts an die Verarbeitung von Nutzungs- und Abrechnungsdaten. Mit der Erlaubnis zur privaten Nutzung der Kommunikationsanlage erbringt er weiterhin einen geschäftsmäßigen Telekommunikationsdienst gemäß § 3 Nr. 5 Telekommunikationsgesetz (TKG). Die private Nutzung des E-Mail-Dienstes unterliegt damit dem Fernmeldegeheimnis nach § 85 Abs. 2 TKG. Dieses erstreckt sich auf die Inhalte der Telekommunikation und ihre näheren Umstände.

Nach § 4 Abs. 2 Nr. 2 TDDSG hat der Diensteanbieter durch technisch-organisatorische Vorkehrungen sicherzustellen, dass 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. Die Dauer der Speicherung von Abrechnungsdaten richtet sich nach § 6 Abs. 2 Nr. 2 TDDSG und beträgt bei Einzelnachweisen in der Regel 80 Tage nach Rechnungsversand. Die Nutzer sind nach § 3 Abs. 5 TDDSG über Art, Umfang, Ort und Zwecke der Verarbeitung personenbezogener Daten zu unterrichten.

Bei Vorliegen tatsächlicher Anhaltspunkte dürfen personenbezogene Daten der Nutzer für die Aufklärung einer missbräuchlichen Inanspruchnahme des Dienstes ermittelt werden (vgl. Nr. 7). In der Dienstanweisung sollte daher festgelegt werden, ob und ggf. mit welchen Einschränkungen eine private Nutzung zugestanden wird.

Angesichts der unterschiedlichen medienrechtlichen Anforderungen an die dienstliche und private E-Mail-Nutzung sollte letztere über einen separaten Account erfolgen und anhand eines unterschiedlichen Adressierungsschemas unterscheidbar sein (z. B. *name.privat@dienststelle.de*). Dies dient auch der in den Telekommunikationsanschlussvorschriften des Landes geforderten getrennten Erfassung der privaten Nutzung (VV FM Nr. 2.3.1, MinBl. 1998, 119).

10. Anmeldung zum Datenschutzregister; Geräte- und Verfahrensverzeichnis

Soweit im Rahmen der E-Mail-Kommunikation personenbezogene Daten verarbeitet werden, besteht eine Anmeldepflicht nach § 27 LDSG. Das Verfahren und die eingesetzten Programme sind in das Geräte- und Verfahrensverzeichnis nach § 10 Abs. 2 und 3 LDSG aufzunehmen.

Für die Anmeldung zum Datenschutzregister gelten die im 16. Tätigkeitsbericht des LfD, Tz. 21.8.3, genannten Kriterien. Aus einer E-Mail-Anbindung ergeben sich Risiken für die angeschlossenen IT-Systeme. Soweit auf diesen meldepflichtige Verfahren nach § 27 LDSG betrieben werden, stellt dies eine wesentliche Änderung der technischen Rahmenbedingungen dar, die dem LfD mitzuteilen ist. Ausreichend ist die einmalige Anmeldung des Verfahrens unter Angabe der Zahl der angeschlossenen Arbeitsplätze und Mail-Server. Anmeldungen für die einzelnen Rechner sind nicht erforderlich.

Anlage 22

Datenschutzrechtliche Anforderungen
an die Gestaltung von Internet-Zugängen und -Angeboten öffentlicher Stellen in Rheinland-Pfalz

1. Welche personenbezogenen Daten dürfen im Internet von öffentlichen Stellen des Landes zum Abruf bereitgehalten werden?

Im Internet dürfen nur solche personenbezogenen Daten zum Abruf für die Allgemeinheit bereitgestellt werden,

- die allgemein zur Nutzung offen stehen oder deren Veröffentlichung zulässig wäre (§ 7 Abs. 6 Landesdatenschutzgesetz – LDSG);
- dazu gehören auch solche Amtsträger-Daten, die nicht dem informationellen Selbstbestimmungsrecht unterliegen (Namen, Amts- und Funktionsbezeichnung sowie dienstliche Erreichbarkeitsangaben solcher Funktionsträger im öffentlichen Dienst, die nach außen gegenüber dem Bürger tätig werden; zu dieser „Amtsträger-Theorie“ vgl. den 16. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz Rheinland-Pfalz, Tz. 17.3, sowie grundlegend den 13. Tätigkeitsbericht, Tz. 17.3).
- Selbstverständlich können auf der Basis einer freiwilligen Einwilligung, die den Anforderungen des § 5 LDSG entspricht, auch sonstige personenbezogene Daten zum Abruf bereitgestellt werden, wenn dies der Aufgabenerfüllung der öffentlichen Stelle dient.

2. Technisch-organisatorische Anforderungen nach dem Landesdatenschutzgesetz [3)]

a) Risikoanalyse/Datenschutzkonzept

Wenn der Anbieter seinen Web-Server in eine vorhandene IT-Struktur integriert, ist es erforderlich, die besonderen Gefährdungen, die sich aus einer Internet-Anbindung ergeben, in einer Risikoanalyse darzustellen und die notwendigen Maßnahmen in einem Sicherheitskonzept festzulegen. Wegen der Vorgehensweise wird – ergänzend zu den unter b) bis j) genannten Gesichtspunkten – auf das IT-Grundschutzhandbuch des BSI verwiesen.

b) Technische Abschottung des Internet-Anschlusses

Grundsätzlich 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, Email/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 die gesicherte Anbindung erfolgen, z. B. separate Modemverbindungen am Arbeitsplatz, sind zu untersagen und soweit möglich technisch zu unterbinden.

Solange ein abgesicherter Zugang zum Internet nicht zur Verfügung steht, lassen sich die Risiken dadurch begrenzen, indem davon abgesehen wird, eine Internet-Anbindung auf zentralen Systemen oder Netzwerken bereitzustellen. Entsprechende Zugangsmöglichkeiten sollten lediglich auf solchen Rechnern bestehen, die vom lokalen Netzwerk physikalisch getrennt sind und auf welchen keine datenschutzrelevanten Daten verarbeitet werden.

c) Beschränkung der zugelassenen Dienste

Bei der Einrichtung 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. Falls z. B. lediglich die Erreichbarkeit per E-Mail sichergestellt werden soll, ist es ausreichend, statt des umfassenden WWW-Zugriffs nur einen entsprechenden Client zu installieren und den Dienst freizugeben.

d) Nutzerdaten-Protokollierung

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.

3) Eine Orientierungshilfe zu technischen Fragen beim „Anschluss von Netzen der öffentlichen Verwaltung an das Internet“ kann beim LfD Rheinland-Pfalz angefordert werden. Im Übrigen ist darauf hinzuweisen, dass die Anforderungen nur zugrunde zu legen sind, soweit das Landesdatenschutzgesetz Anwendung findet.

Eine aussagefähige Protokollierung erfordert dabei nicht unabdingbar die Speicherung personenbezogener Benutzerdaten. Dies wäre im Blick auf § 13 Abs. 2 Nr. 2 MDStV und § 4 Abs. 2 Nr. 2 TDDSG auch unzulässig, da danach die anfallenden Daten über den Ablauf des Abrufs oder Zugriffs unmittelbar nach deren Beendigung zu löschen sind, soweit nicht eine längere Speicherung für Abrechnungszwecke erforderlich ist. Damit kommt lediglich die Speicherung ausreichend anonymisierter Nutzerdaten zu Protokollierungszwecken in Betracht.

Zur Protokollierung der Daten derjenigen Personen, die das Internet im Rahmen einer besonderen Rechtsbeziehung für eine öffentliche Stelle nutzen (Bedienstete, Angehörige der Universität o. Ä.), s. unten Nr. 4.

e) Schutz vor Computerviren und Software mit Schadensfunktionen

Bestimmte Internet-Dienste (z. B. ftp, smtp) bergen das Risiko, dass die aus dem Internet übernommenen Dateien Schadensfunktionen wie 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-Komponenten oder Java-Applikationen, über welche unter Umständen auf die Festplatte des Client-Rechners zugegriffen werden kann. Aufgrund der in diesem Zusammenhang bekannt gewordenen Sicherheitslücken sollte, soweit keine entsprechenden Vorkehrungen getroffen sind, diese Möglichkeit in den eingesetzten Internet-Browsern deaktiviert werden. Ähnlich dem Einsatz von Virensuchprogrammen empfiehlt sich die Verwendung geeigneter Zusatzsoftware.

f) Authentizität und Manipulationssicherheit der Internet-Inhalte

Die im Internet bereitgestellten Web-Seiten unterliegen dem Risiko der unbefugten Veränderung und Verfälschung; entsprechende und zum Teil spektakuläre Fälle sind aus der Vergangenheit bekannt. Falls sich aufgrund der Sensitivität der abrufbaren Daten und aufgrund der Öffentlichkeitswirkung erfolgreicher vorsätzlicher Manipulationen eine Gefährdung der Rechte Unbeteiligter ergeben kann, ist der sicheren Konfiguration und dem sicheren Betrieb der Web-Server besondere Bedeutung zuzumessen. Insoweit verweist der Landesbeauftragte für den Datenschutz auf die Maßnahmenempfehlungen des Bundesamtes für Sicherheit in der Informationstechnik im IT-Grundschutzhandbuch. Unter anderem sollte sichergestellt sein, dass bei erkannten Schwachstellen, z. B. über CERT-Advisories, regelmäßig eine Überprüfung und ggf. Anpassung der eingesetzten Programme erfolgt.

Gegen Manipulationen, die auf Schwächen der eingesetzten Protokolle beruhen (z. B. DNS-Spoofing) können Vorkehrungen nur in begrenztem Umfang getroffen werden. Die bestehenden Möglichkeiten sind jedoch in den Fällen erhöhter Missbrauchsanfälligkeit des Angebots zu nutzen. Hierzu zählen die Vergabe zufälliger statt aufsteigender Anfragenummern durch den eingesetzten DNS-Server sowie die Protokollierung von Paketen mit unerwarteten Query-IDs. Weiterhin sollte die Möglichkeit, bei DNS-Anfragen IP-Zuordnungen als so genannte „additional information“ mitzuliefern, unterbunden werden.

Da vorsätzliche Manipulationen an den Internet-Seiten nicht grundsätzlich auszuschließen sind, sollte zumindest sichergestellt sein, dass Manipulationen oder entsprechende Versuche frühzeitig erkannt werden (s. hierzu oben Buchstabe d Nutzerdaten-Protokollierung).

Eine weitere Maßnahme in diesem Zusammenhang ist die Überprüfung der Integrität der im Internet bereitgestellten Daten anhand von Checksummen, wodurch bei Abweichungen eine Meldung an die Systembetreuung erzeugt wird. Auf längere Sicht hält der Landesbeauftragte für den Datenschutz bei sensiblen Anwendungen den Einsatz digitaler Signaturverfahren für geboten.

g) Verschlüsselung personenbezogener Daten bei der Übertragung im Internet

Im Rahmen des Zugriffs einzelner Dienststellen bei der Bearbeitung des Internet-Angebots sowie bei der Kommunikation zwischen Bürger und öffentlicher Stelle über HTML-Formulare sollte eine Verschlüsselung, z. B. auf der Basis des Secure Socket Layer-Protokolls (SSL), vorgesehen werden. Für den Fall, dass diese Form der Verschlüsselung auch zur Absicherung bei der Übertragung vertraulicher Daten vorgesehen ist, ist darauf hinzuweisen, dass die standardmäßige Schlüssellänge im SSL-Protokoll mit 40 Bit nur eine eingeschränkte Sicherheit bietet. Nachgewiesenermaßen ist es mit der verfügbaren Technik möglich, die Verschlüsselung innerhalb kurzer Zeit aufzuheben. Für Anwendungen mit höheren Anforderungen an die Vertraulichkeit ist daher eine größere Schlüssellänge, ($\geq$ 75 Bit) zu wählen.

h) Information der Internet-Nutzer

Falls es das Internet-Angebot ermöglicht, im Rahmen der Beratung, der Entgegennahme von Hinweisen u. a. Informationen in elektronischer Form mit der öffentlichen Stelle auszutauschen, muss sichergestellt sein, dass die Nutzer über die bei der Übertragung bestehenden Risiken in Bezug auf unbefugte Dritte, die mögliche Verarbeitung ihrer Daten durch die öffentliche Stelle, den Verwendungszweck und den möglichen Empfängerkreis ausreichend unterrichtet werden (vgl. § 5 Abs. 3 LDSG). Im Internet-Angebot ist dann also eine entsprechende Information vorzusehen, die vor der Übermittlung und ausdrücklich, z. B. per Mausklick, zur Kenntnis genommen werden kann (zu weiteren Informationspflichten nach den Mediengesetzen siehe Punkt 3 d).

i) Besondere Löschungsverpflichtungen für Abrufer personenbezogener Daten

Nach dem gegenwärtigen Kenntnisstand ist bei für den allgemeinen Zugriff im World Wide Web (WWW) bereitgestellten Daten eine Einschränkung der freien Kopierbarkeit nicht möglich. Damit können Inhalte des Internet-Angebots von Dritten beliebig kopiert und auf eigenen Internet-Servern vorgehalten werden. Dies kann insbesondere für personenbezogene Daten, die lediglich zeitlich befristet im Internet eingestellt werden, von Bedeutung sein (z. B. polizeiliche Fahndungsaufrufe).

Die Möglichkeiten zu erreichen, dass Kopien von Inhalten, deren Speicherungsfrist abgelaufen ist, aus dem Netz entfernt werden, sind daher begrenzt. Eine gewisse Einflussnahme ist dort möglich, wo einem Kreis von Abonnenten Inhalte über Mailing-Listen oder Informationskanäle (Push-Technologie) automatisch zur Verfügung gestellt werden. Soweit auf diesem Weg personenbezogene Daten verteilt werden, sollte die Aufnahme in einen Verteiler von der Verpflichtung abhängig gemacht werden, im Internet-Angebot der öffentlichen Stelle nicht mehr vorgehaltene personenbezogene Daten ebenfalls zu löschen. Dies könnte z. B. als zu bestätigender Hinweis im Rahmen der Abonnementsfunktion realisiert werden. Ein Hinweis auf zu löschende Informationen könnte dabei per E-Mail über die entsprechenden Verteiler erfolgen.

In Fällen, in welchen personenbezogene Inhalte lediglich für einen bestimmten Nutzerkreis zum Abruf vorgehalten werden, ergibt sich grundsätzlich die Notwendigkeit der Authentifizierung wie sie etwa im Rahmen der Kontrolle des Zugriffs über Wählleitungen in der Praxis teilweise vorgesehen ist (SSL). Dies sollte nach Möglichkeit gegenseitig, d. h. sowohl für den Client als auch für den Server erfolgen. Mit dem Einsatz zertifizierter Server können die hierfür notwendigen Voraussetzungen geschaffen werden.

j) Anmeldung zum Datenschutzregister, Dienstanweisung

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. Eine Anmeldepflicht ergibt sich weiterhin, soweit im Rahmen des Betriebs des Internet-Angebots personenbezogene Daten verarbeitet werden.

Die für die Absicherung getroffenen technischen und organisatorischen Maßnahmen sowie die Einrichtung und Nutzung der Internet-Anbindung sind in einer Dienstanweisung nach § 9 Abs. 5 LDSG zu regeln.

3. Zusätzliche Anforderungen insbesondere zum Nutzerdatenschutz aus den Mediengesetzen

Internet-Angebote öffentlicher Stellen fallen regelmäßig entweder unter den Begriff der „Teledienste“ (die im Teledienstegesetz [TDG] und im Teledienstedatenschutzgesetz [TDDSG] geregelt sind) oder unter den der „Mediendienste“ (die im Mediendienste-Staatsvertrag [MDStV] geregelt sind). Aus beiden Rechtsgrundlagen folgen Anforderungen, die im Wesentlichen gleich sind und die insbesondere den Datenschutz der Nutzer, also der abrufenden Privatpersonen, bezwecken.

a) Begriff der Teledienste

Zu den Telediensten gehören die Angebote der modernen Kommunikationstechnik, die nicht unter die Definition der Mediendienste fallen. Dies sind insbesondere:

- Angebote im Bereich der Individualkommunikation, z. B. Telebanking, Datenaustausch, E-Mail (§ 2 Abs. 2 Nr. 1 TDG).
- Angebote zur Information oder Kommunikation, soweit nicht die redaktionelle Gestaltung zur Meinungsbildung für die Allgemeinheit im Vordergrund steht: Datendienste, z. B. Verkehrs,- Wetter- und Umweltdaten, Verbreitung von Informationen über Waren und Dienstleistungsangebote (§ 2 Abs. 2 Nr. 2 TDG).
- Angebote zur Nutzung des Internets oder weiterer Netze (§ 2 Abs. 2 Nr. 3 TDG).
- Angebote von Waren und Dienstleistungen in elektronisch abrufbaren Datenbanken mit interaktivem Zugriff und unmittelbarer Bestellmöglichkeit (§ 2 Abs. 2 Nr. 5 TDG).

Das Teledienstegesetz gilt ausdrücklich nicht für inhaltliche Angebote bei Verteildiensten und Abrufdiensten, soweit die redaktionelle Gestaltung zur Meinungsbildung für die Allgemeinheit im Vordergrund steht, soweit also § 2 des Mediendienste-Staatsvertrages (MDStV) anzuwenden ist (§ 2 Abs. 4 Nr. 3 TDG). Die Darstellung von Dienstleistungsangeboten des Anbieters ist jedoch ein typischer Teledienst.

b) Begriff der Mediendienste

Zum Bereich Mediendienste gehören die an die Allgemeinheit gerichteten Verteildienste wie Fernseheinkauf, Verbreitung von Messergebnissen in Text und Bild, Fernsehtext, Radiotext und vergleichbare Textdienste. Ausgenommen sind diejenigen Dienste, bei denen die individuelle Verbindung im Vordergrund steht, wie z. B. bei Abrufen und Bestellungen aus Datenbanken; diese gehören zu den Telediensten (§ 2 Abs. 2 Nr. 5 TDG).

Nach § 2 Abs. 2 Nr. 4 MDStV fallen auch solche Dienste, die auf Abruf durch den Nutzer zur Verfügung gestellt werden, unter die Definition der Mediendienste. Hier ergeben sich Abgrenzungsschwierigkeiten zu den Telediensten, die ebenfalls der Information dienen können.
Zu den Mediendiensten gehören aber nur solche an die Allgemeinheit gerichteten Informations- und Unterhaltungsangebote, bei denen eine redaktionelle Gestaltung erfolgt und die einen Beitrag zur Meinungsbildung der Allgemeinheit liefern sollen. Ausgenommen sind Dienste, bei denen der individual-kommunikative Charakter im Vordergrund steht, und solche Informationsdienste, bei denen keine oder nur eine nachrangig bedeutsame redaktionelle, mit dem Ziel der Meinungsbildung erfolgende Gestaltung vorgenommen wird.

Der individuelle Leistungsaustausch steht z. B. dann im Vordergrund, wenn die elektronisch erbrachten Leistungen auf ein konkretes Individualverhältnis zwischen dem Nutzer und dem Anbieter bezogen sind, z. B. Telebanking oder E-Mail. Ausgenommen vom Begriff des Mediendienstes sind auch solche Dienste, bei denen die reine Übermittlung von „Dateninformationen“ im Vordergrund steht, wie dies z. B. bei Fahrplänen, Flugplänen, Veranstaltungshinweisen und Ähnlichem der Fall ist.

Danach sind im Regelfall die Internet-Angebote öffentlicher Stellen, in denen sie ihre Aufgaben und Kompetenzen präsentieren, unter die Definition des Teledienstes zu subsumieren. Ausnahme: Die Einstellung von Presseerklärungen ins Internet ist als Betreiben eines Mediendienstes anzusehen.

c) Auswirkungen der Anwendung des TDG einerseits bzw. des Staatsvertrages andererseits

Die inhaltlichen Anforderungen aus TDG bzw. TDDSG einerseits und MDStV andererseits sind weitgehend identisch. Auch die Zuständigkeiten der datenschutzrechtlichen Kontrollbehörde unterscheiden sich nicht: In beiden Bereichen ist für öffentliche Stellen des Landes als Anbieter der Landesbeauftragte für den Datenschutz für die datenschutzrechtliche Kontrolle zuständig.

Ein Unterschied besteht allerdings bei der Frage, welche Folgen Verstöße gegen die jeweilige Rechtsnorm haben: Der Mediendienste-Staatsvertrag sieht detaillierte Bußgeldregelungen für den Fall der Zuwiderhandlung gegen die datenschutzrechtlichen Anforderungen des Staatsvertrages vor. Zuständige Bußgeldbehörde ist das Ministerium des Innern und für Sport. Demgegenüber enthalten TDG bzw. TDDSG keine Bußgeldregelung.

d) Inhaltliche Anforderungen aus TDDSG bzw. Mediendienste-Staatsvertrag

Für öffentliche Stellen des Landes, die ein Internet-Angebot verbreiten wollen, sind insbesondere folgende gesetzliche Anforderungen bedeutsam:

- Pflicht zur Anbieterkennzeichnung (§ 6 MDStV, § 6 TDG).
- Beachtung anerkannter journalistischer Grundsätze bei Berichterstattung und Informationsangeboten (§ 7 Abs. 2 MDStV).
- Besondere Kennzeichnungspflicht bei der Wiedergabe von Meinungsumfragen; Angabe, ob Repräsentativität besteht (§ 7 Abs. 3 MDStV).
- Beschränkung der Verarbeitung personenbezogener Daten: Diese dürfen vom Anbieter nur erhoben, verarbeitet und genutzt werden, soweit eine Rechtsvorschrift es erlaubt oder soweit der Betroffene eingewilligt hat (§ 12 Abs. 2 MDStV, § 3 Abs. 1 TDDSG). Diese Regelung hat allerdings für öffentliche Stellen des Landes angesichts der oben unter Punkt 1 dargestellten Rechtslage gemäß § 7 LDSG nur in Bezug auf die Nutzerdaten Bedeutung.
- Der Anbieter darf die Erbringung von Diensten nicht von einer Einwilligung des Nutzers in eine Verarbeitung oder Nutzung seiner Daten für andere Zwecke abhängig machen (§ 12 Abs. 4 MDStV, § 3 Abs. 3 TDDSG).
- Das Prinzip der „Datenvermeidung“ ist zu beachten (§ 12 Abs. 5 MDStV, § 3 Abs. 4 TDDSG).
- Der Nutzer ist vor der Erhebung über Art, Ort und Zwecke der Erhebung, Verarbeitung und Nutzung seiner personenbezogenen 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 (§ 12 Abs. 6 MDStV, § 3 Abs. 5 TDDSG).
- Der Nutzer ist vor einer Einwilligung auf sein Recht auf jederzeitigen Widerruf mit Wirkung für die Zukunft hinzuweisen (§ 12 Abs. 7 MDStV, § 3 Abs. 6 TDDSG).
- Der Anbieter hat dem Nutzer die Inanspruchnahme von Diensten anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist. Der Nutzer ist über diese Möglichkeit zu informieren (§ 13 Abs. 1 MDStV, § 4 Abs. 1 TDDSG).

- Der Anbieter hat durch technische und organisatorische Vorkehrungen sicherzustellen, dass
  - der Nutzer seine Verbindung mit dem Anbieter jederzeit abbrechen kann,
  - die anfallenden Daten über den Ablauf des Abrufs oder Zugriffs oder der sonstigen Nutzung unmittelbar nach deren Beendigung gelöscht werden,
  - der Nutzer Mediendienste gegen Kenntnisnahme Dritter geschützt in Anspruch nehmen kann (§ 13 Abs. 2 Nrn. 1 bis 3 MDStV, § 4 Abs. 2 Nrn. 1 bis 3 TDDSG).
- Die Weitervermittlung zu einem anderen Anbieter ist dem Nutzer anzuzeigen (§ 13 Abs. 3 MDStV, § 4 Abs. 3 TDDSG).
- Nutzungsprofile sind nur bei Verwendung von Pseudonymen zulässig (§ 13 Abs. 4 MDStV, § 4 Abs. 4 TDDSG).
- Der Nutzer ist berechtigt, jederzeit die zu seiner Person oder zu seinem Pseudonym gespeicherten Daten unentgeltlich beim Anbieter von Mediendiensten einzusehen. Die Auskunft ist auf Verlangen des Nutzers auch elektronisch zu erteilen (§ 16 Abs. 1 MDStV, § 7 TDDSG).

4. Interne Nutzerdatenverarbeitungen bei öffentlichen Stellen

Soweit öffentliche Stellen Internet-Anschlüsse nutzen, um selbst Informationen abzurufen, ergeben sich datenschutzrechtliche Fragen insbesondere im internen Verhältnis von der tatsächlich das Internet nutzenden Person (dem Bediensteten, dem Schüler oder Studenten) zu der medienrechtlich als Nutzer anzusehenden öffentlichen Stelle, die Inhaber des Internet-Anschlusses ist.

Im Vordergrund steht hierbei das Problem, welche personenbezogenen Nutzungsinformationen die öffentliche Stelle beim Anbieter speichern lassen und von dort abrufen (oder auch selbst intern speichern und nutzen) darf. Diese Frage wird nicht von den Mediengesetzen geregelt: Das interne Verhältnis der in einer nutzenden Stelle tätigen natürlichen Personen zu dieser öffentlichen Stelle gehört nicht zu deren Regelungsgegenstand. Diese Frage ist vielmehr nach dem jeweils für die öffentlichen Stellen geltenden Datenschutzrecht zu beurteilen:

Im Verhältnis von öffentlichen Stellen zu ihren Bediensteten gilt das Personaldatenschutzrecht (§ 31 LDSG für Angestellte und Arbeiter, §§ 102 ff. LBG für Beamte sowie Vorschriften des Personalvertretungsgesetzes über die Mitwirkung des Personalrats). Im hier vorliegenden Zusammenhang könnten die Regelungen als Beispiel dienen, die bei den Dienststellen in Ausführung dieser gesetzlichen Regelungen für die Erfassung und Nutzung von dienstlichen Telefongesprächsdaten geschaffen worden sind. Es ist also datenschutzrechtlich nicht verboten, die anfallenden Daten über den Ablauf des Abrufs oder Zugriffs zu protokollieren. Die Zulässigkeit im konkreten Fall hängt allerdings vom Ergebnis des Mitbestimmungsverfahrens ab.

Für das Verhältnis von Schulen zu ihren Schülern bildet § 54 a Abs. 1 SchulG mit der Betonung des Erforderlichkeitsgrundsatzes in Bezug auf die Erfüllung schulischer Aufgaben die entscheidende gesetzliche Grundlage für diese Fragen; ergänzt wird diese Schranke durch die Aufklärungspflicht gemäß § 12 Abs. 2 LDSG. Im Verhältnis von Hochschulen zu den Studenten ist mangels speziellerer Regelungen das LDSG (§§ 12 und 13) heranzuziehen, wonach der Erforderlichkeitsgrundsatz und eine umfassende Aufklärungspflicht gegenüber den Betroffenen (§ 12 Abs. 1 i. V. m. Abs. 2 LDSG) gelten.

Wenn allerdings öffentliche Stellen ihren Bediensteten oder auch privaten Dritten (z. B. in einer öffentlichen Bibliothek) das Angebot machen, zu privaten Zwecken Internet-Abrufe durchzuführen, ist dies ein Teledienst, der nur bei Beachtung der mediengesetzlichen Anforderungen zum Schutz der Nutzer zulässig ist (§ 2 Abs. 2 Nr. 3 TDG).

Anlage
zur Orientierungshilfe des LfD Rheinland-Pfalz
„Internet-Zugänge und -Angebote“

Gestaltungsmuster

Hinweis in Internet-Angeboten öffentlicher Stellen gem. § 5 Abs. 3 LDSG

(Der Hinweis sollte in einer Dialogbox erscheinen, wenn z. B. per Bildschirmformular personenbezogene Daten der Nutzer erfragt werden.)

Um dieses Internet-Angebot des/der … (Bezeichnung der Daten verarbeitenden Stelle) … nutzen zu können, ist die Verarbeitung der dargestellten personenbezogenen Daten erforderlich. Die Daten werden lediglich für … (Verwendungszweck) … verwendet. Ihre Daten werden nach … (Angabe einer Speicherungsfrist/Erfüllung des Zwecks) … gelöscht. *(Alternative: Ihre Daten werden … [dauerhaft/bis auf Widerruf] … gespeichert.)*
Eine Weitergabe an Dritte erfolgt … (nicht/an [Bezeichnung der empfangenden Stelle]) … .

Mit der Bestätigung dieses Hinweises willigen Sie in die o. g. Verarbeitung Ihrer Daten ein. Sie können diese Einwilligung schriftlich oder per E-Mail gegenüber dem/der … (Bezeichnung der Daten verarbeitenden Stelle) … jederzeit mit Wirkung für die Zukunft widerrufen. Nachteile entstehen Ihnen daraus nicht.

Bei einer unverschlüsselten Übertragung Ihrer Daten im Internet besteht die Möglichkeit, dass diese durch Unbefugte zur Kenntnis genommen oder verändert werden können. Dieses Angebot unterstützt daher die Verschlüsselung Ihrer Daten mit … (Art der Verschlüsselung, z. B. SSL, PGP und Darstellung der erforderlichen Schritte bzw. Verweis auf den öffentlichen Schlüssel/das Zertifikat der Daten verarbeitenden Stelle) … *(Alternative: Dieses Angebot unterstützt gegenwärtig keine Datenverschlüsselung. Bei der Übertragung Ihrer Daten im Internet besteht daher die Möglichkeit, dass diese durch Unbefugte zur Kenntnis genommen oder verändert werden können.)ap*

Ich willige in die o. g. Verarbeitung meiner Daten ein.	Ich willige <u>nicht</u> in die Verarbeitung meiner Daten ein (Abbruch).

Anlage 23

Die vom Arbeitskreis Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder herausgegebene „Orientierungshilfe zu Datenschutzfragen des Anschlusses von Netzen der öffentlichen Verwaltung an das Internet“ steht in einer überarbeiteten Fassung zur Verfügung (Stand: September 1998).

Wegen des Umfangs wurde von einer Veröffentlichung im Tätigkeitsbericht abgesehen. Sie kann jedoch beim Landesbauftragten für den Datenschutz Rheinland-Pfalz, Deutschausplatz 12, 55116 Mainz, bezogen oder in elektronischer Form im Internet unter der Adresse *www.datenschutz.rlp.de* abgerufen werden.

Anlage 24

Entwicklung der Anmeldungen zum Datenschutzregister