LANDTAG RHEINLAND-PFALZ
14. Wahlperiode

Drucksache 14/486
22. 11. 2001

Unterrichtung

durch den Landesbeauftragten für den Datenschutz

Achtzehnter Tätigkeitsbericht nach § 29 Abs. 2 Landesdatenschutzgesetz – LDSG – für die Zeit vom 1. Oktober 1999 bis 30. September 2001

Inhaltsverzeichnis

		Seite
1.	**Vorbemerkung**	18
1.1	Schwerpunkte des Datenschutzes in den letzten zwei Jahren	18
1.2	Bewertung	19
1.3	Ausblick	19
2.	**Weiterentwicklung des Datenschutzrechts**	20
2.1	Entwicklung des allgemeinen Datenschutzrechts: Novellierung des Bundesdatenschutzgesetzes sowie des Landesdatenschutzgesetzes	20
2.2	Zur optimalen Organisation der Datenschutzkontrolle	20
2.3	Erlass eines „Informationsfreiheitsgesetzes“	20
3.	**Datenschutz in Europa**	21
3.1	Die Umsetzung der EG-Datenschutzrichtlinie	21
3.2	Anwendung der Datenschutzvorschriften durch die Organe und Einrichtungen der Gemeinschaft	21
3.3	Das Grundrecht auf Datenschutz in der Charta der Grundrechte der Europäischen Union	22
3.4	Der Entwurf einer „Cyber-Crime“-Konvention des Europarats	23
3.5	Die Prinzipien des „sicheren Hafens“ – USA und EU einigen sich über den Schutz der Privatsphäre	24
3.6	Die „Artikel 29-Gruppe“	24
3.7	Zugang der Öffentlichkeit zu Dokumenten	25
4.	**Meldewesen**	25
4.1	EWOIS – quo vadis?	25
4.2	Der Entwurf des Dritten Änderungsgesetzes des Melderechtsrahmengesetzes	26
4.3	„Dauerbrenner“ im Bereich Meldewesen	26
4.3.1	Erforderliche Hinweise	26
4.3.2	Fragen zur Gruppenauskunft	27
4.4	Berücksichtigung der Auskunftssperre bei Gefährdung schutzwürdiger Interessen durch die in einem anderen Bundesland angesiedelte Wegzugsbehörde	28
4.5	Datenübermittlung an die GEZ	29
4.6	Zulässigkeit der Übermittlung von Meldedaten der Schulanfänger	29
4.7	Wahlwerbung – oder „Wenn die rechte Hand nicht weiß, was die linke tut“	30
4.8	Beantragung von Führungszeugnissen per E-Mail?	30
4.9	Zuständigkeit bei Beantragung eines Führungszeugnisses	31
4.10	Örtliche Feststellungen bei der automatisierten Übermittlung von Meldedaten	31

Dem Präsidenten des Landtags mit Schreiben vom 21. November 2001 zugeleitet. Der Bericht wurde in der Sitzung der Kommission beim Landesbeauftragten für den Datenschutz am 15. November 2001 nach § 26 Abs. 3 Satz 4 LDSG vorberaten.

Druck: Landtag Rheinland-Pfalz, 14. Dezember 2001

		Seite
5.	**Polizei**	32
5.1	Örtliche Feststellungen bei Polizeidienststellen	32
5.2	POLADIS-neu	32
5.3	INPOL-neu	34
5.4	Erfassung von Rauschgiftdelikten im „KAN-Bund“ und in der „Falldatei Rauschgift“ (FDR)	34
5.5	Speicherung von Haftmitteilungen der Justizvollzugsanstalten in den polizeilichen Informationssystemen	35
5.6	DNA-Merker	35
5.7	Anmeldung von EDV-Verfahren nach § 27 Abs. 1 LDSG	35
5.8	Videoaufnahmen durch Streifenwagen der Polizei	36
5.9	Abhören von Mobiltelefonen mit einem Abhörgerät, bei dem Unbeteiligte erfasst werden	36
5.10	Wahllichtbildvorlage	37
5.11	Konzeption zur Intensivierung der Zielfahndung	37
5.12	Übermittlung von Daten aus Gewerbeanzeigen durch die Kommunalbehörden an die Polizei	37
5.13	Datenübermittlung der Polizei zur Ausführung von § 11 Gewerbeordnung	38
5.14	Dienstanweisung der Polizei zum Datenschutz	38
5.15	Richtlinie über Auskünfte der Polizei an Ordnungsbehörden	39
5.16	Presserichtlinie	39
5.17	*Aufbewahrung von beschlagnahmten Patientenunterlagen bei der Polizei*	39
5.18	Datenschutzverstöße durch Polizeibeamte	39
6.	**Verfassungsschutz**	40
6.1	Auskunftsansprüche gegenüber dem Verfassungsschutz	40
6.2	Anforderungen an eine Novellierung des Landesverfassungsschutzgesetzes im Bereich der Telekommunikationsüberwachung	40
6.3	Video- und Tonaufzeichnungen von Veranstaltungen in geschlossenen Räumen	41
6.4	Regelanfrage von Ausländerbehörden an den Verfassungsschutz vor Einbürgerungen	41
7.	**Justiz**	41
7.1	Kontrollbefugnis des LfD bei Gerichten	41
7.2	Parlamentarische Kontrolle von Lauschangriffen in den Bundesländern	42
7.3	Telefonüberwachungen	43
7.4	Zugriff von Polizei und Staatsanwälten auf Verbindungsdaten der Telekommunikation	43
7.5	Das Rückmeldeverfahren von der Justiz an die Polizei	43
7.6	Täter-Opfer-Ausgleich und Datenschutz	44
7.7	DNA-Analyse im Strafverfahren	44
7.8	Internetveröffentlichungen justizieller Daten, insbesondere aus Insolvenzverfahren	45
7.9	Einführung des elektronischen Grundbuchs	45
7.10	Automatisierte Führung des Schuldnerverzeichnisses; unterlassene Unterrichtung der Bezieher von Abdrucken über eine Löschung	46
7.11	Löschung von Haftdaten eines lange zurückliegenden Verfahrens aus der Gefangenenpersonalakte	46
7.12	Eurojust	47
7.12.1	Pro Eurojust	47
7.12.2	Eurojust	47
7.12.3	Verhältnis von Eurojust zu EUROPOL	48
7.12.4	Datenschutzrechtliche Bewertungen	48
7.13	Bezeichnung strafrechtlicher Ermittlungsverfahren gegen mehrere Beschuldigte nach Verfahrenseinstellung gegen einen Namensgeber	49
8.	**Schulen, Hochschulen, Wissenschaft**	49
8.1	Schulen	49
8.1.1	MARKUS tanzt WALZER im IGLU	49
8.1.2	Umfrage des Landeselternbeirats über Unterrichtsausfälle an Schulen	50
8.1.3	Das schwarze Brett	50
8.1.4	Schulen im Internet	51
8.2	Hochschulen	51
8.2.1	Anmeldeverfahren für Lehrveranstaltungen	51
8.2.2	Datenschutzbeauftragter an der Hochschule	51
8.2.3	Forschungsdatenbank des Landes Rheinland-Pfalz	51
8.2.4	Datenschutz in der Landesverfassung und Personaldatenverarbeitung in der Hochschule	52
8.2.5	Übermittlung von Personalakten durch die Fachhochschule an das Ministerium	52

		Seite
8.2.6	Big Brother an der Hochschule? – Datenschutzrechtliche Aspekte von Webcams	52
8.2.7	Chipkarte als Studierendenausweis	53
8.2.8	Verwertung von Internet-Verbindungsdaten zum Zweck der Strafverfolgung	53
8.3	Wissenschaft	54
8.3.1	Online-Befragung über Internet-Nutzung in Schulen	54
8.3.2	Gentechnik	54
8.4	Verarbeitung personenbezogener Daten von Bibliotheksbenutzern	54
8.5	Verwendung von Daten ehemaliger Zwangsarbeiter für eine Ortschronik	55
9.	**Umwelt**	55
9.1	Umweltinformationsgesetz	55
9.1.1	Anzahl der Parkplätze als Umweltinformation?	55
9.1.2	Kein freier Zugang zu Umweltinformationen während eines strafrechtlichen Ermittlungsverfahrens	56
9.2	Beachtung datenschutzrechtlicher Bestimmungen bei Anfragen nach Datenmaterial in Bezug auf Altlasten	56
9.3	Haushaltserklärungen für die Gebührenerhebung bei der Abfallentsorgung	56
10.	**Gesundheitswesen**	57
10.1	Auskunft und Akteneinsicht im Gesundheitswesen	57
10.2	Ärztliche Untersuchung von Beschäftigten der Kreisverwaltungen und ihren Angehörigen	58
10.3	Einschaltung einer „Medizinischen Verbindungsstelle“ bei Inruhestandsversetzungen	58
10.4	Datenschutz im Rahmen der Aufnahmekonferenz innerhalb Gemeindepsychiatrischer Wohnverbünde	59
10.5	Weitergabe von Patientendaten an Betreuer	59
10.6	Zeugnisverweigerungsrechte im Erbscheinsverfahren	60
10.7	Datenschutzfragen in Zusammenhang mit der Bestellung von Transplantationsbeauftragten	60
10.8	Chipkarten im Gesundheitswesen	61
10.8.1	Einführung eines Arzneimittelpasses	61
10.8.2	Krankenversichertenkarte mit Lichtbild	62
10.9	Studie „Risikofaktoren für sporadische EHEC-Infektionen“	62
10.10	Datenschutz in Kindertagesstätten	62
11.	**Sozialdatenschutz**	63
11.1	Krankenkassen, Kassenärztliche Vereinigungen	63
11.1.1	Anforderung medizinischer Unterlagen durch Krankenkassen bei Krankenhäusern	63
11.1.2	Sozialdatenschutz auf dem Parkplatz	64
11.1.3	Datenschutz im sozialgerichtlichen Verfahren	64
11.2	Medizinischer Dienst der Krankenversicherung	65
11.2.1	Die Schere im Kopf – Zweckändernde Datennutzung beim MDK	65
11.2.2	MDK-Gutachten als „unrichtiges Sozialdatum“ im Sinne des § 84 Abs. 1 SGB X	66
11.3	Dialogverfahren der Rentenversicherungsträger	66
11.4	Outsourcing im Bereich des Landesamtes für Soziales, Jugend und Versorgung	67
11.5	Jugendhilfe	67
11.5.1	Datenschutz im Zusammenhang mit Leistungen nach dem Unterhaltsvorschussgesetz	67
11.5.2	Informationsaustausch zwischen Jugendamt und Sozialamt	68
11.5.3	Einsicht in Adoptionsunterlagen	68
11.6	Sozialhilfe	69
11.6.1	Arbeit statt Sozialhilfe	69
11.6.2	Ermittlungstätigkeiten der Sozialhilfeträger	70
11.6.3	Vorlage von Kontoauszügen und Befreiung vom Bankgeheimnis	70
12.	**Datenschutz im Ausländerwesen**	71
12.1	Entwurf eines Gesetzes zur Steuerung und Begrenzung der Zuwanderung und zur Regelung des Aufenthalts und der Integration von Unionsbürgern und Ausländern (Zuwanderungsgesetz)	71
12.2	Anteil der Speicherung von abgelehnten Asylbewerbern in INPOL	71
12.3	Ausschreibungen im Schengener Informations-System (SIS) zur Einreiseverweigerung	72
12.3.1	Wahrnehmung der Prüffristen	72
12.3.2	Beginn der Prüffristen im SIS	72
12.3.3	Ausschreibungen im SIS bei untergetauchten Asylbewerbern	73
12.4	Einführung einer Asyl-Card	73

		Seite
13.	**Finanzverwaltung**	73
13.1	Abgabenordnung	73
13.1.1	§ 31 a Abs. 1 AO	73
13.1.2	Zugriff der Finanzverwaltung auf DV-gestützte Buchführungssysteme	73
13.2	Datenerhebungen durch das Finanzamt	74
13.2.1	Fahrtenbuch zu steuerlichen Zwecken	74
13.2.2	Steuerliche Geltendmachung eines PCs	74
13.2.3	Lohnsteueraußenprüfung	74
13.3	Datenübermittlungen durch das Finanzamt	75
13.3.1	Auskünfte an Gewerbeamt	75
13.3.2	Auskünfte nach dem Sozialgesetzbuch	75
13.4	Hundesteuersatzung	75
13.4.1	Auskunftspflicht der Hundehalter	75
13.4.2	Mitteilungspflicht des Tierschutzvereins an das Hundesteueramt	76
13.5	Korruption in der öffentlichen Verwaltung	76
14.	**Wirtschaft und Verkehr**	76
14.1	Daten aus der Handwerksrolle im Internet?	76
14.2	Löschung von Daten aus der Gewerbeanzeige nach Abmeldung des Gewerbes	76
14.3	Auskünfte aus dem Gewerberegister an Parteien zum Zwecke der Wahlwerbung	77
14.4	Eine Gewebeabmeldung der besonderen Art	77
14.5	Neuerteilung der Fahrerlaubnis und Datenschutz	78
14.6	Probleme bei den Verwertungsregelungen im neuen Fahrerlaubnisrecht	78
14.7	Zweckwidrige Nutzung von TÜV-Daten	79
14.8	Tagesnachweis des Fahrlehrers	80
14.9	Identitätsausweis in Taxen?	80
14.10	Das Parken und der Datenschutz	81
14.10.1	Parkerleichterungen für Schwerbehinderte	81
14.10.2	Anwohnerparken	81
14.10.3	Ausnahmegenehmigungen für Soziale Dienste	81
15.	**Landwirtschaft, Weinbau und Forsten**	82
15.1	Veröffentlichung der Namen von Futtermittelherstellern im Zuge von BSE	82
15.2	Nutzung der Landwirtschaftlichen Betriebsdatenbank	82
16.	**Statistik**	82
16.1	Das Zensusvorbereitungsgesetz für eine registergestützte Volkszählung	82
16.2	Nutzung personenbezogener Daten zur Erarbeitung einer Statistik für den zweiten Versorgungsbericht der Bundesregierung	83
16.3	Umfrage gemäß § 7 Statistikregistergesetz	83
17.	**Personaldatenverarbeitung**	84
17.1	Multifunktionskarte für Bedienstete	84
17.2	Outsourcing im Bereich der Beihilfe	84
17.3	Heimarbeitsplätze beim Medizinischen Dienst der Krankenversicherung	85
17.4	Datenschutzfragen in Zusammenhang mit der Internet- und E-Mail-Nutzung durch Bedienstete	86
17.5	Aufbewahrung der Ergebnisse von Einstellungstests in der Personalakte	87
17.6	Personaldatenschutz bei Mitarbeitergesprächen	87
17.7	Datenschutz bei Konkurrentenklagen	88
17.8	Gesamtübersicht über Krankheitstage	88
17.9	Mitarbeiterbefragung im Rahmen von Organisationsuntersuchungen	89
18.	**Datenschutz im kommunalen Bereich**	89
18.1	E-Government	89
18.2	Kommunale Videoüberwachung	90
18.2.1	Videoüberwachung eines Dorfplatzes durch den Ortsbürgermeister	90
18.2.2	Videoüberwachung des Geldausgabeautomaten eines städtischen Sozialamtes	90
18.2.3	Videoüberwachung einer Feuerwache	91
18.2.4	Videoüberwachung eines Friedhofs	91
18.3	Stimmungsvoller Marktplatz	92

Seite

18.4 Bürgerbüros ... 92
18.5 Veröffentlichungen auf kommunalen Homepages im Internet ... 93
18.5.1 Privatadressen und Privattelefonnummern von Ratsmitgliedern ... 93
18.5.2 Privatadressen und Privattelefonnummern der Vorsitzenden örtlicher Vereine ... 93
18.6 Einsicht in das Wählerverzeichnis ... 93
18.7 Nutzung eines internetgestützten Wahlergebniserfassungsdienstes ... 94
18.8 Landesgesetz über die Volksinitiative sowie zur Änderung der Bestimmungen über Volksbegehren und Volksentscheide ... 94
18.9 Gemeinderatsfraktionen und Datenschutz ... 95
18.10 Ratsmitglieder im Bilde – Das Fotografieren während einer Stadtratssitzung ... 95
18.11 Namentliche Erfassung der Besucher öffentlicher Stadtratssitzungen ... 95
18.12 Schrankenlose Zugriffsmöglichkeiten für die Behördenleitung? ... 96
18.13 Grundstücks- und Grundeigentümerdaten für einen Windpark ... 96
18.14 Datenschutz im Zusammenhang mit der Ausführung der „Gefahrenabwehrverordnung Gefährliche Hunde“ ... 97
18.15 Keine Blankoeinwilligung zu Datenerhebungen der Unterhaltssicherungsstelle ... 97
18.16 Datenschutz und Ortschronik ... 98
18.17 Opfernamen auf einem Denkmal ... 98
18.18 Weitergabe von Listen der Beschäftigungsstellen ehemaliger NS-Zwangsarbeiter aus dem Stadtarchiv ... 99

19. Telekommunikation ... 99
19.1 Die Telekommunikations-Datenschutzverordnung (TDSV 2000) ... 99
19.2 Entwurf einer Telekommunikaitons-Überwachungsverordnung ... 100
19.3 EG-Richtlinienentwurf zum Datenschutz in den elektronischen Kommunikationsmedien ... 101

20. Medien ... 102
20.1 Entwurf eines Gesetzes über rechtliche Rahmenbedingungen für den elektronischen Geschäftsverkehr (Elektronischer Geschäftsverkehr-Gesetz-EGG) ... 102
20.2 Das neue Signaturgesetz ... 102
20.3 Datenschutz bei der Befreiung von der Rundfunkgebühr (automatisierte Verfahrensbearbeitung) ... 103
20.4 Datensparsamkeit bei der Rundfunkfinanzierung ... 103
20.5 Anfragen zur GEZ ... 104
20.6 Datenschutz im rundfunkrechtlichen Erlaubnisverfahren ... 104
20.7 Publizitätspflicht nach § 23 Rundfunkstaatsvertrag ... 105
20.8 Neue Medienordnung ... 106

21. Technischer und organisatorischer Datenschutz ... 106
21.1 Kontroll- und Beratungstätigkeit ... 106
21.2 Technisch-organisatorische Datenschutzfragen in ausgewählten Verfahren ... 107
21.2.1 Einwohnerinformationssystem Rheinland-Pfalz (EWOIS) ... 107
21.2.1.1 Neukonzeption des Verfahrens ... 107
21.2.1.2 Betrieb des Verfahrens ... 108
21.2.2 Landesdaten- und Kommunikationsnetz ... 109
21.2.2.1 Änderung der Netzstruktur ... 109
21.2.2.2 Einsatz kryptografischer Verfahren im Landesdaten- und Kommunikationsnetz ... 109
21.2.2.3 Penetrationstest der Firewall des Landesdaten- und Kommunikationsnetzes ... 110
21.2.3 Auswertungs- und Analysedatei der Polizei „Analyst Notebook“ ... 110
21.2.4 Internet-Anbindung von Verwaltungen über das Landesdaten- und Kommunikationsnetz ... 111
21.2.5 Einsatz von Stimmenzählgeräten bei Wahlen zum Landtag ... 112
21.2.6 Datenaustausch über ISDN-Verbindungen im Verfahren „Arbeit und Bildung statt Sozialhilfe“ ... 112
21.2.7 Telemedizinprojekt im Bereich der Schlaganfallversorgung ... 113
21.2.8 Einsatz von Pretty Good Privacy im Rahmen des automatisierten Mahnverfahrens ... 113
21.2.9 Datenkommunikation des DIZ mit dem Kraftfahrtbundesamt ... 113
21.2.10 Kooperation des DIZ Rheinland-Pfalz mit TÜV-Einrichtungen ... 114
21.2.11 Beantragung von Kfz-Wunschkennzeichen über das Internet ... 114
21.2.12 Einheitliche Pflege von Steuerungsdaten in statistischen Verbundverfahren (SYST) ... 114
21.2.13 Zugangskontrolle im Bereich einer Anstalt des Landes ... 115
21.2.14 Verfahren MEDIKOS des Medizinischen Dienstes der Krankenversicherung ... 115
21.2.15 Sicherung des Beleg- und Datenträgertransports bei einer Kassenärztlichen Vereinigung ... 115
21.3 Allgemeine technisch-organisatorische Aspekte ... 116

Seite

21.3.1 Wählleitungszugänge zum Landesdaten- und Kommunikationsnetz ... 116
21.3.2 Anforderungen an den Einsatz elektronischer Signaturlösungen in der Verwaltung ... 116
21.3.3 Verschlüsselung und elektronische Signatur bei der Übertragung von Personaldaten ... 117
21.3.4 Verschlüsselung und Elektronische Signatur bei der Befundübertragung per E-Mail ... 117
21.3.5 Datenschutzrechtliche Probleme beim Einsatz des Betriebssystems Windows ... 118
21.3.6 Einsatz des Betriebssystems Windows 2000 in der Landesverwaltung ... 118
21.3.7 Einsatz von Laptops im Rahmen mobiler Bürger-Service-Büros ... 119
21.3.8 Datenschutz am Informationsschalter eines Finanzamts ... 119
21.3.9 Struktur und Betreuung der Informationstechnik unter datenschutzrechtlichen Aspekten ... 119
21.3.10 Zugriffsmöglichkeiten für Gemeinderatsmitglieder auf IT-Systeme der Gemeindeverwaltung ... 120
21.3.11 Preisgabe von Passworten bei Abwesenheit der zuständigen Mitarbeiter ... 121
21.3.12 Speicherung von Personal- und Gesundheitsdaten auf zentralen Servern ... 121

22. Datenverarbeitung bei Sparkassen ... 122
22.1 Änderung der Meldepflicht für öffentlich-rechtliche Kreditinstitute ... 122
22.2 Datenweitergabe durch Sparkassen ... 122
22.3 Kontodaten des Überweisenden auf dem Kontoauszug des Empfängers ... 122
22.4 Zustellung von Rechnungen ... 122
22.5 Datenübermittlung zur Kundenpflege ... 122
22.6 Data Warehouse bei Sparkassen ... 123

23. Sonstiges ... 124
23.1 Weitergabe von Informationen im Rahmen einer Bauvoranfrage ... 124
23.2 Verpflichtung zur Übernahme des Amtes des behördlichen Datenschutzbeauftragten ... 124
23.3 Fernseh-Reportagen über behördliches Handeln und Datenschutz ... 124
23.4 Videoüberwachung von Hauseingangsbereichen ... 125
23.5 Unterhaltssicherungsgesetz ... 125

24. Schlussbemerkung ... 125
24.1 Zur Situation der Geschäftsstelle ... 125
24.2 Zur Öffentlichkeitsarbeit des Landesbeauftragten für den Datenschutz ... 126
24.3 Zusammenarbeit mit anderen Datenschutzinstitutionen ... 126
24.4 Resümee und Ausblick ... 127

Anlagenübersicht (Anlage 1 bis Anlage 32) ... 7

Abkürzungen ... 9
Glossar technischer Begriffe ... 11

Anlagen

Seite

1 Entschließung der 58. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 7./8. Oktober 1999 – Patientendatenschutz durch Pseudonymisierung 128

2 Entschließung der 58. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 7./8. Oktober 1999 – DNA-Analysen zur künftigen Strafverfolgung auf der Grundlage von Einwilligungen 128

3 Entschließung der 58. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 7./8. Oktober 1999 – Beschluss des Europäischen Rates zur Erarbeitung einer Charta der Grundrechte der Europäischen Union 129

4 Entschließung der 58. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 7./8. Oktober 1999 – Eckpunkte der deutschen Kryptopolitik – ein Schritt in die richtige Richtung 129

5 Entschließung der 58. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 7./8. Oktober 1999 – Aufbewahrung des Schriftguts der ordentlichen Gerichtsbarkeit und Staatsanwaltschaften 130

6 Entschließung der 58. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 7./8. Oktober 1999 – Täter-Opfer-Ausgleich und Datenschutz 131

7 Entschließung der 58. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 7./8. Oktober 1999 – Zugriff der Strafverfolgungsbehörden auf Verbindungsdaten in der Telekommunikation 131

8 Entschließung der 59. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14./15. März 2000 – Konsequenzen aus dem Urteil des Bundesverfassungsgerichtes zu den Abhörmaßnahmen des BND 132

9 Entschließung der 59. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14./15. März 2000 – Data Warehouse, Data Mining und Datenschutz 133

10 Entschließung der 59. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14./15. März 2000 – Für eine freie Telekommunikation in einer freien Gesellschaft 134

11 Entschließung der 59. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14./15. März 2000 – Unzulässiger Speicherungsumfang in „INPOL-neu“ geplant 136

12 Entschließung der 59. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14./15. März 2000 – Strafverfahrensänderungsgesetz 1999 (StVÄG 1999) 137

13 Entschließung der 59. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14./15. März 2000 – Risiken und Grenzen der Videoüberwachung 138

14 Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26. Juni 2000 – Effektive parlamentarische Kontrolle von Lauschangriffen durch aussagekräftige jährliche Berichte der Bundesregierung 139

15 Entschließung der 60. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 12./13. Oktober 2000 – Datenschutzrechtliche Konsequenzen aus der Entschlüsselung des menschlichen Genoms 140

16 Entschließung der 60. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 12./13. Oktober 2000 – Entschließung zur Novellierung des BDSG 141

Seite

17 Entschließung der 60. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 12./13. Oktober 2000 – Datensparsamkeit bei der Rundfunkfinanzierung 142

18 Entschließung der 60. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 12./13. Oktober 2000 – Vom Bürgerbüro zum Internet – Empfehlungen zum Datenschutz für eine serviceorientierte Verwaltung 142

19 Entschließung der 60. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 12./13. Oktober 2000 – Auftragsdatenverarbeitung durch das Bundeskriminalamt (Umlaufbeschluss) 143

20 Entschließung der 61. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8./9. März 2001 – Äußerungsrecht der Datenschutzbeauftragten 143

21 Entschließung der 61. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8./9. März 2001 – Informationszugangsgesetz 144

22 Entschließung der 61. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8./9. März 2001 – Datenschutz bei der Bekämpfung von Datennetzkriminalität 144

23 Entschließung der 61. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8./9. März 2001 – Novellierung des G 10-Gesetzes 145

24 Entschließung der 61. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8./9. März 2001 – Novellierung des Melderechtsrahmengesetzes 146

25 Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 12. März 2001 – Anlasslose DNA-Analyse aller Männer verfassungswidrig 147

26 Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 10. Mai 2001 – Entwurf der Telekommunikations-Überwachungsverordnung 147

27 Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 24. April 2001 – Umlaufbeschluss – Veröffentlichung von Insolvenzinformationen im Internet 148

28 Entschließungen der 47. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 9./10. März 1994 zu Chipkarten im Gesundheitswesen (A) und der 50. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 9./10. Oktober 1995 zu den datenschutzrechtlichen Anforderungen an den Einsatz von Chipkarten im Gesundheitswesen (B) 149

29 Entschließung der Europäischen Kommission vom 27. Juli 2000 zum Datentransfer in die USA, Grundsätze des „Sicheren Hafens“ zum Datenschutz 152

30 Orientierungshilfe des LfD vom 16. November 2000 „Zugriffsberechtigungen der kommunalen Behördenleitungen“ 159

31 LfD- Entwurf eines Musterantrags auf Einrichtung einer Übermittlungssperre 160

32 Entschließung des Sondertreffens der Datenschutzbeauftragten des Bundes und der Länder zur Terrorismusbekämpfung vom 1. Oktober 2001 161

Abkürzungen

ABl.	Amtsblatt
AO	Abgabenordnung
AOK	Allgemeine Ortskrankenkasse
BDSG	Bundesdatenschutzgesetz
BeamtVG	Beamtenversorgungsgesetz
BfD	Bundesbeauftragter für den Datenschutz
BFH	Bundesfinanzhof
BGB	Bürgerliches Gesetzbuch
BGBl.	Bundesgesetzblatt
BGH	Bundesgerichtshof
BKA	Bundeskriminalamt
BKAG	Bundeskriminalamtgesetz
BOKraft	Verordnung über den Betrieb von Kraftunternehmen im Personenverkehr
BSHG	Bundessozialhilfegesetz
BSI	Bundesamt für Sicherheit in der Informationstechnik
BVerwG	Bundesverwaltungsgericht
BVG	Bundesversorgungsgesetz
BVerfGE	Sammlung der Entscheidungen des Bundesverfassungsgerichts
BZRG	Bundeszentralregistergesetz
DIZ	Daten- und Informationszentrum Rheinland-Pfalz
DNA	Desoxyribonuclein acid (acid = Säure)
DNA-IFG	DNA-Identitätsfeststellungsgesetz
Drs.	Drucksache
EG	Europäische Gemeinschaften
EGG	Elektronischer Geschäftsverkehr-Gesetz
EGV	Vertrag über die Europäische Gemeinschaft
EU	Europäische Union
EuGH	Europäischer Gerichtshof
EUROPOL	Zentrales Europäisches Kriminalpolizeiamt
EWOIS	Einwohnerinformationssystem
FahrlG	Fahrlehrergesetz
FeV	Fahrerlaubnis-Verordnung
ff.	(fort-)folgende
FÜV	Fernmeldeüberwachungsverordnung
G10	Gesetz zu Artikel 10 GG
GemO	Gemeindeordnung
GewO	Gewerbeordnung
GEZ	Gebühreneinzugszentrale der öffentlich-rechtlichen Rundfunkanstalten in der Bundesrepublik Deutschland
GG	Grundgesetz
ggf.	gegebenenfalls
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
i. V. m.	in Verbindung mit
JVA	Justizvollzugsanstalt
KAG	Kommunalabgabengesetz
KAN	Kriminalaktennachweis
KBA	Kraftfahrtbundesamt
KfSachvG	Kraftfahrsachverständigengesetz
KpS	Kriminalpolizeiliche personenbezogene Sammlungen – Kriminalakten –
KunstUrhG	Kunsturhebergesetz
KV	Kassenärztliche Vereinigung
LAbfWAG	Landesabfallwirtschafts- und Altlastengesetz
LArchG	Landesarchivgesetz
LBG	Landesbeamtengesetz
LDKN	Landesdaten- und Kommunikationsnetz Rheinland-Pfalz
LDSG	Landesdatenschutzgesetz
LfD	Landesbeauftragter für den Datenschutz
LG	Landgericht
lit.	littera (Buchstabe)
LKA	Landeskriminalamt
LKG	Landeskrankenhausgesetz
LKRG	Landesgesetz zur Weiterführung des Krebsregisters
LPersVG	Landespersonalvertretungsgesetz
LPR	Landeszentrale für private Rundfunkveranstalter
LRG	Landesrundfunkgesetz
LSG	Landessozialgericht
LV	Landesverfassung für Rheinland-Pfalz
LVA	Landesversicherungsanstalt
LWG	Landeswahlgesetz
MDK	Medizinischer Dienst der Krankenversicherung
MeldDÜVO	Meldedatenübermittlungsverordnung
MG	Meldegesetz
MRRG	Melderechtsrahmengesetz
n. F.	neue Fassung
NJW	Neue Juristische Wochenschrift
OFD	Oberfinanzdirektion
ÖGdG	Landesgesetz über den öffentlichen Gesundheitsdienst
OLG	Oberlandesgericht
OVG	Oberverwaltungsgericht
PBefG	Personenbeförderungsgesetz
PC	Personalcomputer
POG	Polizei- und Ordnungsbehördengesetz
POLIS	Polizeiliches Informationssystem Rheinland-Pfalz
PStG	Personenstandsgesetz
PsychKG	Landesgesetz für 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
StatRegG	Statistikregistergesetz
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
StVÄG	Strafverfahrensänderungsgesetz
StVG	Straßenverkehrsgesetz
StVollzG	Strafvollzugsgesetz
StVZO	Straßenverkehrs-Zulassungsordnung
Tb.	Tätigkeitsbericht
TDDSG	Teledienstedatenschutzgesetz
TDG	Teledienstegesetz
TDSV 1996	Telekommunikationsdienstunternehmen-Datenschutzverordnung
TDSV 2000	Telekommunikations-Datenschutzverordnung
TKG	Telekommunikationsgesetz
TKÜV	Telekommunikations-Überwachungsverordnung (Entwurf)
TÜV	Technischer Überwachungsverein
Tz.	Textziffer
u. a.	unter anderem
UIG	Umweltinformationsgesetz
USG	Unterhaltssicherungsgesetz
u. U.	unter Umständen
VG	Verwaltungsgericht
VGH	Verwaltungsgerichtshof
VwVfG	Verwaltungsverfahrensgesetz
ZEVIS	Zentrales Verkehrsinformations-System
ZfStrVo	Zeitschrift für Strafvollzug und Straffälligenhilfe
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.
ADABAS/Natural	Ein – überwiegend im Großrechnerbereich eingesetztes – Verfahren zur Verwaltung und Auswertung von in einer Datenbank gespeicherten Informationen (siehe auch *Relationales Datenbanksystem*).
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 Microsoft 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-Attack	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-Attack 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.
DICOM	Im Bereich der Medizin genutztes Kommunikationsprotokoll für die Übertragung von Radiologiedaten.
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.
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.*
Elektronische 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.
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, welche 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.
FTP	File Transfer Protocol. Speziell auf die Übertragung von Datenbeständen ausgerichtetes Kommunikationsprotokoll aus der Familie der Internet-Protokolle.
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.
HTTP	Hypertext Transfer Protocol. Internet-Protokoll zur Darstellung vom *HTML*-Seiten via *Browser*.
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*.

IP-Protokoll	Kommunikationsprotokoll im Internet. Die Datenübertragung erfolgt dabei in einzelnen Paketen, deren Absender und Empfänger durch *IP-Adressen* gekennzeichnet werden.
IPSec-Protokoll	Erweiterung des IP-Protokolls um Funktionen zur Sicherung der Vertraulichkeit und Integrität der Kommunikation.
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.
Kompilierung	Vorgang zur Umwandlung des Quellcodes eines Programms in *Maschinencode*, den Befehlssatz des jeweiligen Prozessors.
Krypto-Box	Komponente, die entsprechend voreingestellter Parameter für eine Kommunikationsverbindung eine kryptografische Absicherung gewährleistet. Sie erfordert empfängerseitig eine entsprechende Gegenstelle. Kryptoboxen machen benutzerseitige Eingriffe für eine Verschlüsselung oder Integritätssicherung i. d. R. entbehrlich.
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.
LDKN	Das vom Daten- und Informationszentrum betriebene Landesdaten- und Kommunikationsnetz Rheinland-Pfalz (siehe auch *rlp-Netz*).
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.
Maschinencode	Die im Rahmen der *Kompilierung* aus dem Quellcode erzeugten und an den Befehlssatz des jeweiligen Prozessors angepassten binären Programmbefehle.
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.
OCR	Optical Character Recognition. Verfahren zur automatisierten Erkennung und Erfassung von Texten.
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.
PKI	Public Key Infrastructure. Gesamtheit der für die Verwendung von *Public Key*-Verfahren erforderlichen Komponenten und Dienste (u. a. Schlüsselerzeugung, Zertifizierungs-, Verzeichnis-, Sperr- und Zeitstempeldienste).
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.
Quellcode	Der in einer Programmiersprache vorliegende, noch nicht in Maschinencode umgewandelte Programmcode (vgl. *Kompilierung*). Quellcodeanweisungen ermöglichen aufgrund der im Vergleich zum *Maschinencode* höheren Abstraktionsebene grundsätzlich eine Analyse der jeweiligen Programmbefehle.
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.
rlp-netz	siehe *LDKN.*
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-Attack*).
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.
Tunneling	Verfahren zur Absicherung einer Datenübertragung über unsichere oder nicht vertrauenswürdige Kommunikationsverbindungen mit Hilfe kryptografischer Verfahren.
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	*Server*dienst, 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 *World Wide Web.*
World 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 *World 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
17.	Tätigkeitsbericht	Drucksache 13/4836	vom	18. Oktober 1999

1. Vorbemerkung

1.1 Schwerpunkte des Datenschutzes in den letzten zwei Jahren

Der Datenschutz ist im Berichtszeitraum erneut von den fortschreitenden technischen Entwicklungen und Möglichkeiten geprägt worden:

Das Internet hat eine Verbreitung sowohl bei den Bürgern wie bei den Verwaltungen gefunden, deren Umfang vor zwei Jahren in dieser Form kaum absehbar war; derzeit lauten Schätzungen, dass 15 Millionen Personen Internet-Anschlüsse nutzen. Vor zwei Jahren lag die entsprechende Zahl bei vier Millionen. Mit der Internet-Nutzung ist eine Vielzahl datenschutzrechtlicher Fragen verbunden, die in diesem Bericht näher dargestellt werden, beginnend bei den medienrechtlichen Fragen, welche Datenspuren durch gewerbliche oder sonstige Anbieter von Internet-Dienstleistungen zu deren eigenen Zwecken gespeichert werden dürfen, über die Frage, welche Datenspuren diese Anbieter im Interesse der Strafverfolgungsbehörden speichern müssen, bis zu dem Problem, welche Selbstschutzmöglichkeiten die Internet-Nutzer haben, um sich vor ungewollten Datenerfassungen zu schützen. Auch die Sicherheit des E-Mail-Verkehrs für den Nutzer ist ein wesentlicher Diskussionspunkt; hierbei sind die Fragen der Verschlüsselung von besonderer Bedeutung. Der Einsatz der Internet-Dienste für Verwaltungszwecke (unter dem Stichwort „e-government", s. Tz. 18.1) ist ein weiterer wichtiger aktueller Diskussionspunkt. Hier stehen Fragen nach der Sicherheit der Kommunikationswege zwischen Bürger und Verwaltung (Stichwort: elektronische Signatur) und nach gleichen Teilhabemöglichkeiten aller Bürger an den damit gegebenen Möglichkeiten (Stichwort: „digital divide") im Vordergrund.

Die technische Entwicklung bildet aber auch den maßgeblichen Hintergrund für die Diskussion um die Novellierung des allgemeinen Datenschutzrechts (s. Tz. 2.1). Auf der Ebene des Bundes ist in diesem Zusammenhang ein wichtiger Zwischenschritt mit der Anpassung des Bundesdatenschutzgesetzes an die europäische Datenschutzrichtlinie erreicht worden. Auf der Ebene des Landes stehen wir vor einem vergleichbaren Ergebnis, wobei in einigen Details aus datenschutzrechtlicher Sicht Verbesserungen gegenüber dem Bundesgesetzentwurf zu konstatieren sind. Eine grundlegendere Anpassung des allgemeinen Datenschutzrechts an den Fortschritt der technischen Entwicklung bleibt auf der Tagesordnung: Die „zweite Stufe der Novellierung des BDSG" steht dafür als Stichwort. Inhaltlich geht es um die Einführung neuer Instrumente im Datenschutzrecht wie „Selbstdatenschutz" und „Datenschutzaudit".

Auch die Diskussion um den Einsatz der Data Warehouse-Technik beruht auf dem rasanten Fortschritt der Datenverarbeitungstechnik. Die Begriffe „Data Warehouse" und „Data Mining" stehen für die Analyse der Gesamtheit aller verfügbaren Daten zu einer Person und ihren Beziehungen zu anderen, um den Besitzern des „Data Warehouse" oder des „Daten-Bergwerks" ein aussagefähiges Gesamtbild über eine bestimmte Person zu liefern. Der Einsatz derartiger Datenverarbeitungsverfahren in der öffentlichen Verwaltung ist am Grundrecht auf informationelle Selbstbestimmung jedes Einzelnen zu messen; die Grundsätze der Zweckbindung und Erforderlichkeit der personenbezogenen Datenverarbeitung lassen ihren Einsatz nur in Grenzen zu. Bei rheinland-pfälzischen öffentlichen Stellen sind Ansätze eines konkreten Einsatzes dieser Technik allerdings ausschließlich im Sparkassenbereich zu konstatieren (s. Tz. 22.6).

Die rasante Entwicklung der Biotechnologie ist Hintergrund der aktuellen datenschutzrechtlichen Diskussionen um die Gefahren gentechnischer Untersuchungen. In diesem Zusammenhang haben sich eine Reihe von neuen Fragen gestellt, die der Gesetzgeber noch nicht eindeutig beantwortet hat (s. auch Tz. 5.6 und 7.7).

Nach wie vor spielt die Frage der Videoüberwachung öffentlicher Straßen und Plätze eine große Rolle. Dieses Thema ist als ein weiterer Schwerpunkt der letzten beiden Jahre zu betrachten (s. Tz. 5.8, 6.3, 8.2.6 und 18.2).

Daneben gibt es eine Vielzahl von datenverarbeitungstechnischen Entwicklungen in unterschiedlichsten Bereichen, die den Datenschutz vor immer neue Herausforderungen gestellt haben. Stichwortartig seien genannt

- die Entwicklungen bei der Automatisierung der Justizregister und deren Anbindung an das Internet (s. Tz. 7.8);
- die Neuentwicklung des zentralen polizeilichen Informationssystems auf der Ebene des Bundeskriminalamts, an dem die Länder maßgeblich beteiligt sind (INPOL-neu, s. Tz. 5.3), sowie die hiermit zusammenhängende umfassende DV-Ausstattung der Polizei;
- das Projekt der Neuentwicklung des landesweiten Einwohnerinformationssystems (EWOIS-neu, s. Tz. 4.1 und 21.2.1).

Schließlich ist erkennbar, dass die Frage der Privatisierung staatlicher Datenverarbeitungen in allernächster Zeit in unserem Bundesland eine neue Qualität erhalten wird: Nicht nur die Meldedatenverarbeitung, die gesamte bislang vom DIZ verantwortete Datenverarbeitung steht hinsichtlich ihrer Privatisierung zur Diskussion.

Entsprechend der Zuweisung nach § 2 des Landesgesetzes über die Errichtung des Daten- und Informationszentrums Rheinland-Pfalz nimmt das DIZ wesentliche Aufgaben im Zusammenhang mit dem Einsatz von Informationstechnik in der Landesverwaltung wahr. Hierzu zählen der Betrieb des LDKN sowie zentraler Verfahren. Als öffentlich-rechtliche Anstalt des Landes unterliegt das DIZ dabei unmittelbar der Aufsicht des fachlich zuständigen Ministeriums sowie der Datenschutzkontrolle durch den LfD.

Vor dem Hintergrund sich ändernder IT-Strukturen werden gegenwärtig Überlegungen angestellt, bislang vom DIZ als Anstalt erbrachte Aufgaben auf Stellen in privater Rechtsform auszulagern. In welchem Umfang diese in der Hand des Landes verbleiben und damit unmittelbare Einwirkungsmöglichkeiten erhalten bleiben, ist dabei offen. Die mit einer Verlagerung auf nichtöffentliche Stellen u. U. verbundene Einschränkung von Aufsichts- und Kontrollmöglichkeiten kann durch vertragliche Vereinbarungen meist nur bedingt kompensiert werden.

Die für die datenschutzrechtliche Beurteilung solcher Vorhaben maßgebenden datenschutzrechtlichen Gesichtspunkte hat der LfD bereits in seinem 17. Tb. (Tz. 14.6 und 14.7) deutlich gemacht. Inwieweit gegenwärtig vom DIZ wahrgenommene Aufgaben für eine entsprechende Verlagerung in Betracht kommen, bedarf aus Sicht des LfD daher sorgfältiger Überlegungen. Nach seiner Auffassung sind IT-Aufgaben mit wesentlicher Bedeutung im Rahmen hoheitlicher Tätigkeiten grundsätzlich durch öffentliche Stellen zu erbringen. Insbesondere gilt dies für die Bereiche Polizei, Justiz und Steuerverwaltung.

1.2 Bewertung

Zwar ist festzustellen, dass all diese Entwicklungen mit datenschutzrechtlichen Gefährdungen der betroffenen Bürger einhergehen. Insgesamt ist aber die rechtliche Bindung dieser Entwicklungen wirksam und in weitem Umfang bestehen auch technische und organisatorische Vorkehrungen gegen missbräuchliche Datennutzungen. Bei allen faktischen Defiziten in der Kontrolle und der Transparenz vieler Verfahren besteht kein Anlass, davon auszugehen, dass das Persönlichkeitsrecht der Bürgerinnen und Bürger derzeit weniger wirksam geschützt wäre als in der Vergangenheit. Im Land ist besonders zu betonen, dass die vielfältigen Beratungsaktivitäten im Vorfeld von Neuentwicklungen häufig zu Verbesserungen im Sinne des Datenschutzes geführt haben. Dies konnte mit überschaubarem materiellen Aufwand erreicht werden und belegt die Wirksamkeit des Datenschutzgedankens in der Verwaltung, aber auch die Notwendigkeit der Begleitung solcher Entwicklungen durch eine unabhängige externe Stelle wie den LfD.

Diese Aussage beschränkt sich allerdings auf das Verhältnis zu den staatlichen Stellen. Die zunehmende Nutzung der elektronischen Kommunikationsmittel ermöglicht es den daran beteiligten und dafür verantwortlichen privaten Stellen (den Netzbetreibern, Providern etc.) und möglicherweise auch nichtbeteiligten Dritten („Hackern"), Verhaltens- und Interessenprofile der nutzenden Bürger in großem Umfang zu verwerten. Diese Gefahren sind unleugbar, denn die Situation ist nur schwer überschaubar. Allerdings sollte diese für den einzelnen Nutzer, aber auch für die Kontrollbehörden bestehende Undurchsichtigkeit des technisch Möglichen nicht zu irrationalen Ängsten führen. Das adäquate Gegenmittel ist nicht die Technikverweigerung oder der Maschinensturm, sondern der effektive Selbstschutz durch Nutzung beispielsweise von Verschlüsselung, pseudonymen Kommunikationsformen und sonstigen Maßnahmen des „Selbstdatenschutzes" (vgl. 17. Tb., Tz. 19.1). Festzuhalten bleibt nämlich auch, dass trotz des Schreckensszenarios der grundsätzlichen negativen Möglichkeiten der modernen Kommunikationstechnik konkrete Erkenntnisse über tatsächlich erfolgte Datenmissbräuche nur für wenige Einzelfälle vorliegen.

1.3 Ausblick

Seit dem 11. September 2001 haben sich auch die für den Datenschutz maßgeblichen außerrechtlichen Paradigmen gewandelt. Der bloße Zweifel an der Wirksamkeit staatlicher Datensammlungen reicht nicht mehr aus, um bestimmte der Sicherheit dienende Vorhaben der Sicherheitsbehörden abzulehnen. Die weithin grassierende Unsicherheit über das tatsächlich in Deutschland bestehende terroristische Zerstörungspotential und die konkreten Pläne solcher Kräfte machen es schwer zu beurteilen, welche staatlichen Maßnahmen noch verhältnismäßig, welche dagegen als übermäßig und unangemessen freiheitsschädigend anzusehen sind.

Über diese Bewertungen muss aber weiter gestritten werden können. Dies zeichnet den freiheitlichen Rechtsstaat aus. Als unnötig erkannte gesetzlich geregelte Freiheitsbeschränkungen müssen wieder rückgängig gemacht werden. Hierfür müssen Prüffristen vorgesehen werden. Für einen rationalen Diskurs auch unter den Bedingungen terroristischer Bedrohung und für einen optimalen Ausgleich der widerstreitenden Rechtsgüter wird sich der LfD künftig ebenso wie bislang einsetzen. Die Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 1. Oktober 2001 (s. Anlage 32), der der LfD in vollem Umfang zugestimmt hat, bringt dieses Anliegen ebenfalls deutlich zum Ausdruck.

2. Weiterentwicklung des Datenschutzrechts

2.1 Entwicklung des allgemeinen Datenschutzrechts: Novellierung des Bundesdatenschutzgesetzes sowie des Landesdatenschutzgesetzes

Die in den vergangenen Tätigkeitsberichten angesprochene Notwendigkeit, das nationale Datenschutzrecht an die EG-Datenschutzrichtlinie (Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, Amtsblatt der Europäischen Gemeinschaften Nr. L 281 vom 23. November 1995, S. 31, zuletzt geändert am 8. Februar 1997) anzupassen, hat im Berichtszeitraum zu Ergebnissen geführt: Das Bundesdatenschutzgesetz ist mit Gesetz vom 26. Juni 2001 an die EG-Datenschutzrichtlinie angepasst worden (BGBl. I S. 1254). Dem dienen insbesondere Regelungen über:

- Vorabkontrolle vor der Einführung neuer automatisierter DV-Systeme,
- besonderer Schutz von besonders sensiblen Daten (über weltanschauliche und religiöse Überzeugungen, sexuelle Orientierungen, gesundheitliche Verhältnisse etc.),
- Widerspruchsrecht Betroffener gegen ausnahmsweise im Einzelfall unverhältnismäßige Datenverarbeitungen,
- Erleichterung der grenzüberschreitenden Datenübermittlungen in EG-Partnerländer,
- Erweiterung von Auskunftsrechten Betroffener.

Darüber hinaus sind Regelungen zur Videoüberwachung (§ 6 b BDSG) sowie zum Chipkarteneinsatz (§ 6 c BDSG) getroffen worden. Weiter gehende datenschutzrechtliche Anliegen (z. B. Einführung eines Datenschutzaudits, Regelungen zum Selbstdatenschutz) sollen in einer zweiten Stufe realisiert werden. Zu diesem Zweck erfolgen intensive Diskussionen zwischen Sachverständigen und Politikern. Die Regierungsfraktionen haben einen Beirat einberufen, in dem diese Erörterungen unmittelbar auch zu gesetzgeberischen Vorschlägen führen sollen. Der LfD ist Mitglied dieses Beirats und hat regelmäßig an entsprechenden Sitzungen teilgenommen.

Auf der Ebene des Landes liegt nunmehr ein Referentenentwurf für eine Novellierung des Landesdatenschutzgesetzes vor, der demnächst in den Landtag eingebracht werden soll. Der LfD hat hierzu umfassend Stellung genommen und insbesondere den Gesichtspunkt betont, dass im Interesse der Normenklarheit auch vom Vorbild des Bundesgesetzes abgewichen werden sollte. In den Detaildiskussionen ist es gelungen, auch in den Einzelfragen weitgehend Übereinstimmung zu erzielen, so dass der jetzt vorliegende Entwurf grundsätzlich auf Zustimmung des LfD trifft. Allerdings betont der LfD folgendes Anliegen, das im Gesetzentwurf nicht berücksichtigt worden ist: Es sollte klargestellt werden, dass die Gerichte nur insoweit von den allgemein geltenden Regelungen ausgenommen werden, wie dies zur Wahrung der richterlichen Unabhängigkeit erforderlich ist (Näheres hierzu s. unter Tz. 7.1).

Besonders hervorzuheben sind die für den Chipkarteneinsatz sowie die Videoüberwachung durch öffentliche Stellen des Landes vorgesehenen Regelungen, durch die – in gleichem Sinne wie dies auf der bundesgesetzlichen Ebene erfolgt ist – Neuland betreten wird und deren Bewährung in der Praxis auch vom LfD kritisch begleitet werden wird.

2.2 Zur optimalen Organisation der Datenschutzkontrolle

Im Rahmen von Anhörungen ist der LfD gegenüber dem nordrhein-westfälischen und gegenüber dem hessischen Landtag bei der Novellierung der jeweiligen Landesdatenschutzgesetze gutachtlich tätig geworden und hat Stellungnahmen abgegeben. Dabei stand jeweils die Frage im Zentrum des Interesses, ob die Aufhebung der gespaltenen Datenschutzkontrolle zwischen öffentlich-rechtlichen und privaten datenverabeitenden Stellen wünschenswert oder vielleicht sogar rechtlich geboten sei.

Er hat sich hierzu ausführlich in dem Sinn geäußert, dass eine Änderung des gegenwärtig in Rheinland-Pfalz bestehenden Rechtszustandes nicht geboten sei, dass vielmehr verfassungsrechtliche Gründe eine solche Zusammenlegung schwierig machen und dass im Ergebnis weder rechtliche noch praktische Gründe diese erzwingen. Im Gegenteil: Insgesamt befürwortet der LfD eine Beibehaltung der gegenwärtigen Organisation der Datenschutzkontrolle, da sie allein geeignet ist, die völlige Unabhängigkeit der Datenschutzkontrolle im öffentlichen Bereich von den zu kontrollierenden Stellen, insbesondere auch im Bereich des hoheitlichen Handelns des Staates, wo sie von besonderer Bedeutung ist, im Interesse eines wirksamen Grundrechtsschutzes zu gewährleisten.

2.3 Erlass eines „Informationsfreiheitsgesetzes“

Bislang ist in Rheinland-Pfalz noch keine Gesetzesinitiative mit dem Ziel der Schaffung eines Informationsfreiheitsgesetzes ersichtlich, wie es in einigen Bundesländern (Berlin, Brandenburg, Schleswig-Holstein) existiert. Allerdings wird auf der Ebene des Bundes ein entsprechender Referentenentwurf diskutiert, zu dem der LfD von Journalisten und auch von interessierten Bürgern um Stellungnahme gebeten wurde. Auf entsprechende Anfragen hin hat er sich wie folgt geäußert:

Anliegen des Datenschutzes ist die Wahrung des Grundrechts auf Datenschutz, des informationellen Selbstbestimmungsrechts des Einzelnen. In diesem Zusammenhang hat der Auskunftsanspruch des Betroffenen gegenüber staatlichen Stellen eine besondere Bedeutung. Dieser Auskunftsanspruch ist in den geeigneten Fällen durch Gewährung von Akteneinsicht zu erfüllen.

Die Informationsfreiheitsgesetze haben demgegenüber nicht die Stärkung des Grundrechts auf Datenschutz bzw. des informationellen Selbstbestimmungsrechts des Betroffenen zum Ziel. Ihre Zielrichtung ist vielmehr Herstellung von Transparenz der Verwaltung sowie u. a. die Verstärkung der Teilhabe des Bürgers am demokratischen Meinungs- und Willensbildungsprozess.

Diese Anliegen unterstützt der LfD – unabhängig von den ihm gesetzlich zugewiesenen Aufgaben – grundsätzlich, wobei allerdings auch mögliche nachteilige Wirkungen allgemeiner Akteneinsichtsregelungen für jedermann auf Verwaltungseffizienz und Verfahrensbeschleunigung zu untersuchen und zu bewerten sind. Eine unmittelbare Verknüpfung dieser Ziele mit seinen amtlichen Aufgaben als unabhängigem Wächter über das Datenschutzgrundrecht ist für ihn – im Gegensatz zu einigen seiner Kollegen in den anderen Ländern – nicht ersichtlich.

Unbestreitbar ist, dass die Informationsansprüche aus einem Informationsfreiheitsgesetz mit Datenschutzgrundrechten Betroffener kollidieren können. Wie bei anderen Rechtskollisionen kommt es dann darauf an, durch gesetzliche Formulierungen und durch die Beachtung des Verhältnismäßigkeitsgrundsatzes in der Verwaltungspraxis eine Konkordanz herzustellen. Dabei wäre im Gesetzesvollzug sicher auch der Datenschutzbeauftragte gefordert.

Zusammenfassend ist festzustellen, dass aus datenschutzrechtlicher Sicht keine zwingenden Einwände grundsätzlicher Art gegen die Verabschiedung eines Informationsfreiheitsgesetzes bestehen. In diesem Sinn hat sich auch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder in einer Entschließung geäußert (s. Anlage 21).

3. Datenschutz in Europa

3.1 Die Umsetzung der EG-Datenschutzrichtlinie

Seit dem 13. Tb. vom 16. Dezember 1991 hat der LfD über wichtige datenschutzrechtliche Entwicklungen in der Europäischen Union berichtet. Schwerpunkt war stets die EG-Datenschutzrichtlinie (vgl. 14. Tb., Tz. 3; 15. Tb., Tz. 3.1; 16. Tb., Tz. 3.1 und 3.2; 17. Tb., Tz. 3.1, 3.2 und 3.3), deren dreijährige Umsetzungsfrist in deutsches Recht im Oktober 1998 ablief. Wegen der mangelnden Umsetzung der Richtlinie in Deutschland und vier weiteren EU-Staaten (Frankreich, Luxemburg, Niederlande, Irland) hatte die Europäische Kommission im Januar 2000 den Europäischen Gerichtshof angerufen. Zwischenzeitlich ist es im Mai 2001 – wohl nicht zuletzt unter dem Druck dieses Zwangsverfahrens – zu einer Umsetzung durch die Novellierung des Bundesdatenschutzgesetzes gekommen (vgl. dazu Tz. 2.1).

Auch in Rheinland-Pfalz ist nunmehr die Anpassung des Landesdatenschutzgesetzes, die – in Übereinstimmung mit dem LfD – wegen der möglichst weit gehenden inhaltlichen Übereinstimmungen mit den Bestimmungen des Bundesdatenschutzgesetzes zurückgestellt wurde, auf den Weg gebracht worden (s. Tz. 2.1).

3.2 Anwendung der Datenschutzvorschriften durch die Organe und Einrichtungen der Gemeinschaft durch Verordnung geregelt

Die durch den Amsterdamer Vertrag neu in das Gemeinschaftsrecht aufgenommene Vorschrift des Art. 286 EGV hat den Datenschutz gegenüber Gemeinschaftsorganen und -einrichtungen auf primärrechtlicher Ebene verankert.

Neben einer weiteren Konkretisierung der Datenschutzverpflichtungen stand daher vor allem die Schaffung einer unabhängigen Kontrollinstanz in der Form eines Europäischen Datenschutzbeauftragten an.

Das Europäische Parlament und der Ministerrat haben nun eine Verordnung zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr verabschiedet. Die genaue Bezeichnung lautet: Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr (ABl. L 8 vom 12. Januar 2001).

Zum Hintergrund: Die Organe und Einrichtungen der Gemeinschaft, und insbesondere die Kommission, bearbeiten bei der Ausübung ihrer Tätigkeit ständig personenbezogene Daten. Im Rahmen der gemeinsamen Agrarpolitik, der Verwaltung des gemeinschaftlichen Zollsystems und der Strukturfonds und im Zusammenhang mit anderen gemeinschaftsrechtlichen Maßnahmen tauscht die Kommission personenbezogene Daten mit den Mitgliedstaaten aus. Damit diese Datenübermittlungen von den Mitgliedstaaten nicht aus Datenschutzgründen in Frage gestellt wurden, hatte die Kommission bislang lediglich erklärt, dass sie sich ebenfalls an die Grundsätze der Richtlinien 95/46/EG (Richtlinie des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr; ABl. L 281 vom 23. November 1995, S. 31 bis 50) und 97/66/EG (Richtlinie des Europäischen Parlaments und des Rates vom 15. Dezember 1997 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation; ABl. L 024 vom 30. Januar 1998, S. 1 bis 8) halten werde.

Um den Vorgaben des Art. 286 EGV gerecht zu werden, war es erforderlich, den Schutz der Grundrechte und Grundfreiheiten natürlicher Personen, insbesondere den Schutz ihrer Privatsphäre, durch Verordnung sicherzustellen. So legt Artikel 3 fest, dass die Verordnung für alle Organe und Einrichtungen der Gemeinschaft gilt, soweit diese personenbezogene Daten im Rahmen von Tätigkeiten verarbeiten, die ganz oder teilweise in den Anwendungsbereich des Gemeinschaftsrechts fallen. Die Verordnung betrifft die Verarbeitung personenbezogener Daten durch folgende Organe der Gemeinschaft: das Europäische Parlament, den Rat der Europäischen Union, die Europäische Kommission, den Gerichtshof und den Rechnungshof. Ferner ist sie auf weitere durch EG-Vertrag, EGKS-Vertrag und EURATOM-Vertrag geschaffene Einrichtungen anwendbar: die Europäische Zentralbank, die Europäische Investitionsbank, den Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen. Schließlich gilt sie für Einrichtungen, die durch das Sekundärrecht der Gemeinschaft geschaffen wurden: das Europäische Zentrum für die Förderung der Berufsbildung, die Europäische Stiftung zur Verbesserung der Lebens- und Arbeitsbedingungen, die Europäische Umweltagentur, die Europäische Stiftung für Berufsbildung, die Europäische Beobachtungsstelle für Drogen und Drogensucht, die Europäische Agentur für die Beurteilung von Arzneimitteln, das Harmonisierungsamt für den Binnenmarkt, die Europäische Agentur für Sicherheit und Gesundheitsschutz am Arbeitsplatz, das Gemeinschaftliche Sortenamt und das Übersetzungszentrum der Einrichtungen der Union. Die Organe und Einrichtungen, die personenbezogene Daten verarbeiten, sind verpflichtet, den betroffenen Personen zweckdienliche Informationen zur Verfügung zu stellen, so dass sie die ihr durch die Verordnung verliehenen Rechte in Anspruch nehmen kann. So haben diese ein Recht auf Zugang zu den sie betreffenden Daten und auf deren Berichtigung, auf Sperrung und Löschung unter den in der Verordnung vorgesehenen Voraussetzungen; ferner können sie unter bestimmten Bedingungen Widerspruch gegen die Verarbeitung der sie betreffenden Daten einlegen. Die Organe und Einrichtungen der Gemeinschaft dürfen indessen in bestimmten Fällen aus genau definierten Gründen des Allgemeininteresses von einigen dieser Bestimmungen abweichen.

Die Verordnung sieht außerdem die Einsetzung einer unabhängigen Kontrollinstanz, des Europäischen Datenschutzbeauftragten, vor und enthält besondere Garantien, um seine Unabhängigkeit zu gewährleisten. Diese Bestimmungen betreffen insbesondere seine Ernennung und Entlassung, die Dauer seiner Amtszeit und das Verbot, Weisungen entgegenzunehmen. Aufgabe des Datenschutzbeauftragten ist es, die Anwendung der Verordnung sicherzustellen. Darüber hinaus muss jedes Organ und jede Einrichtung der Gemeinschaft zumindest eine Person zum Datenschutzbeauftragten bestellen, der mit dem Europäischen Datenschutzbeauftragten zusammenarbeitet und die Anwendung der Verordnung bei den einzelnen Organen und Einrichtungen sicherstellt.

Damit sind auch die Gemeinschaftsorgane und nicht nur – wie zuvor – die Mitgliedstaaten an den Datenschutz gebunden.

Keine Anwendung findet die Verordnung auf das Europäische Polizeiamt Europol, deren datenschutzrechtliche Pflichten sich unmittelbar aus der Europol-Konvention ergeben. Diese zwischenstaatliche Organisation ist im Rahmen der Zusammenarbeit in den Bereichen Justiz und Inneres (sog. „dritte Säule“) geschaffen worden. Es handelt sich nicht um eine Einrichtung der Gemeinschaft im Sinne von Art. 286 EGV. Ebenso wenig gilt die Verordnung für das durch Titel IV des Schengener Durchführungsübereinkommens errichtete Schengener Informationssystem (Verbleib in der dritten – nicht vergemeinschafteten – Säule).

3.3 Das Grundrecht auf Datenschutz in der Charta der Grundrechte der Europäischen Union

Am 7. Dezember 2000 wurde die Charta der Grundrechte der Europäischen Union vom Rat, Europäischen Parlament und der Kommission in Nizza unterzeichnet.

Mit diesem Akt erlangte die Charta allerdings keine Verbindlichkeit im Recht der Europäischen Union. Vielmehr soll die Möglichkeit der Integration der Charta in das Recht der Europäischen Union im Rahmen der nächsten Regierungskonferenz geprüft werden. Vorerst stellt sie also nur eine politische Deklaration dar. Dennoch wird nach Auffassung des LfD auch die rechtlich unverbindliche Charta das Umfeld von Unionsrecht und nationalem Verfassungsrecht – insbesondere durch die zu erwartende Heranziehung der Grundrechtscharta durch den EuGH – beeinflussen.

Ausweislich der Präambel soll die Charta nichts Neues schaffen, sondern Bestehendes zusammenfassen. So heißt es in Erwägung Nr. 5 der Präambel: „Diese Charta bekräftigt die Rechte, die sich von allen aus den gemeinsamen Verfassungstraditionen der Mitgliedstaaten, aus dem Vertrag über die Europäische Union und aus den Gemeinschaftsverträgen, aus der Europäischen Konvention zum Schutz der Menschenrechte und Grundfreiheiten, aus den von der Gemeinschaft und dem Europarat beschlossenen Sozialchartas der Europäischen Gemeinschaften und des Europäischen Gerichtshofs für Menschenrechte ergeben.“

Ihr Anwendungsbereich ist in Art. 50 Abs. 1 umschrieben: „Diese Charta gilt für die Organe und Einrichtungen der Union unter Einhaltung des Subsidiaritätsprinzips und für die Mitgliedstaaten ausschließlich bei der Durchführung des Rechts der Union.“

Sie enthält im ersten Kapitel („Würde des Menschen“) einige fundamentale Menschenrechte, die in ähnlicher Form in der Europäischen Menschenrechtskonvention enthalten sind. Das Recht auf Schutz personenbezogener Daten (Art. 8 der Charta) ist jedoch nicht der EMRK nachgebildet, sondern der EG-Datenschutzrichtlinie. Die Regelung in Art. 8 verbindet insbesondere neben dem grundsätzlichen Anspruch einzelne Grundsätze des Art. 6 der Richtlinie sowie die in Art. 12 der Richtlinie enthaltenen Ansprüche auf Auskunft und auf Berichtigung von Daten. Die Bestimmung lautet:

„Art. 8 (Schutz personenbezogener Daten)

(1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.

(2) Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Personen oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.

(3) Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht."

Für die Aufnahme des Grundrechts auf Datenschutz in den Europäischen Grundrechtskatalog haben sich die Datenschutzbeauftragten des Bundes und der Länder sowie deren Kolleginnen und Kollegen in den anderen Mitgliedstaaten der Europäischen Union eingesetzt (vgl. z. B. Entschließung vom 8. Oktober 1999, Anlage 3). Auch die gem. Art. 29 der EG-Datenschutzrichtlinie geschaffene Datenschutzgruppe (zu deren Aufgaben s. Tz. 3.6) hatte die Aufnahme eines Grundrechts auf Datenschutz in den Europäischen Grundrechtskatalog empfohlen und hierzu Folgendes ausgeführt:

„Der Europäische Rat hat anlässlich seiner Zusammenkunft am 4. Juni in Köln die Ausarbeitung einer Charta der Grundrechte der Europäischen Union beschlossen. In dem Ratsbeschluss heißt es: Im gegenwärtigen Entwicklungszustand der Union ist es erforderlich, eine Charta dieser Rechte zu erstellen, um die überragende Bedeutung der Grundrechte und ihre Tragweite für die Unionsbürger sichtbar zu verankern.

Die Gruppe, bestehend aus den Datenschutzbeauftragten der Mitgliedstaaten der Europäischen Union, unterstützt nachhaltig die Initiative des Europäischen Rates zur Ausarbeitung einer EU-Charta der Grundrechte. Sie weist darauf hin, dass einige europäische Länder ein Datenschutzgrundrecht in ihre Verfassung aufgenommen haben. In einigen anderen Ländern wurde dem Datenschutz durch die Rechtsprechung Grundrechtsgeltung zuerkannt.

Schließlich bestimmt ein neuer Artikel 286 im Vertrag über die Europäische Union, dass die Rechtsakte der Gemeinschaft zum Datenschutz ab dem 1. Januar 1999 auf die europäischen Organe und Einrichtungen Anwendung finden.

Eine Verankerung des Datenschutzes im Rahmen der europäischen Grundrechte würde diesen Schutz rechtsverbindlich auf die gesamte Union erstrecken und der steigenden Bedeutung des Datenschutzes in der Informationsgesellschaft Rechnung tragen.

Die Gruppe empfiehlt daher der Europäischen Kommission, dem Europäischen Parlament und dem Rat der Europäischen Union, das Grundrecht auf Datenschutz in die Charta der Grundrechte aufzunehmen."

3.4 Der Entwurf einer „Cyber-Crime"-Konvention des Europarates

Die Bekämpfung der Kriminalität im „Cyberspace" bedarf zweifellos einer verbesserten internationalen Zusammenarbeit. So ist der Konventionsentwurf ausgerichtet auf die strafrechtliche Verfolgung von Handlungen, die gegen die Vertraulichkeit, Integrität und Verfügbarkeit von Computersystemen, Netzwerken und Computerdaten sowie den Missbrauch solcher Systeme, Netzwerke und Daten gerichtet sind. Zu diesem Zweck sollen die in der Konvention beschriebenen Handlungen unter Strafe gestellt und den zuständigen Stellen ausreichende Kompetenzen zur effektiven Verfolgung der Straftaten eingeräumt werden. Das Aufspüren, das Ermitteln und die Verfolgung solcher Delikte sollen auf innerstaatlicher wie internationaler Ebene erleichtert werden und Vereinbarungen sollen eine schnelle und verlässliche internationale Kooperation gewährleisten. Der Konventionsentwurf kann nach Art. 36 auch von solchen Staaten unterzeichnet werden, die dem Europarat nicht angehören, aber an der Ausarbeitung des Konventionsentwurfs beteiligt waren. Dies sind die USA, Kanada, Japan und Südafrika. Mittlerweile ist das Vertragswerk angesichts der Komplexität des Themas auf 116 Seiten angeschwollen, wobei zwei Drittel der zuletzt veröffentlichten Version aus Kommentar und Anhang bestehen.

Seit der erstmaligen Veröffentlichung (Version Nr. 19 des Cybercrime-Vertragswerks, das von 1997 an zunächst hinter verschlossenen Türen ausgehandelt wurde) im Mai 2000 wurden allerdings aus dem Kreis der Datenschutzbeauftragten schwer wiegende Einwände gegen die Verabschiedung der Konvention vorgetragen (vgl. Entschließung der DSB-Konferenz vom 8. März 2001, Anlage 22). Ein grundlegender Mangel des Konventionsentwurfs bestand z. B. in dem völligen Fehlen von materiellen Bestimmungen zum Umgang mit personenbezogenen Daten, die bei der Überwachung der Telekommunikation oder dem Zugriff auf Verkehrsdaten anfallen. Die Konvention geriet insgesamt auch dadurch in Schieflage, dass der Entwurf das Schutzniveau, das der Europarat seit seinem Bestehen in Konventionen und Empfehlungen selbst aufgestellt hat, erheblich unterschritt. Hier sind insbesondere die Europäische Menschenrechtskonvention von 1950 und die Konvention Nr. 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten von 1981 zu nennen, aber auch die Empfehlung R (95) 4 über den Schutz personenbezogener Daten im Bereich der Telekommunikationsdienste.

Auch die internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation und die Datenschutzgruppe nach Art. 29 der EG-Datenschutzrichtlinie haben grundsätzliche Kritik an dem Entwurf geäußert. Die umfangreiche Liste von Änderungsbegehren wurde seitens des Europarates jedenfalls offiziell zur Kenntnis genommen. Zum Ende des Berichtszeitraums hin hat das Bundesjustizministerium darauf hingewiesen, dass die Arbeiten an dem Entwurf inzwischen weitergegangen seien und auch zu verschie-

denen Verbesserungen geführt hätten. Die Bundesregierung habe sich dafür eingesetzt, dass die menschen- und grundrechtsrelevanten Prinzipien des internationalen Rechts beachtet würden. Es sei durchgesetzt worden, dass in das Übereinkommen eine Regelung über „Bedingungen und Garantien" aufgenommen wurde, die vorsehe, dass die Ausgestaltung der in den Artikeln 14 ff. geregelten Eingriffsmöglichkeiten dem Recht des jeweiligen Vertragsstaats unterliege. Hier sei sichergestellt, dass unsere rechtsstaatlichen Prinzipien (z. B. Verhältnismäßigkeitsgrundsatz, Interessenabwägung, justizielle Kontrolle) nicht eingeschränkt würden. Auf deutsches Drängen wären zudem ausdrückliche Hinweise auf die Europäische Menschenrechtskonvention aufgenommen worden.

Äußerst bemerkenswert ist nach Auffassung des LfD im Zusammenhang mit den Arbeiten an der „Cyber-Crime"-Konvention die „Mitteilung der Europäischen Kommission über die Schaffung einer sichereren Informationsgesellschaft durch Verbesserung der Sicherheit von Informationsinfrastrukturen und Bekämpfung der Computerkriminalität" (Dokumentenbezeichnung: KOM[2000] 890 endgültig). Danach soll in einem transparenten Verfahren öffentlich ein Diskussionsprozess beginnen, in dem Strafverfolgungsbehörden, Internet-Diensteanbieter, Telekommunikationsbetreiber und Datenschutzbehörden zusammengebracht werden, um ihr gegenseitiges Verständnis und ihre Zusammenarbeit zu fördern mit dem Ziel, das öffentliche Bewusstsein für die Gefährdung durch über das Internet begangene Straftaten zu schärfen, optimale Sicherheitsbedingungen zu schaffen sowie Instrumente und Verfahren für eine wirksame Bekämpfung der Computerkriminalität aufzuzeigen. In dem vorgenannten Dokument weist die Europäische Kommission auf die Notwendigkeit der Berücksichtigung des nach den geltenden EG-Richtlinien im Bereich Datenschutz und Telekommunikation bereits erreichten Schutzes der Privatsphäre gegenüber Abhörmaßnahmen und anderen Befugnissen der Strafverfolgungsbehörden hin. Dabei kommt in Ziff. 5.3 zum Ausdruck, dass auch ein grundsätzliches Recht auf anonymen oder pseudonymen Zugang und entsprechender Nutzung von Netzangeboten anzuerkennen ist.

Der LfD begrüßt den von der Europäischen Kommission in Gang gebrachten Meinungsbildungsprozess, dessen Ziel es sein muss, die Interessen an effektiver Strafverfolgung und an wirkungsvollem Datenschutz zum Ausgleich zu bringen.

3.5 Die Prinzipien des „sicheren Hafens" – USA und EU einigen sich über den Schutz der Privatsphäre

Nach jahrelangen Verhandlungen haben sich die Europäische Kommission und das US-Department für Außenhandel über Richtlinien zum Schutz der Privatsphäre bei Datenexporten geeinigt. Zum Hintergrund: Die EG-Datenschutzrichtlinie soll die Übermittlung personenbezogener Daten innerhalb der Union erleichtern, indem sie ein harmonisiertes Datenschutzniveau in allen Mitgliedstaaten schafft. Der Export personenbezogener Daten in Drittstaaten außerhalb der Europäischen Union ist grundsätzlich nur dann zulässig, wenn im Empfängerland ein angemessenes Datenschutzniveau herrscht.

Die USA haben sich bereit erklärt, die als „Safe Harbour" (sicherer Hafen) bekannten Regeln zu akzeptieren. Daraufhin hat die Kommission die Angemessenheit des Datenschutzniveaus bei solchen Unternehmen in den USA anerkannt, die diese Prinzipien akzeptieren (*Entscheidung der Europäischen Kommission vom 27. Juli 2000; bevor sie eine formelle Entscheidung treffen konnte,* musste die Safe-Harbour-Vereinbarung zunächst von den Mitgliedstaaten in dem Ausschuss nach Art. 31 der EG-Datenschutzrichtlinie befürwortet werden, was Ende Mai 2000 einstimmig erfolgte). Die Europäische Kommission und das US-Handelsdepartment haben in diesem Zusammenhang Leitlinien zum Datenschutz ausgearbeitet. Diese Leitlinien sind u. a. in „Grundsätze zum Datenschutz" und „Antworten auf häufig gestellte Fragen" (Frequently Asked Questions – FAQ) gefasst. Um die hier vorhandene Themenvielfalt darzustellen, wurden die erwähnten Grundsätze und eine Auswahl der Antworten auf häufig gestellte Fragen als Anlage 29 aufgenommen.

Die Kommissionsentscheidung ist für alle Mitgliedstaaten bindend. Gem. Art. 25 Abs. 6 Satz 2 der EG-Datenschutzrichtlinie treffen die Mitgliedstaaten die aufgrund der Feststellung der Kommission gebotenen Maßnahmen. Auch in Rheinland-Pfalz wirkt sich also diese Entscheidung aus. So muss sichergestellt werden, dass personenbezogene Daten nur dann von Behörden (oder Unternehmen) in die USA übermittelt werden, wenn gewährleistet ist, dass sie dort im „sicheren Hafen" ankommen, also keinem geringeren Schutz unterliegen als in ihrem Ursprungsland. Soweit bekannt, akzeptieren bislang nur wenige Organisationen in den USA diese Grundsätze.

Es bleibt abzuwarten, ob die Safe-Harbour-Lösung mit ihrem gegenwärtigen Datenschutzkonzept Bestand haben wird. So enthält Art. 4 der Kommissionsentscheidung eine Überprüfungsklausel, die es ermöglicht, dass die Feststellung der Angemessenheit des Schutzniveaus im Lichte der Erfahrungen und der US-Gesetzgebung angepasst werden kann. Gem. Art. 4 Ziff. 1 Satz 2 der Entscheidung nimmt die Kommission in jedem Fall nach drei Jahren eine Bewertung der Umsetzung der Kommissionsentscheidung vor. Falls sich herausstellen sollte, dass eine der in den USA für die Einhaltung der Datenschutzgrundsätze zuständigen Kontrolleinrichtungen ihrer Aufgabe nicht wirkungsvoll nachkommt, könnte die Kommission, soweit erforderlich, gemäß dem Verfahren nach Art. 31 der EG-Datenschutzrichtlinie Maßnahmen zur Aufhebung, Aussetzung oder zur Beschränkung des Geltungsbereichs der Safe-Harbour-Entscheidung vorschlagen. Es besteht also die Möglichkeit, die Feststellung der Angemessenheit des Datenschutzniveaus auf diesem Wege zu revidieren.

3.6 Die „Artikel 29-Gruppe"

Immer häufiger ist in Bezug auf aktuelle datenschutzrechtliche Themen (vgl. z. B. die Beiträge in Tz 3.5 – „Sicherer Hafen" und Tz 3.3 – Grundrechtecharta –) von einer „Artikel 29-Gruppe" die Rede. Diese auf der Grundlage von Art. 29 der EG-Datenschutzrichtlinie geschaffene Datenschutzgruppe bildet keine den nationalen Kontrollstellen übergeordnete Instanz, da Europäische Kommission und Rat bewusst auf jede supranationale Intervention in die nationale Kontrolltätigkeit verzichtet haben. Sie stellt

aber die Verbindung zwischen einer unverändert nationalen Kontrolle und der in der Richtlinie zum Ausdruck gebrachten überstaatlichen Verantwortung einen wirksamen Datenschutz her (s. Dammann/Simitis, EG-Datenschutzrichtlinie, Kommentar, Baden-Baden 1997, Einleitung RdNr. 41).

Die Gruppe setzt sich gem. Art. 29 Abs. 2 aus je einem Vertreter der Kontrollstellen der Mitgliedstaaten zusammen. Der Gruppe sind nach Art. 30 Abs. 1 folgende Aufgaben übertragen:

- alle Fragen im Zusammenhang mit den zur Umsetzung der Richtlinie erlassenen einzelstaatlichen Vorschriften zu prüfen, um zu einer einheitlichen Anwendung beizutragen,
- zum Schutzniveau in der Gemeinschaft und in Drittländern gegenüber der Kommission Stellung zu nehmen,
- die Kommission bei jeder Vorlage zur Änderung der EG-Datenschutzrichtlinie, zu allen Entwürfen zusätzlicher oder spezifischer Maßnahmen zur Wahrung der Rechte und Freiheiten natürlicher Personen bei der Verarbeitung personenbezogener Daten sowie zu allen anderen Entwürfen von Gemeinschaftsmaßnahmen zu beraten, die sich auf diese Rechte und Freiheiten auswirken, und
- Stellungnahmen zu den auf Gemeinschaftsebene erarbeiteten Verhaltensregeln abzugeben.

Ihre Beratungsergebnisse hat die Gruppe der Öffentlichkeit in sog. „Arbeitspapieren" zugänglich gemacht, die über die Website der Europäischen Kommission (www.europa.eu.int/comm/dg15) abrufbar sind.

3.7 Zugang der Öffentlichkeit zu Dokumenten

Auf der Grundlage der Verordnung (EG) Nr. 1049/2001 vom 30. Mai 2001 (ABl. L 145/2001, 43-48) haben alle natürlichen und juristischen Personen künftig das Recht, Dokumente aus Rat, Europäischem Parlament und Kommission sowie der übrigen Organe einzusehen. In der Entwurfsphase der Verordnung gab es lediglich bei der Problematik der Ausnahmen vom Zugangsrecht Unstimmigkeiten zwischen Europäischem Parlament und Europäischer Kommission. Die Ausnahmen wurden auf wenige Fälle reduziert. Sie sind in den Bereichen Sicherheit, Verteidigung und militärische Angelegenheiten möglich. Dasselbe gilt für die Verletzung der Privatsphäre. Wenn die Veröffentlichung eines internen Papiers oder einer internen Akte den „innerinstitutionellen" Abstimmungsprozess enorm behindern würde, darf der Zugang ebenfalls verweigert werden; es sei denn, es gäbe ein übergeordnetes öffentliches Interesse an der Publizierung.

4. Meldewesen

4.1 EWOIS – quo vadis?

Für das bundesweit in seiner Ausprägung (bezogen auf ein Flächenland) einzigartige zentrale rheinland-pfälzische Einwohnerinformationssystem, das inzwischen auch als „EWOIS classic" bezeichnet wird, trägt bislang das Innenministerium die Verantwortung. Auch in diesem Berichtszeitraum hat die Änderung der Meldedatenübermittlungsverordnung – bezogen auf EWOIS als zentrales System – wiederum zu einer Erweiterung der Zugriffsmöglichkeiten geführt. Hier wurden seitens des LfD in einer Stellungnahme gegenüber dem Innenministerium insbesondere die neu geschaffenen Möglichkeiten der Meldedatenübermittlungen für Zwecke der Energie- und Wasserversorgung sowie an den SWR (vgl. hierzu Tz. 4.5) angesprochen.

Von der auch datenschutzrechtlich verursachten Bestrebung geleitet, Städte und Verbandsgemeinden in die Lage zu versetzen, ihre Einwohnerdaten selbst zu verarbeiten, ist das Innenministerium seit Jahren bemüht, ein Nachfolgeverfahren (EWOIS-neu) zu konzipieren. Die Neuentwicklung war darauf fokussiert, das Verfahren mit einer dezentralen Komponente auszustatten. Über den Gesamtzusammenhang wurde im 17. Tb. (Tz. 4.1 ff.) berichtet.

Das nunmehr in weiten Teilen vorliegende Ergebnis der Entwicklung sieht vor, dass die Meldedaten dezentral bei den Städten und Verbandsgemeinden geführt werden. Über das so genannte Integrationssystem können die Meldeämter insbesondere bei Zuzug und Wegzug bestimmte Einwohnerdaten übernehmen. Das Informationssystem bietet öffentlichen Stellen (z. B. Polizei, Finanzämtern, Ordnungsbehörden usw.) die Möglichkeit, auf eine Teilmenge des Meldebestandes im Online-Verfahren direkt zuzugreifen. Zum Verfahrensstand dieses Systems haben verschiedene Meinungsaustausche mit dem LfD stattgefunden. Sie betrafen insbesondere die technische Ausgestaltung des künftigen Systems (vgl. dazu die ausführliche Darstellung in Tz. 21.2.1).

Es könnte nun der Fall eintreten, dass insbesondere jene EDV-technisch von der Dezentralisierung überforderten Kommunen nach Möglichkeiten suchen, die Meldedatenverarbeitung auszulagern. Als „Lagerstätten" kommen öffentliche und private Rechenzentren in Deutschland, aber auch – nach den Regelungen der umgesetzten EG-Datenschutzrichtlinie – in den Mitgliedstaaten der Europäischen Union in Betracht. Hier zeichnet sich eine heterogene EDV-Landschaft der Einwohnermeldedatenverarbeitung ab. So sind grundsätzlich verschiedene „Hosting-Modelle" denkbar, wobei es Städte und Verbandsgemeinden geben mag, die sich zwecks Auslagerung der dezentralen Komponente z. B. an ein Rechenzentrum in öffentlich-rechtlicher Trägerschaft in Rheinland-Pfalz wenden, andere werden u. U. private Anbieter in anderen Bundesländern oder Staaten der Europäischen Union – die ihre Leistungen vielleicht besonders billig anbieten – bevorzugen.

In diesem Zusammenhang ist zu bedenken, dass sowohl das Integrationssystem als auch (in reduzierter Form) das Informationssystem aus diesen Datenbeständen gespeist werden. Der Betrieb der Systeme soll nach dem Willen der Beteiligten (Kommunen, Innenministerium) im Auftrag einer gemeinsamen Tochtergesellschaft des Gemeinde- und Städtebundes und des Städtetages ausgeschrieben werden. Auch hier steht die (oben beschriebene) Palette der denkbaren Auftragnehmer zur Verfügung. Unter diesen Rahmenbedingungen würde natürlich auch die Datenschutzkontrolle schwieriger werden.

Gegenwärtig liegt für das Einwohnerinformationssystem der Betrieb und die Verfahrenspflege zentral beim DIZ. Zu welchem Gebilde die skizzierte Entwicklung künftig auch führen mag: Die datenschutzrechtlichen Probleme werden sicherlich nicht geringer.

4.2 Der Entwurf des Dritten Änderungsgesetzes des Melderechtsrahmengesetzes

Nach dem Willen der Bundesregierung – so war kürzlich in Presseartikeln zu den beabsichtigten Änderungen im Melderecht zu lesen – sollen künftig „die Daten laufen – nicht die Bürger".

Mit dem Gesetzentwurf werden die Rahmenbedingungen für den Einsatz moderner Informations- und Kommunikationstechniken geschaffen. Hierdurch soll es Meldepflichtigen künftig ermöglicht werden, sich auch elektronisch bei der zuständigen Meldebehörde anzumelden, ohne persönlich bei der Meldebehörde vorsprechen zu müssen. Voraussetzung für dieses Verfahren ist allerdings, dass im Landesrecht in den einschlägigen Bestimmungen die elektronische Signatur eingeführt wird.

Im Rahmen der Novellierung müssen die melderechtlichen Regelungen den ordnungspolitischen Bedürfnissen des Staates einerseits und den datenschutzrechtlichen Grundpositionen der Einwohner andererseits Rechnung tragen.

Der LfD begrüßt, dass auch den Bürgerinnen und Bürgern der Umgang mit dem Melderegister auf elektronischem Wege ermöglicht werden soll. Allerdings ist die Tendenz mit Sorge zu betrachten, das Melderegister in Abkehr von der bisherigen Rechtslage in ein Verfahren umzuwandeln, das für jedermann – auch für ausländische Stellen – auf elektronischem Wege zugänglich ist, ohne dass die Meldebehörden z. B. prüfen können, ob schutzwürdige Interessen der Betroffenen beeinträchtigt werden.

In diesem Zusammenhang hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder mit der Entschließung vom 9. März 2001 in Bezug auf die zu diesem Zeitpunkt aktuelle (Referenten-)Entwurfsfassung ihre Einschätzung abgegeben (vgl. Anlage 24). Zwischenzeitlich liegt der Gesetzentwurf der Bundesregierung in der Fassung der Bundesratsdrucksache 578/01 vom 17. August 2001 vor. Zu begrüßen ist, dass hier

- zumindest eine Widerspruchsmöglichkeit für Melderegisterauskünfte per Internet geschaffen wurde und
- sich die Meldebehörden bei der Einrichtung von Auskunftssperren unverzüglich zum Schutz der Persönlichkeitsrechte der betroffenen Personen zu unterrichten haben, um zu verhindern, dass trotz Vorliegens einer Auskunftssperre bei der Zuzugsmeldebehörde Auskünfte (seitens der Wegzugsmeldebehörde) über den Verbleib des Einwohners erteilt werden (vgl. BR-Drs. 578/01, Begründung zu § 17 Abs. 3 MRRG-E; s. a. Tz. 4.4).

Die weiteren Forderungen der vorgenannten Entschließung, insbesondere bei der Weitergabe der Meldedaten an die politischen Parteien zum Zwecke der Wahlwerbung, die Widerspruchs- durch eine Einwilligungslösung zu ersetzen, fanden keine Berücksichtigung.

Allerdings kommt im allgemeinen Teil der Begründung des Gesetzentwurfs (BR-Drs. 578/01, S. 19/20) zum Ausdruck, dass dem Datenschutz und der Datensicherheit höchste Priorität einzuräumen sind: „Es muss sichergestellt sein, dass die Authentizität der Kommunikationspartner unzweifelhaft feststeht und die Daten bei der elektronischen Übermittlung nicht Unbefugten zur Kenntnis gelangen. Die vertrauliche Übermittlung ist durch geeignete technisch-organisatorische Verfahren, insbesondere durch Verschlüsselung sicherzustellen. Damit ist auch gewährleistet, dass die Daten während der Übertragung nicht verändert werden können (Integrität)."

Der LfD wird die weitere Entwicklung des Gesetzentwurfs zur Änderung des Melderechtsrahmengesetzes aufmerksam begleiten.

4.3 „Dauerbrenner" im Bereich Meldewesen

4.3.1 Erforderliche Hinweise

Insbesondere aufgrund von Bürgereingaben und örtlichen Feststellungen sieht sich der LfD veranlasst, auf Folgendes hinzuweisen:

- Oft werden in den Mitteilungsblättern der Gemeinden Namen und Anschriften derjenigen Einwohner veröffentlicht, die 70 Jahre und älter geworden sind, sofern diese keinen Widerspruch eingelegt haben. § 35 Abs. 3 MG, der die Zulässigkeit der Datenübermittlung regelt, spricht insoweit jedoch von einem Alters-„Jubiläum". Allgemein üblich ist, dass danach nur im Zeitraum von fünf Jahren erneut Jubiläumsdaten übermittelt werden. Mit Einwilligung der Betroffenen bestehen jedoch keine Bedenken, in der bisherigen Weise zu verfahren.

- Um Missbräuchen vorzubeugen, empfiehlt der LfD, bei der Veröffentlichung von Jubiläumsdaten im Mitteilungsblatt der Gemeinde künftig auf die Nennung der Straße zu verzichten.

- Die von den Meldeämtern verwendeten Vordrucke für Anträge auf Errichtung einer Übermittlungssperre enthalten auf der Rückseite häufig den Hinweis, dass das Widerspruchsrecht bei Ehejubiläen nur gemeinsam ausgeübt werden kann. Dies trifft nicht zu. Der Widerspruch ist auch dann beachtlich, wenn nur ein Ehegatte widersprochen hat.

- Die Vordrucke für Anträge enthalten keinen Hinweis auf die Möglichkeit, der Weitergabe von Meldedaten an politische Parteien, Wählergruppen etc. nach § 35 Abs. 1 MG zu widersprechen.

- Auf die Möglichkeit, eine Auskunftssperre wegen einer Gefahr für Leben, Gesundheit, persönliche Freiheit oder ähnliche schutzwürdige Interessen eintragen zu lassen, wird manchmal lediglich in der Fußnote hingewiesen, welche leicht übersehen werden kann. Das seitens des LfD aufgrund häufiger Anfragen entworfene Muster eines Antrags auf Einrichtung einer Übermittlungssperre ist diesem Bericht als Anlage 31 beigefügt.

- Die Widerspruchsmöglichkeiten nach dem Meldegesetz sind zumindest einmal jährlich zu veröffentlichen. Der Veröffentlichungstext sollte auch auf die zeitliche Befristung der Auskunftssperren bei Gruppenauskünften und der erweiterten Melderegisterauskunft sowie auf die Zulässigkeit einer erneuten Beantragung hinweisen.

- Ausdrückliche gesetzliche Regelungen, ob und in welchem Umfang Ortsbürgermeistern Gesamteinwohnerlisten überlassen werden dürfen, sind weder im Meldegesetz noch in der Meldedatenübermittlungsverordnung vorgesehen. § 8 dieser Verordnung sieht eine regelmäßige Datenübermittlung lediglich für die Zwecke der Ehrung von Alters- und Ehejubilaren und zur Erfüllung der Aufgaben der Ortsgemeinden im Zusammenhang mit der Anmeldung eines Einwohners vor. Auskünfte, die den Namen, akademische Grade und die Anschrift enthalten, dürfen allerdings nach § 34 Abs. 1 MG an jedermann erteilt werden, ohne dass hierfür ein berechtigtes Interesse dargelegt werden müsste, und auch die entsprechende Datenweitergabe an Adressbuchverlage ist nach § 35 Abs. 4 MG zulässig, soweit nicht der Betroffene Widerspruch hiergegen eingelegt hat. Daran anknüpfend ist nach Auffassung des LfD auch die Überlassung einer Gesamteinwohnerliste mit den vorgenannten Daten auf Anforderung eines Ortsbürgermeisters nach § 31 Abs. 1 MG zulässig. Eine derartige Liste kann von der Ortsgemeinde aufgrund der regelmäßigen Übermittlung von Meldedaten nach § 8 der MeldDÜVO ergänzt und fortgeschrieben werden. Selbstverständlich ist bei der Verwendung der übermittelten Daten das Zweckbindungsgebot des Meldegesetzes zu beachten.

- Sollte die Einwohnerliste seitens der Ortsgemeinde z. B. als Grundlage für „Jubiläums-Ermittlungen“ dienen, so ist es von besonderer Bedeutung, mittels einer aktuellen Rückfrage beim Einwohnermeldeamt sicherzustellen, dass eingetragene Widersprüche und Übermittlungssperren berücksichtigt werden. Auskunftserteilungen aus dieser Liste durch die Ortsgemeinde sind unzulässig.

- Für die Erteilung einer Auskunft über die im Einwohnerinformationssystem gespeicherten Daten kann die Sonderfunktion „Totalauskunft“ (vgl. Nr. 2.1 der Verwaltungsvorschrift zur Durchführung des Meldegesetzes vom 19. Februar 1999, MinBl. 1999, S. 203) genutzt werden. Der Antrag des Betroffenen auf Auskunftserteilung über die zur seiner Person gespeicherten Daten ist an keine bestimmte Form gebunden. Die Auskunft ist nur zu erteilen, wenn die Identität des Betroffenen zweifelsfrei festgestellt werden kann. Antragsberechtigt sind Betroffene, die das 16. Lebensjahr vollendet haben. Für einen Betroffenen, der das 16. Lebensjahr noch nicht vollendet hat, ist der gesetzliche Vertreter antragsberechtigt. Ein Auskunftsanspruch besteht nach § 9 Abs. 2 MG nicht bei den Daten, die einen Rückschluss auf die Rechtsstellung eines Kindes und seiner leiblichen Eltern zulassen, und zwar in den Fällen, in denen es sich um eine Annahme als Kind, um ein Kind, dessen Eltern nicht miteinander verheiratet sind, oder um ein Kind handelt, für das ein Adoptionsverhältnis oder ein Adoptionspflegeverhältnis besteht (vgl. Nr. 2.4 der vorgenannten Verwaltungsvorschrift).

4.3.2 Fragen zur Gruppenauskunft

Den Schwerpunkt behördlicher Anfragen im Berichtszeitraum bildeten Probleme bei der Anwendung der Vorschriften zur Gruppenauskunft.

Als Beispiel einer Problemlage bei der Gruppenauskunft kann folgender Fall dienen:

In Rede stand die Zulässigkeit einer Adressdatenübermittlung seitens des Einwohnermeldeamts einer Verbandsgemeindeverwaltung an die Ortsgemeinde zum Zwecke der Beteiligung Jugendlicher einer bestimmten Altersgruppe an der Planung eines Jugendraums in der Ortsgemeinde. Als Rechtsgrundlage kommt hier sowohl § 31 Abs. 1 als auch § 34 Abs. 3 MG in Betracht.

Nach § 31 Abs. 1 MG darf die Meldebehörde einer sonstigen öffentlichen Stelle aus dem Melderegister bestimmte Daten – auch im Rahmen einer Gruppenauskunft – übermitteln, wenn dies zur Erfüllung der in der Zuständigkeit des Empfängers liegenden Aufgaben erforderlich ist.

Gemäß § 34 Abs. 3 MG sind Gruppenauskünfte zulässig, wenn sie im öffentlichen Interesse liegen. Nach Nr. 16.3 der Verwaltungsvorschrift zur Durchführung des Meldegesetzes vom 19. Februar 1999 (MinBl. S. 203) ist das öffentliche Interesse für eine Gruppenauskunft in der Regel anzunehmen u. a. bei Auskunftsersuchen der Spitzenverbände der freien Wohlfahrtspflege und der ihnen angeschlossenen Verbände zum Zwecke der Betreuung alter Menschen, Jugendlicher und sonstiger Betreuungsgruppen. Sogar die Erteilung von Gruppenauskünften an Markt- und Meinungsforschungsinstitute wäre grundsätzlich zulässig (vgl. Nr. 16.4 der vorgenannten Verwaltungsvorschrift).

Von der im Rahmen des § 31 Abs. 1 MG zu begründenden Erforderlichkeit ist dann auszugehen, wenn die Empfängerseite ohne die zu übermittelnden Daten ihre Aufgaben nicht oder nicht sachgerecht erledigen kann. Es könnte nun problematisiert werden, ob diese Voraussetzung bei enger Auslegung des Begriffs der Erforderlichkeit im Hinblick auf einen Beteiligungsaufruf zu Fragen der Planung eines Jugendraums erfüllt ist. Dies mag indessen dahinstehen. Wenn nämlich – wie im vorliegenden Fall – die Datenübermittlung in Form der Gruppenauskunft sogar an private Stellen nach § 34 Abs. 3 MG zulässig wäre, dann muss erst recht die entsprechende Auskunft an eine öffentliche Stelle, den Ortsbürgermeister, erlaubt sein.

Zusammenfassend hielt der LfD die Datenübermittlung in entsprechender Anwendung des § 34 Abs. 3 MG – mit der Maßgabe, dass vorhandene Auskunftssperren zu berücksichtigen sind – für zulässig; denn ein öffentliches Interesse an der Einbeziehung Jugendlicher in das gemeindliche Leben ist im vorliegenden Zusammenhang offensichtlich gegeben.

4.4 Berücksichtigung der Auskunftssperre bei Gefährdung schutzwürdiger Interessen durch die in einem anderen Bundesland angesiedelte Wegzugsbehörde

Anlässlich einer Eingabe hat sich gezeigt, dass die unterschiedliche Handhabung in den Meldeämtern einzelner Bundesländer im Umgang mit einer Auskunftssperre zu einer Verletzung der Datenschutzrechte der Betroffenen führen kann. Eine junge Frau wurde von Teilen ihrer Familie aus religiösem Wahn verfolgt und bedroht. Sie ist daraufhin mit ihrer Tochter in ein anderes Bundesland, nach Rheinland-Pfalz, gezogen. Damit ihre Adresse nicht bekannt wird, wurde hier nach eingehender Prüfung des Antrags eine melderechtliche Auskunftssperre wegen Gefährdung schutzwürdiger Interessen eingetragen. Zur Gewährleistung eines umfassenden Schutzes hat die junge Frau für sich und ihre Tochter auch bei der Wegzugsbehörde eine Auskunftssperre beantragt. Dieser Antrag wurde allerdings abgelehnt mit der Begründung, eine akute und aktuell bestehende Gefahr sei nicht nachgewiesen bzw. glaubhaft dargelegt. Die Wegzugsbehörde hat also im Rahmen der Bescheidung des Antrags eigenes Ermessen ausgeübt und ist in der Würdigung der Antragsbegründung der örtlich zuständigen (rheinland-pfälzischen) Meldebehörde nicht gefolgt. Sie könnte mithin ohne Rücksicht auf eine am Zuzugsort eingetragene Auskunftssperre Melderegisterauskünfte erteilen.

Der LfD hatte sich diesbezüglich mit der Frage zu befassen, ob rechtliche Möglichkeiten vorhanden sind, die Verletzung von Datenschutzrechten, nämlich die Nichtbeachtung einer bei dem örtlich zuständigen Meldeamt eingetragenen Auskunftssperre durch die Wegzugsbehörde, auszuschließen. Dann müsste die früher zuständige – in einem anderen Bundesland angesiedelte – Meldebehörde verpflichtet sein, die seitens der Zuzugsbehörde eingetragene Sperre bei Anfragen zu berücksichtigen, und zwar ohne ihr die Möglichkeit einzuräumen, eigenes Ermessen auszuüben.

Zu untersuchen war zunächst, ob eine Meldebehörde aufgrund der ihr bekannten in einem anderen Bundesland bei dem zuständigen Meldeamt eingetragenen Auskunftssperre nach den Regelungen des Melderechtsrahmengesetzes daran gehindert ist, Auskünfte aus ihrem Melderegister zu erteilen.

Nach § 21 Abs. 5 MRRG ist jede Melderegisterauskunft unzulässig, wenn der Betroffene der Meldebehörde das Vorliegen von Tatsachen glaubhaft macht, die die Annahme rechtfertigen, dass ihm oder einer anderen Person hieraus eine Gefahr für Leben, Gesundheit, persönliche Freiheit oder ähnliche schutzwürdige Belange erwachsen kann. Das Auskunftsrecht der Meldebehörde und demzufolge auch eine ggf. bestehende Auskunftssperre beziehen sich auf die bei dieser Meldebehörde gespeicherten personenbezogenen Daten. Ob dagegen die Meldebehörde aufgrund einer anderen Orts bestehenden Auskunftssperre daran gehindert ist, Auskünfte aus ihrem Melderegister nach § 21 Abs. 1 und 2 MRRG zu erteilen, lässt sich § 21 Abs. 5 MRRG nicht entnehmen. Eine derartige Verpflichtung der Meldebehörde ergibt sich auch nicht aus anderen Vorschriften des Melderechtsrahmengesetzes, insbesondere nicht aus § 17 Abs. 1 MRRG. Danach ist bei einer Wohnungsummeldung oder bei der Anmeldung weiterer Wohnungen eine gegenseitige Unterrichtung zwischen der bisher zuständigen und der nunmehr zuständigen Meldebehörde über bestimmte personenbezogene Daten vorgesehen. Das Bestehen einer Auskunftssperre gehört allerdings nicht zu den bundesrechtlich zur Übermittlung vorgesehenen Daten.

Gemäß § 17 Abs. 1 Satz 3 MRRG können, soweit Meldebehörden desselben Landes beteiligt sind, für die Datenübermittlung weiter gehende Regelungen durch Landesrecht getroffen werden. Von dieser bundesrechtlichen Ermächtigung ist im rheinland-pfälzischen Meldegesetz Gebrauch gemacht worden. Gemäß § 30 Abs. 3 MG R-P hat in den Fällen der in § 34 Abs. 5 MG R-P geregelten Auskunftssperre die zuständige Meldebehörde die für die vorherige Wohnung und die für weitere Wohnungen zuständigen Meldebehörden zu unterrichten.

Aus dieser landesrechtlich begründeten Unterrichtungspflicht lässt sich bundesrechtlich allerdings keine zu beachtende Auskunftssperre für Meldebehörden anderer Bundesländer hinsichtlich der dort gespeicherten personenbezogenen Daten des betroffenen ehemaligen Einwohners herleiten.

Der entscheidende Anknüpfungspunkt für eine Problemlösung liegt darin, dass Normadressat für die Vorschriften über die Erteilung von Melderegisterauskünften sowie die Nichterteilung aufgrund einer Auskunftssperre die „zuständige" Meldebehörde ist. Dies ist grundsätzlich die Meldebehörde, in deren Zuständigkeitsbereich der Betroffene seinen Wohnsitz hat. Insoweit muss gesehen werden, dass jeder Bürger einen durch das Rechtsstaatsprinzip verfassungsrechtlich gewährleisteten Anspruch darauf hat, dass die Verwaltung die zu seinem Schutz bestimmten Vorschriften strikt beachtet. Hier besteht nach Auffassung des LfD die staatliche Verpflichtung, ein für den Bürger kaum zu durchschauendes Verwaltungsverfahren so zu organisieren, dass schwer wiegende Beeinträchtigungen seiner schutzwürdigen Belange zuverlässig ausgeschlossen sind. Dazu gehört die vorbehaltlose Berücksichtigung der Auskunftssperre bei Gefährdung schutzwürdiger Interessen durch die Wegzugsbehörde.

Bei der Zusammenarbeit zwischen den Meldebehörden der Länder ist also offensichtlich melderechtlicher Handlungsbedarf vorhanden, den der Gesetzgeber nunmehr erkannt hat und im Zuge der anstehenden Novellierung des Melderechtsrahmengesetzes eine Bestimmung aufnehmen wird, wonach über die Eintragung einer Auskunftssperre die für die frühere Wohnanschrift zuständige Meldebehörde zu unterrichten ist, die ihrerseits diese Auskunftssperre zum Schutz der Persönlichkeitsrechte des Betroffenen zu berücksichtigen hat (vgl. Tz. 4.2).

4.5 Datenübermittlung an die Gebühreneinzugszentrale

Den LfD erreichen häufig Anfragen zur Zulässigkeit der Datenübermittlung an die GEZ. Hier hat sich die Rechtslage während des Berichtszeitraums geändert. Eine Rechtsgrundlage für die regelmäßige Übermittlung von Meldedaten aus Anlass der An- und Abmeldung von Einwohnern sowie von Sterbefällen zum Zwecke des Rundfunkgebühreneinzugs bestand in Rheinland-Pfalz bis zur Novellierung der MeldDÜVO im August 2000 nicht. Bislang war es lediglich zulässig, dem Südwestrundfunk oder einer von ihm beauftragten Stelle (GEZ) im Wege des automatisierten Datenabgleichs Einwohnerdaten zur Verfügung zu stellen. Hierbei wurde der Meldebehörde zunächst ein (inaktueller) Datenbestand zum Zwecke der Berichtigung übermittelt. Diese Verfahrensweise war wohl als Grundlage für die Suche nach unbekannten Gebührenschuldnern nur wenig geeignet. Dies mag der Grund dafür sein, dass diese Datenübermittlung an den Südwestrundfunk, für die seit September 1994 eine Rechtsgrundlage existierte, nicht praktiziert wurde.

Die Rundfunkanstalten haben eine andere Form der regelmäßigen Datenübermittlung angestrebt und hatten Erfolg: Sie erhalten nunmehr aufgrund einer Änderung der Meldedatenübermittlungsverordnung von den Meldeämtern Adressdaten in Fällen des Zuzugs, des Wegzugs und in Sterbefällen. Nach § 16 MeldDÜVO dürfen dem Südwestrundfunk zum Zwecke der Erhebung und des Einzugs der Rundfunkgebühren nach § 7 des Rundfunkgebühren-Staatsvertrags oder der von ihm beauftragten Stelle (GEZ) aus Anlass der An- oder Abmeldung oder des Todes volljähriger meldepflichtiger Personen folgende Daten übermittelt werden: Vor- und Familienname, Doktorgrad, frühere Namen, Tag der Geburt, gegenwärtige und frühere Anschriften, Haupt- und Nebenwohnung, Tag des Ein- und Auszugs, Familienstand sowie Sterbetag und -ort. Die übermittelten Daten dürfen nur genutzt werden, um den Beginn und das Ende der Rundfunkgebührenpflicht sowie diejenige Landesrundfunkanstalt zu ermitteln, der die Gebühr zusteht. Der Südwestrundfunk und die von ihm beauftragte Stelle haben durch organisatorische und technische Maßnahmen sicherzustellen, dass nur berechtigte Bedienstete zur rechtmäßigen Aufgabenerfüllung Kenntnis erhalten und dass nicht mehr benötigte Daten unverzüglich, spätestens jedoch innerhalb von sechs Monaten, gelöscht werden.

Eine andere Rechtsgrundlage für die Übermittlung von Meldedaten an die GEZ bietet § 31 MG, der die Datenübermittlung an andere Behörden oder sonstige öffentliche Stellen regelt. Wenn die GEZ in Schwerpunktbereichen, die beispielsweise altersmäßig abzugrenzen sind, ihrer nach dem Staatsvertrag bestehenden Befugnis zur Ermittlung unbekannter Gebührenpflichtiger nachkommt, so können hierfür Adressdaten aus dem Melderegister übermittelt werden. Diese Rechtsauffassung wurde durch den VGH Mannheim in einem Urteil vom 15. November 1994 (Az.: I S 310/94) für Baden-Württemberg ausdrücklich bestätigt.

Im Ergebnis ist somit die Übermittlung von Meldedaten an die GEZ datenschutzrechtlich zulässig.

4.6 Zulässigkeit der Übermittlung von Meldedaten der Schulanfänger

Im Rahmen einer Eingabe wurde gefragt, ob durch die Eintragung einer Auskunftssperre nach dem Meldegesetz verhindert werden kann, dass Kreditinstituten im Wege der Gruppenauskunft die Meldedaten der Schulanfänger zwecks Zusendung von Geschenksparbüchern übermittelt werden.

Gruppenauskünfte unterscheiden sich von Einzelauskünften dadurch, dass Informationen nicht bezüglich einer bestimmten, namentlich bezeichneten oder in anderer Weise individualisierten Person begehrt werden, sondern das Auskunftsinteresse auf solche Personen gerichtet ist, die einer durch ein bestimmtes Merkmal gekennzeichneten Gruppe angehören.

§ 34 Abs. 3 MG lässt die Erteilung einer Gruppenauskunft nur dann zu, wenn diese Auskunft im öffentlichen Interesse liegt, lässt also kommerzielle Interessen als Übermittlungsgrund nicht gelten.

Die von den Petenten angesprochenen Geschenksparbücher des Kreditinstituts dienen offensichtlich Werbezwecken. Eine Übermittlung von Meldedaten der Schulanfänger an Kreditinstitute ist daher nicht zulässig. Daraus folgt: Auch ohne eingetragene Sperre bezüglich Gruppenauskünften ist es melderechtlich unzulässig, personenbezogene Daten der Schulanfänger an ein Kreditinstitut

zu übermitteln. Besondere melderechtliche Vorkehrungen, um zu erreichen, dass die Daten der Schulkinder nicht zum Zwecke von Werbemaßnahmen seitens Kreditinstituten aus dem Melderegister übermittelt werden können, sind nicht erforderlich.

Das Melderecht erlaubt lediglich die Übermittlung von Schulanfängerdaten an die Grundschulen. Gemäß § 7 Abs. 1 MeldDÜVO dürfen von der Meldebehörde an die zuständige Grundschule zur Feststellung der allgemeinen Schulpflicht die Daten jener Kinder übermittelt werden, die in einem bestimmten Zeitrahmen das sechste Lebensjahr vollenden.

Was den Bereich des schulischen Umgangs mit den Schulanfängerdaten anbelangt, so wäre eine Übermittlung beispielsweise an Kreditinstitute nur zulässig, wenn die Eltern eingewilligt hätten (§ 54 a Abs. 2 letzter Satz SchulG).

Ferner hat der LfD darauf hingewiesen, dass – unabhängig von einer Übermittlung – für Kreditinstitute die Möglichkeit besteht, Schulanfängerdaten aus allgemein zugänglichen Quellen dadurch zu erlangen, dass die Geburtsanzeigen in den Tageszeitungen ausgewertet und gespeichert werden.

4.7 Wahlwerbung – oder „Wenn die rechte Hand nicht weiß, was die linke tut"

Eine Eingabe betraf eine häufig gestellte Frage zur Wahlwerbung unter Verwendung von Meldedaten. Dem Petenten wurde mitgeteilt, dass nach § 35 Abs. 1 Satz 1 MG die Meldebehörde Parteien, Wählergruppen und anderen Trägern von Wahlvorschlägen im Zusammenhang mit Parlaments- und Kommunalwahlen in den sechs der Wahl vorangehenden Monaten eine einfache Melderegisterauskunft über Wahlberechtigte erteilen darf, für deren Zusammensetzung das Lebensalter der Betroffenen bestimmend ist. Die Regelung gilt gem. § 35 Abs. 2 MG entsprechend für Auskünfte an Antragsteller von Volksbegehren, Volksentscheiden und vergleichbaren Abstimmungen. Die einfache Melderegisterauskunft erstreckt sich nach § 34 Abs. 1 MG auf Vor- und Familiennamen, akademische Grade sowie Anschriften. Gemäß § 35 Abs. 1 Satz 2 MG können die Bürgerinnen und Bürger der diesbezüglichen Weitergabe ihrer Daten widersprechen. Die Meldebehörden dürfen dann die Daten nicht mehr für Wahlwerbezwecke weitergeben. Die Eintragung des Widerspruchs kann schriftlich oder bei einem persönlichen Besuch im zuständigen Meldeamt beantragt werden. Hierauf ist bei der Anmeldung nach § 13 Abs. 1 MG sowie mindestens einmal jährlich durch öffentliche Bekanntmachung hinzuweisen. Außerdem darf der Empfänger die Daten nur für den Zweck verwenden, zu dem sie übermittelt worden sind. Spätestens einen Monat nach der Wahl sind die Daten bei ihm zu löschen.

Auf entsprechende Anfrage des LfD hat das zuständige Meldeamt mitgeteilt, dass von dort aus für Wahlwerbezwecke keine Einwohnerdaten übermittelt worden sind. Bei der Suche nach der Datenquelle ergab sich, dass nach entsprechender Anforderung einer politischen Partei zum Zwecke der Wahlwerbung das DIZ die Anschriften aller Einwohner einer bestimmen Altersgruppe einer Gebietskörperschaft an die Geschäftsstelle der Partei weitergegeben hat. Hier stand zu fragen, inwieweit die Städte und Gemeinden als Auftraggeber von der Auftragnehmerin DIZ bei der Verarbeitung von Meldedaten im Rahmen der Wahlwerbung beteiligt worden sind.

Im Zuge der weiteren Nachforschungen hat sich dann folgender Sachverhalt ergeben:

Die Parteigeschäftsstelle trat hinsichtlich der Melderegisterauskunft nach § 35 Abs. 1 MG (Wahlwerbung) zwar direkt an das DIZ heran, hatte jedoch die diesbezügliche schriftliche Zustimmung der Städte und Gemeinden dem Auswertungsersuchen beigefügt. Bei näherer Betrachtung fiel indessen – bezogen auf die ursprünglich zugrunde liegende Eingabe – auf, dass die „Datenfreigabe" nicht durch den „Herrn der Daten", nämlich das Meldeamt, sondern seitens des städtischen Wahlamtes erfolgte.

Mit dieser Verfahrensweise wurde gegen melderechtliche Vorschriften verstoßen, was der LfD zum Anlass nahm, die Verantwortlichen eindringlich auf die Einhaltung der Sorgfaltspflichten im Umgang mit Meldedaten hinzuweisen. Er bat darum, künftig durch organisatorische Maßnahmen sicherzustellen, dass die Weitergabe von Meldedaten ausschließlich durch das Meldeamt und nicht durch unzuständige Stellen innerhalb der Stadtverwaltung erfolgt, und über das Veranlasste zu berichten.

4.8 Beantragung von Führungszeugnissen per E-Mail?

Die Anfrage, ob Bedenken bestehen, den Bürgerinnen und Bürgern die Beantragung von Führungszeugnissen per E-Mail im Internet anzubieten, hat der LfD wie folgt beantwortet:

Wenn die Antragstellung nach § 30 Abs. 2 Satz 1 BZRG per elektronischer Post möglich sein soll, geht es in dieser Situation zunächst einmal darum, das Verfahren überschaubar zu gestalten, damit die „elektronischen Antragsteller" beispielsweise Kenntnis davon erhalten, welche Datenflüsse, ihre Person betreffend, ausgelöst werden. Sie sollten auch darauf hingewiesen werden, dass Führungszeugnisse ausschließlich vom Bundeszentralregister erteilt werden. Wenn Eintragungen vorhanden sind, handelt es sich in aller Regel um rechtskräftige Verurteilungen durch Strafgerichte; daneben können bestimmte Verwaltungsentscheidungen (z. B. Passversagungen oder waffen- und gewerberechtliche Entscheidungen) im Bundeszentralregister eingetragen werden. Es kann ein Führungszeugnis für private Zwecke in Rede stehen, das z. B. anlässlich der Einstellung bei einem privaten Arbeitgeber, hinsichtlich der Einschreibung bei einer Universität oder bezüglich der Anerkennung als Kriegsdienstverweigerer benötigt wird. Daneben gibt es das Führungszeugnis zur Vorlage bei Behörden. Es hat gegenüber dem Führungszeugnis für Private einen erweiterten Inhalt. Zum Bei-

spiel gibt es auch Auskunft über geringfügige Strafen, die nicht in ein Führungszeugnis für Private aufgenommen werden, wenn es sich um Straftaten handelte, die bei der Ausübung eines Gewerbes begangen wurden und das Führungszeugnis für die behördliche Entscheidung über eine Gewerbeerlaubnis dienen soll. Diese Führungszeugnisse für Behörden werden zwar von den Betroffenen beantragt, aber nicht ihnen, sondern nur der Behörde übersandt. Dies führt nicht selten zu der – unzutreffenden – Vermutung, das Führungszeugnis habe irgendeinen „geheimen" Inhalt, den sie nicht erfahren könnten. Vielmehr haben die Betroffenen verschiedene Möglichkeiten, auch den Inhalt behördlicher Führungszeugnisse zu erfahren. Zum einen können sie das Führungszeugnis bei der Behörde einsehen, an die es adressiert wird. Wenn sie es einsehen wollen, bevor es an die Behörde gesandt wird, können sie verlangen, dass es zunächst an ein von ihnen benanntes Amtsgericht geschickt wird, wo sie Einblick nehmen und entscheiden können, ob es an die Behörde weitergeleitet wird.

Hier wird deutlich, dass die Beantragung eines Führungszeugnisses eine vielschichtige, recht sensible Angelegenheit sein kann und daher zunächst einmal – als Vorstufe zur eigentlichen Antragstellung – entsprechende Erläuterungen der Gemeinde bereitzustellen sind, um die Bürgerinnen und Bürger zu „informierten Antragstellern" zu machen.

Die auf diese Art und Weise „Vorinformierten" müssen dann in die Lage versetzt werden, einen korrekten Antrag zu stellen. Dazu müssen sie wissen, welche Daten sie per elektronischer Post preiszugeben haben. Ihnen muss deutlich gemacht werden, dass theoretisch für jeden anderen Besitzer eines Internet-Anschlusses die Möglichkeit besteht, die eingegebenen Daten zu lesen, sofern die übertragenen Daten nicht verschlüsselt werden.

Bei entsprechender Hinweisgestaltung bestehen nach Auffassung des LfD insoweit keine datenschutzrechtlichen Bedenken gegen die Beantragung eines Führungszeugnisses per elektronischer Post im Internet, denn die Antragsteller nehmen hier selbstbestimmt die Risiken hinsichtlich der Datensicherheit in Kauf. Auch im Bereich der Datenkontrolle und Gebührenkontrolle könnten aufgrund der vorstehenden Erwägungen z. B. erforderliche Datenabgleiche zwischen den Beteiligten im Rahmen des § 5 Abs. 1 LDSG per E-Mail im Internet vorgenommen werden.

Nicht zur Disposition der Beteiligten steht allerdings die Identitätskontrolle. Der Antragsteller hat gemäß der Regelung in § 30 Abs. 2 Satz 2 BZRG seine Identität nachzuweisen. Sinn und Zweck dieser Vorschrift ist es auszuschließen, dass unter falschem Namen Anträge gestellt werden. Diesem Erfordernis kann gegenwärtig aus der Sicht des LfD nur dadurch Rechnung getragen werden, dass der Antragsteller seine Identität durch Vorlage seines Passes oder Personalausweises nachweist.

An der Rechtslage könnte sich erst dann etwas ändern, wenn in den einschlägigen Bestimmungen die elektronische Signatur eingeführt wird.

4.9 Zuständigkeit bei der Beantragung eines Führungszeugnisses

Die an den LfD herangetragene Frage, ob Bedenken bestehen, Bundeszentralregister-Anträge für Personen aufzunehmen, die nicht im Zuständigkeitsbereich der aufnehmenden Behörde gemeldet sind, hat er wie folgt beantwortet:

Aus datenschutzrechtlicher Sicht bestehen keine Bedenken, es jenen Ämtern, die im Online-Verfahren auf Melderegisterdaten zugreifen können, zu ermöglichen, die Informationen, die sie derzeit aufgrund melderechtlicher Übermittlungsbestimmungen bereits aus EWOIS abrufen können, automatisiert in die Anfrage zum Bundeszentralregister zu übernehmen.

So besteht das „Produkt Führungszeugnis" aus den beim Bundeszentralregister zur Person des Antragstellers (bezogen auf die jeweils beantragte Ausprägung des Führungszeugnisses) gespeicherten Daten, und zwar unabhängig davon, über welches Meldeamt des Landes die Beantragung erfolgt. Hinzu kommt, dass es aus dem Blickwinkel des Datenschutzes – beispielsweise bei kleinräumig gegliederten Verbandsgemeinden – für die Betroffenen durchaus ein Anliegen sein kann, das Führungszeugnis gerade nicht im sozialen Umfeld des Wohnorts zu beantragen.

In diesem Zusammenhang ist insbesondere von Bedeutung, dass die antragstellende Person gemäß der Regelung in § 30 Abs. 2 Satz 2 BZRG ihre Identität nachzuweisen hat (vgl. hierzu auch Tz. 4.8). Sinn und Zweck dieser Vorschrift ist es auszuschließen, dass unter falschem Namen Anträge gestellt werden. Diesem Erfordernis wird dadurch Rechnung getragen, dass der Antragsteller seine Identität durch Vorlage seines Passes oder Personalausweises nachweist.

4.10 Örtliche Feststellungen bei der automatisierten Übermittlung von Meldedaten

Es ist im Grunde genommen nichts dagegen einzuwenden, wenn die Verwaltungen immer mehr dazu übergehen, sachbearbeitenden Personen den Online-Zugriff auf Meldedaten einzuräumen, vorausgesetzt, die gesetzlichen Bestimmungen über die automatisierte Datenübermittlung, insbesondere die Erforderlichkeit und Angemessenheit im Rahmen des § 7 LDSG, werden beachtet.

Örtliche Feststellungen haben allerdings ergeben, dass dies wohl nicht immer der Fall ist. So hat sich z. B. bei einer großen Gebietskörperschaft herausgestellt, dass dort die automatisierte Übermittlung von Meldedaten an andere Stellen außerhalb des Meldeamtes in einem außerordentlich weit gehenden Umfang ermöglicht wurde. Die Einrichtung solcher Verfahren steht gem. § 7 Abs. 1 LDSG

unter dem Vorbehalt der Angemessenheit und Erforderlichkeit. Ein entscheidender Gesichtspunkt für die Prüfung der Angemessenheit ist die Zahl der zu erwartenden Abrufe. Es ist danach unverhältnismäßig, die mit der Einrichtung eines automatisierten Übermittlungsverfahrens einhergehenden Missbrauchsgefahren in Kauf zu nehmen, nur um einen gelegentlichen Abruf von Daten zu ermöglichen. In dem angesprochenen Fall hatte es die öffentliche Stelle über Jahre hinweg unterlassen, die gesetzlichen Vorgaben umzusetzen. Aus den vom DIZ zur Verfügung gestellten Statistiken über die Zugriffshäufigkeit auf die Einwohner-Datenbank wurden keine Folgerungen bzgl. der Angemessenheit i. S. von § 7 LDSG gezogen. So wurde aufgrund einer näheren Prüfung offenbar, dass von 344 Zugriffsberechtigungen rund 80 hätten aufgehoben werden müssen. Diesen Umgang mit personenbezogenen Daten hat der LfD als Verstoß gegen datenschutzrechtliche Vorschriften beanstandet.

5. Polizei

5.1 Örtliche Feststellungen bei Polizeidienststellen

Im Berichtszeitraum wurden bei 20 Polizeidienststellen örtliche Feststellungen getroffen. Außerdem wurden zahlreiche Beratungs- bzw. Informationsgespräche bei der Projektgruppe des Innenministeriums zur Entwicklung des EDV-Systems „POLADIS-neu“ und beim LKA geführt.

Beanstandungen wurden hierbei nicht ausgesprochen. Es bestand jedoch Anlass, zahlreiche Verbesserungsvorschläge aus datenschutzrechtlicher Sicht zu formulieren, wobei in allen Fällen ein Einvernehmen mit dem Innenministerium erreicht wurde.

Im Einzelnen sah der LfD bei folgenden Themen Handlungsbedarf:

- Kriminalpolizeiliche Sammlungen über Straftaten mit nicht eindeutiger Beweislage waren in POLIS über längere Zeiträume gespeichert, obwohl kein MiStra-Rücklauf über den Ausgang des Strafverfahrens erfolgt war. Der LfD empfahl, in Zweifelsfällen zunächst eine Prüffrist von maximal zwei Jahren vorzusehen und vor einer Verlängerung ggf. Informationen über den Ausgang des Verfahrens einzuholen.

- Bei einer Polizeibehörde eingesetzte PCs waren mit einer für alle Nutzer zugänglichen Kopierfunktion ausgestattet und verfügten zudem über ein offenes Diskettenlaufwerk. Dies ermöglicht ein unbemerktes Kopieren großer Datenmengen, was nach Auffassung des LfD insbesondere beim Umgang mit sensiblen Daten zu verhindern ist.

- Wie in den Jahren zuvor wurden bei verschiedenen Dienststellen Dateien festgestellt, die beim LfD nicht angemeldet waren.

- Bei einer Polizeibehörde war zwischen Behördenleitung und dem Personalrat noch keine Dienstvereinbarung mit Detailregelungen über die Nutzung des EDV-Systems für Personaldaten (PINS) getroffen worden.

- Waren in den vergangenen Jahren die Einsichtnahmen in die Pass- und Personalausweis-Register mehrfach nicht dokumentiert worden, so wurde neuerdings auf einer Dienststelle eine Dokumentierungsform angetroffen, die der LfD für nicht erforderlich und damit nicht für zulässig hält: Von der Dienststelle war der Ausweis der überprüften Person einschließlich des Lichtbildes kopiert und in einem Ordner verwahrt worden.

- Im Berichtszeitraum wurde bei einer Dienststelle festgestellt, dass bei POLIS-Abfragen, die für andere getätigt wurden, die erforderlichen Zusatzprotokollierungen in weitem Umfang nicht durchgeführt wurden. Hinzu kam noch, dass zumindest in Einzelfällen der Systemnutzer den Raum bzw. sogar die Dienststelle verlassen hatte, ohne sich im System abzumelden. Hierdurch war es anderen Bediensteten möglich, Abfragen durchzuführen, ohne dass diese protokolliert wurden.

- Zahlreiche Patientenunterlagen, die in Arztpraxen sichergestellt worden waren, wurden bei einer Polizeidienststelle in einem Raum verwahrt, bei dem die Sicherheitsvorkehrungen gegen unbefugtes Eindringen nach Ansicht des LfD verstärkt werden müssten.

- In dem Bereich einer Polizeibehörde wurde festgestellt, dass keine Regelung für den Zugang zu den Serverräumen und dem Knotenrechner des LDKN bestand. Dadurch war die Gefahr erhöht, dass sich Unbefugte Zugang zu diesen Räumen hätten verschaffen können.

- Die Erforderlichkeit der im polizeilichen Informationssystem vergebenen personengebundenen Hinweise „fremdenfeindlich“, „Prostitution“, „Sebsttötungsgefahr“, „geisteskrank“ und „Ansteckungsgefahr“ hat der LfD anlässlich einer örtlichen Feststellung bei einer Behörde überprüft. Es hat sich gezeigt, dass allgemein restriktiv bei der Anwendung vorgegangen wurde und lediglich einer der Hinweise nicht zulässig war und somit gelöscht werden musste.

5.2 POLADIS-neu

Nach einer mehrjährigen Entwicklungszeit wurde im Jahr 2001 bei der rheinland-pfälzischen Polizei das EDV-System POLADIS-neu eingeführt. In zeitlichem Zusammenhang damit wurden alle Arbeitsplätze bei der Polizei mit vernetzten PCs ausgestattet.

Bei POLADIS-neu handelt es sich um ein umfassendes Vorgangsbearbeitungssystem, das auch eine elektronische Vorgangsübermittlung zwischen allen Dienststellen des Landes ermöglicht und innerhalb einer Dienststelle den Zugriff auf grundsätzlich alle Daten von jedem Arbeitsplatz aus ermöglicht. Außerdem wird über eine Schnittstelle eine Verbindung zu dem in der Entstehungsphase befindlichen bundesweiten polizeilichen Informationssystem INPOL-neu hergestellt. Zugriffsberechtigungen auf den Datenbestand in POLADIS-neu erfolgen durch Zuweisung von vorher festgelegten Nutzerrollen. Von besonderer Bedeutung bei POLADIS-neu ist die Vermeidung der mehrfachen Erfassung derselben Daten; das bedeutet, dass einmal erfasste Daten zu verschiedenen Zwecken sowohl innerhalb des Systems als auch für Speicherungen in den Verbunddateien beim BKA genutzt werden können.

Die Entwicklung von PPLADIS-neu wurde durch den LfD von Anfang an begleitet. Dabei wurden zunächst im technischen Bereich zahlreiche Hinweise zu den datenschutzrechtlichen Anforderungen gegeben.

– Zur Löschung der „Vorgangsdaten“:

Die Vorgangsdaten umfassen sämtliche zur Sachbearbeitung im Rahmen von POLADIS-neu erfassten Informationen unter Einschluss von Vernehmungsniederschriften. Diese sollen grundsätzlich so lange im automatisierten Verfahren gespeichert werden, wie es zur Sachbearbeitung erforderlich ist; bei Abschluss der Sachbearbeitung wird eine weitere Frist eingegeben, die sich an so genannten „Regelfristen“ orientiert. Anschließend sollen die Daten auf einen Kerndatenbestand reduziert werden, für den weitere Fristen gelten. Die Regelfristen für die Aufbewahrung der Vorgangsdaten waren aus Sicht des LfD zum Teil unangemessen lang bemessen. Es ist nicht plausibel, wieso, wie beabsichtigt, z. B. der Verdacht eines Ladendiebstahls grundsätzlich fünf Jahre lang mit allen Unterlagen im System gespeichert sein muss.

Nach Gesprächen mit dem Ministerium des Innern und für Sport wurden die Regelfristen im Wesentlichen im Sinne der Anregungen des LfD geändert.

Aus datenschutzrechtlicher Sicht ist weiterhin zu bemängeln, dass derzeit der Ausgang des Verfahrens keine Rolle bei der automatischen Setzung von Regelfristen spielen soll. Verfahren, bei denen kein Täter ermittelt wurde, werden in gleicher Weise behandelt wie Verfahren, bei denen ein Täter feststeht und verurteilt wurde. Diese Kriterien müssten jedoch für eine sachangemessene Bewertung und Festlegung von Fristen der Vorgangsdaten maßgeblich sein. Zwar kann und soll die Löschungsfrist für die Vorgangsdaten individuell bestimmt werden; nur für den Fall, dass keine individuelle Bestimmung erfolgt, sollen die Regelfristen greifen. Angesichts des Verfahrens aber, wonach die Regelfristen dem Sachbearbeiter bei Abschluss der Bearbeitung automatisiert vorgeschlagen werden und wonach ein Abweichen von den Regelfristen in jedem Fall individuell zu begründen ist, steht aus Sicht des LfD zu erwarten, dass die automatisiert vorgegebenen Fristen regelmäßig (oder zumindest sehr häufig) Verwendung finden und nur in Ausnahmefällen davon abgewichen werden wird.

Die Anregung des LfD, eine Regelung im System vorzusehen, wonach die Klärung eines Falles zwingend zu erfassen und daraufhin eine im Einzelfall gesondert festzulegende Löschungsfrist einzutragen ist, konnte bisher aus technischen Gründen nicht umgesetzt werden.

– Zur Aufbewahrungsdauer der „Kerndaten“:

Der Umfang der nach Löschung der „Vorgangsdaten“ verbleibenden „Kerndaten“ ist so groß, dass diese Daten aus datenschutzrechtlicher Sicht sensible personenbezogene Informationen enthalten. Andererseits sind die Informationen aber auch so reduziert, dass allein dadurch für betroffene Personen ein erheblicher Belastungseffekt entstehen kann. Hinzu kommt, dass sie mit Hilfe einer Suchfunktion uneingeschränkt auswertbar sind.
Angesichts der Zugriffsmöglichkeiten auf die Kerndaten und ihrer Auswertbarkeit werden diese auch für die Ermittlungstätigkeit eine Rolle spielen. Dieser Umstand hat nach Auffassung des LfD wiederum Auswirkungen auf die zulässige Dauer der Speicherungen. So äußerte er erhebliche Bedenken gegen eine Speicherfrist von pauschal zehn Jahren für die Kerndaten, wobei die Frist erst mit der Löschung der Vorgangsdaten beginnen würde.
Das Innenministerium hat daraufhin deliktsbezogen differenzierte Speicherfristen festgelegt, die zwischen drei Monaten und – in einer geringen Zahl der Fälle – zehn Jahren betragen.

– Zur Zugriffsmöglichkeit auf „Belegdaten“:

Im Rahmen von POLADIS-neu beabsichtigt das Innenministerium ergänzend, dass sog. Belegdaten von jedem PC der Polizei, also auch außerhalb des Exekutivbereichs, abfragbar sein sollen. Bei diesen Daten handelt es sich um Informationen, die zum Auffinden von Vorgängen bzw. zum Erkennen der sachbearbeitenden Stelle dienen sollen. Belegdaten enthalten zwar keine personenbezogenen Daten, jedoch ist es mit ihrer Kenntnis möglich, bei entsprechendem Teilwissen wie z. B. Delikt, Tatzeit, Tatort die Zuordnung von Straftaten zu Personen vornehmen zu können.

Gegen die ursprünglich vorgesehene umfassende Datenfreigabe hatte der LfD Bedenken und regte deshalb eine Begrenzung des Nutzerkreises im Rahmen des Erforderlichen an. Daraufhin schränkte das Ministerium durch eine entsprechende Änderung der Errichtungsanordnung den Nutzerkreis auf die Stellen ein, die bei der Polizei mit der regelmäßigen Suche nach Vorgängen beauftragt sind. Es ist jedoch zurzeit nicht möglich, durch technische Regelungen den Zugriff auf den Belegdatenbestand durch nicht berechtigte Polizeibedienstete zu verhindern. Der LfD hält diese Situation aus datenschutzrechtlicher Sicht noch nicht für zufrieden stellend.

5.3 INPOL-neu

Bei INPOL-neu handelt es sich um das bundesweite polizeiliche Informationssystem, das das bisherige Verfahren INPOL ablösen soll. Dieses System wird mit dem Vorgangsbearbeitungssystem POLADIS-neu der rheinland-pfälzischen Polizei gekoppelt, so dass Mehrfacherfassungen der gleichen Daten entbehrlich werden. Eine Nutzung von INPOL-neu, die ab dem 15. April 2001 im Parallelbetrieb zu INPOL geplant war, ist bisher wegen technischer Schwierigkeiten nicht möglich gewesen.

Von der technischen Konzeption her handelt es sich bei INPOL-neu im Vergleich zu INPOL um ein völlig anderes System. Waren bisher die Daten über eine Person in verschiedenen Teildateien gespeichert, so sollen nun dem Datensatz einer Person alle über sie gespeicherten Informationen zugeordnet werden. Ob diese Planung in absehbarer Zeit umfassend verwirklicht werden kann, ist derzeit aus technischen und arbeitsökonomischen Gründen fraglich. Beispielsweise würde die Übernahme der Daten aus der erheblichen Anzahl der beim BKA bestehenden Sonderdateien einen großen Aufwand erfordern.

Im Zusammenhang mit der Konzeption von INPOL-neu gab es zahlreiche datenschutzrechtliche Probleme, die noch nicht alle zufrieden stellend gelöst werden konnten.

So ist gegenwärtig von den Ländern beabsichtigt, ihre INPOL-neu-Datenbestände nicht selbst zu speichern, sondern – überwiegend aus Zeit- und Kostengründen – in der Form der Auftragsdatenverarbeitung beim BKA vornehmen zu lassen. Diese Form der Datenverarbeitung ist nach § 2 Abs. 5 BKAG möglich, jedoch nach Auffassung der Datenschutzbeauftragten des Bundes und der Länder nicht in dieser umfassenden Form auf unbestimmte Dauer. Die Datenschutzbeauftragten haben in einer gemeinsamen Entschließung ihre Sorge darüber zum Ausdruck gebracht, dass bei einer dauerhaften Speicherung der Landesdaten beim BKA die Trennung der Datenbestände aufgeweicht wird bzw. die direkten Zugriffe auf Landesdaten von außerhalb zunehmen könnten (vgl. Anlage 19).
Die Datenschutzbeauftragten befürchten, dass durch eine solche Verfahrensweise die Vorschrift des § 2 Abs. 1 BKAG, wonach beim BKA nur Daten über Straftaten von länderübergreifender, internationaler oder sonst erheblicher Bedeutung gespeichert werden dürfen, unterlaufen wird.

Weiterhin ist datenschutzrechtlich von Belang, dass die Verantwortung über die von den Ländern gespeicherten Daten, insbesondere was die Löschungs- und Prüffristen betrifft, bei den Ländern verbleibt.

Außerdem ist Sorge dafür zu tragen, dass die Zugriffsmöglichkeiten bei einer umfassenden Speicherung personenbezogener Daten in einer einzigen Datei in differenzierter Form im Rahmen der jeweiligen Erforderlichkeit geregelt werden. So ist z. B. bei einer allgemeinen Abfrage zu einer Person bisher in jedem Fall zu erkennen, ob über diese Person eine DNA-Analyse gespeichert ist. Dies ist eine Information, die in den meisten Fällen für den Zweck der Abfrage nicht erforderlich sein dürfte. Die Freigabe dieser Information sollte von einer gesonderten Abfrage, die wiederum zu protokollieren wäre, abhängig gemacht werden.

Bei den Abfragen in Verbunddateien des BKA wird gemäß den Anforderungen des BKAG nur jeder zehnte Zugriff protokolliert. Nach Auffassung des LfD ist jedoch in INPOL-neu zu Kontrollzwecken eine Vollprotokollierung einzurichten, wie dies auch in POLADIS-neu geschehen ist. Der LfD setzt sich deshalb dafür ein, dass eine vollständige Protokollierung aller rheinland-pfälzischen Zugriffe auf INPOL-neu auf Landesebene erfolgt.

Das weitere Schicksal von Inpol-neu ist derzeit ungewiss.
Der LfD wird sich – in Übereinstimmung mit den Datenschutzbeauftragten des Bundes und der Länder – auch künftig für eine datenschutzkonforme Ausgestaltung dieses Systems entsprechend den o. g. Anforderungen einsetzen.

5.4 Erfassung von Rauschgiftdelikten im „KAN-Bund“ und in der „Falldatei Rauschgift“ (FDR)

Im „Kriminalakten-Nachweis-Bund“ und in der „Falldatei Rauschgift“ – beides Dateien, die beim BKA im Verbund der Polizeien des Bundes und der Länder geführt werden – sollen alle Beschuldigten in Betäubungsmittel-Strafverfahren registriert werden. Hierdurch wird jede Person, die eines Vergehens nach dem Betäubungsmittelgesetz beschuldigt wird, bundesweit für den Zugriff aller Polizeibeamter gespeichert. Dies ist auch dann der Fall, wenn es sich um weniger schwer wiegende Delikte, wie zum Beispiel um den erstmaligen Besitz einer geringen Menge Haschisch zum Eigenverbrauch handelt.

Mit dieser Regelung konnte der LfD nicht einverstanden sein, da nach seiner Auffassung die Erforderlichkeit der Speicherung geringfügiger Delikte in einer Bundesdatei nicht gegeben ist. Eine solche Speicherung ist auch nach § 2 Abs. 1 BKA-Gesetz nicht zulässig, wonach eine Unterstützungskompetenz des BKA auf den Bereich der Verhütung und Verfolgung von Straftaten mit länderübergreifender, internationaler oder erheblicher Bedeutung begrenzt ist.

Als Ergebnis der Einwände des LfD wurde auf Veranlassung des Innenministeriums für die rheinland-pfälzische Polizei die Regelung getroffen, dass in folgenden Fällen eine Speicherung von Daten sowohl im „Kriminal-Akten-Nachweis-Bund“ als auch in der „Falldatei Rauschgift“ unterbleibt:

- Besitz von weniger als zehn Gramm Haschisch oder Marihuana zum Eigenverbrauch in weniger als drei Fällen,
- Straftaten mit anderen Betäubungsmitteln, die nicht zu den harten Drogen zählen (z. B. Psilocybinpilze oder Kath) in Mengen bis zu einem Gramm.

Gegen diese Regelung, die weiterhin eine Erfassung der Verbraucher harter Drogen und alle Straftäter im Zusammenhang mit dem Rauschgifthandel in den bundesweiten Dateien ermöglicht, hatte der LfD keine Bedenken.

5.5 Speicherung von Haftmitteilungen der Justizvollzugsanstalten in den polizeilichen Informationssystemen

Im Rahmen der Bearbeitung einer Eingabe wurde der LfD auf folgendes Problem aufmerksam:

Von den Justizvollzugsanstalten werden in allen Bundesländern gemäß § 13 Abs. 1 Satz 3 BKAG ausnahmslos alle Freiheitsentziehungen, die wegen einer rechtswidrigen Tat von einem Richter angeordnet wurden, der örtlichen Polizei übermittelt. Sie werden dort in das polizeiliche Informationssystem eingegeben, wobei eine pauschale Speicherdauer von zwei Jahren festgelegt wird. So konnte es geschehen, dass mit Datum vom 1. August 2000 in Rheinland-Pfalz 2 438 Personen erfasst waren, zu denen keine gesonderten Angaben über ein Delikt gemacht wurden. Die Speicherung war also ausschließlich wegen der Haftmitteilung erfolgt, während die für die Sachbearbeitung des Falles zuständige Dienststelle eine Speicherung nicht für erforderlich gehalten hatte. Da der LfD dieses Verfahren datenschutzrechtlich für bedenklich hält, hat er eine entsprechende Anfrage an das Ministerium des Innern und für Sport gerichtet.

In seiner Antwort teilt das Ministerium im Wesentlichen die Bedenken des LfD und weist darauf hin, dass es das LKA gebeten habe, zusammen mit den anderen Verbundteilnehmern zu klären, ob sachgerechte Problemlösungen gefunden werden können.

Aus einer weiteren Mitteilung des Innenministeriums geht hervor, dass in Verbindung mit der derzeitig stattfindenden Einführung neuer polizeilicher Informationssysteme keine Haftspeicherungen erfolgen, wenn nicht zuvor die sachbearbeitende Stelle eine Speicherung der Straftat vorgenommen hat. Damit wäre eine datenschutzgerechte Regelung der Haftspeicherungen erreicht.

5.6 DNA-Merker

Von der Polizei wurde nach einer Möglichkeit gesucht, schnellstmöglich festzustellen, ob über eine Person bereits ein DNA-Muster vorliegt. Auf Vorschlag des BKA war hierfür ein entsprechender Merker im sog. „USV"-Feld im bundesweiten elektronischen Informationssystem INPOL vorgesehen.

Im USV-Feld werden grundsätzlich Angaben über Straftaten einer Person gespeichert. In dem mit INPOL verknüpften Informationssystem des Landes (POLIS) sind Angaben über alle Straftaten, in INPOL nur Straftaten von überregionaler Bedeutung verzeichnet. Eine Einstellung des DNA-Merkers in das bestehende USV-Feld hätte zur Folge gehabt, dass bundesweit alle Straftaten, also nicht nur die überregional bedeutsamen, erkennbar geworden wären.

Der LfD wandte sich gegen diese Regelung, zumal sie auch den Vorgaben des BKA-Gesetzes widerspricht. Daraufhin wurde den datenschutzrechtlichen Belangen dadurch Rechnung getragen, dass für jede Speicherung eines DNA-Merkers ein zusätzliches USV-Feld geschaffen wird, das darüber hinaus keine weiteren Informationen enthält. Somit bleibt die bisherige Trennung bei den Abfragemöglichkeiten in überregional bedeutende einerseits und vollständige Dateieninhalte andererseits weiterhin erhalten.

5.7 Anmeldung von EDV-Verfahren nach § 27 Abs. 1 LDSG

Im Berichtszeitraum wurden zahlreiche neue Verfahren sowohl als Verbunddateien beim BKA wie auch als landesweite oder Einzeldateien der Polizeibehörden in Betrieb genommen. Der LfD gab hierzu zahlreiche Anregungen, die auf Landesebene im Wesentlichen umgesetzt wurden. Er hat bei den Verfahrensanmeldungen folgende datenschutzrechtliche Aspekte aufgegriffen:

- Verbunddateien des BKA sollten in einer Errichtungsanordnung den Inhalt des § 2 Abs. 1 BKAG sinngemäß wiedergeben, wodurch die Begrenzung auf den Bereich der Verhütung und Verfolgung von Straftaten mit länderübergreifender, internationaler oder erheblicher Bedeutung gesichert werden soll.
- In Errichtungsanordnungen für Verbunddateien erfolgte grundsätzlich ein Hinweis auf die nach dem BKAG im Höchstfall zulässigen Prüf- und Speicherfristen. Der LfD hat immer wieder darauf hingewiesen, dass er die Festlegung von differenzierten Prüf- und Speicherfristen, die sich an der Art der Datei und dem Inhalt der Speicherungen orientieren, für erforderlich hält.
- Zum Nachweis der Zugriffe auf Dateien forderte der LfD auf Landesebene die Vollprotokollierung. Er hält die im BKAG festgelegte Protokollierung jedes zehnten Zugriffs nicht für ausreichend zur Ausübung einer wirksamen Kontrolltätigkeit.
- Gegen die beabsichtigte pauschale Verlängerung der Speicherfrist in der bundesweit nutzbaren Datei „Gewalttäter Sport" auf die Dauer von fünf Jahren hat der LfD Bedenken geäußert, da nach seinen Feststellungen in dieser Datei zahlreiche Personen gespeichert sind, die selbst noch nicht gewalttätig geworden waren. Für den Bereich Rheinland-Pfalz wurde durch das Innenministerium eine Prüffrist von zwei Jahren festgelegt.

- Für den Einsatz des neuartigen Datenbanksystems „ViCLAS", das der Auswertung von Gewaltdelikten dient, gab der LfD Anregungen, die die Bereiche der Protokollierung, der Zustimmung durch die Betroffenen und der Verschlüsselung betrafen. Die Anregungen wurden in eine Ergänzungsregelung zur Errichtungsanordnung der Datenbank aufgenommen.
- Im Zusammenhang mit einer Verbunddatei gab der LfD zur Verlängerung von Prüffristen folgende Hinweise:

Eine Verlängerung der Prüffrist ist nur zulässig, wenn sich aus den einzelfallabhängigen Verhältnissen die Notwendigkeit der weiteren Speicherung ergibt. Dabei müssen in der Zwischenzeit nicht zusätzliche Erkenntnisse hinzugekommen sein. Umgekehrt kann aber auch die Löschung nicht vom Vorliegen neuer Erkenntnisse, die die Löschung begründen, abhängig gemacht werden. Der Ablauf der Prüffrist begründet vielmehr ein gewisses Indiz, dass bei ihrer Festlegung jedenfalls eine längere Speicherung als nicht zwingend erforderlich angesehen wurde. Eine Verlängerung kann also keinesfalls routinemäßig erfolgen; dann wäre die Prüffrist von Beginn an unzutreffend kurz bemessen gewesen. Bei der Verlängerung sind kürzere erneute Prüffristen zu bestimmen (im Bundesbereich im Regelfall nicht mehr als drei Jahre, vgl. Störzer in Ahlf/Daub/Lersch/Störzer, BKAG-Komm., Anm. 32 zu § 32). Dabei sind selbstverständlich absolute Speicherungshöchstfristen und u. U. auch besondere absolute Verwertungsverbote zu beachten.

5.8 Videoaufnahmen durch Streifenwagen der Polizei

Es besteht die Planung, die Streifenfahrzeuge der Polizei mit Videokameras auszustatten. Zweck dieser Videokameras ist ausschließlich die Eigensicherung der Polizeibeamten bei der Durchführung von konkreten Kontrollen. Dementsprechend wird die Kamera nur dann aktiviert, wenn die Leuchtschrift „Stop Polizei" aufleuchtet, um einen vorausfahrenden Wagen anzuhalten. Die Aufnahmeaktivität der Kamera wird durch ein rotes Blinklicht auch nach außen erkennbar.

Eine zentrale Anforderung des LfD in diesem Zusammenhang ist, dass die Aufnahmen nur dann weiter verwendet bzw. genutzt werden dürfen, wenn im Rahmen der Personen- und Fahrzeugkontrolle rechtswidrige Handlungen erfolgt sind und die gefertigten Aufnahmen zur Aufklärung und zur Beweissicherung dieser Handlungen dienen können. In allen anderen Fällen, das heißt also sicherlich in der übergroßen Mehrzahl der Fälle, sind die Aufnahmen unverzüglich zu löschen. Ein geeigneter Zeitpunkt wäre das Ende der Streifenfahrt. Es ist derzeit geplant, eine Technik einzusetzen, bei der die Aufnahmegeräte gekapselt und verschlossen werden. Dann sollen die eingesetzten Videobänder grundsätzlich im Gerät belassen und kontinuierlich überspielt werden, wenn kein Grund zur Nutzung zu Beweissicherungszwecken besteht.

Ausnahmsweise sollen die Videoaufzeichnungen auch zu Fortbildungszwecken der konkret eingesetzten Streifenwagenbesatzungen unter definierten Bedingungen stichprobenweise unter Hinzuziehung des Dienstgruppenleiters betrachtet werden, um Hinweise auf Fehler oder Verbesserungen beim Einsatz geben zu können. Diese ausnahmsweise erfolgenden Nutzungen sollen kontrolliert und dokumentiert erfolgen. Die Einzelheiten des technischen Systems und des Verfahrens bei der Nutzung der Aufnahmen werden gegenwärtig noch mit dem Innenministerium erörtert.

Nach dem derzeitigen Informationsstand des LfD werden die bereits in zwei Streifenwagen der rheinland-pfälzischen Polizei zu Demonstrations- und Erprobungszwecken eingebauten Videoaufzeichnungsgeräte noch nicht im Echteinsatz genutzt.

Rechtsgrundlage für den Einsatz dieses Verfahrens ist § 25 a Abs. 1 Nr. 1 POG. Danach dürfen Daten erhoben werden, wenn dies zur Abwehr konkreter Gefahren erforderlich ist. Nach Auffassung des LfD kann davon ausgegangen werden, dass jede Kontrollmaßnahme gegenüber unbekannten Personen eine besondere Gefährdung der tätig werdenden Polizeibeamten begründet. Dies ist auf tragische Weise in der letzten Zeit in verschiedenen Einzelfällen deutlich geworden. Die hier erfolgende Datenerhebung ist grundsätzlich geeignet, diese Gefährdung zu reduzieren. Sie ist auch verhältnismäßig, wenn die angesprochenen datenschutzrechtlichen Anforderungen beim Umgang mit den erhobenen Daten beachtet werden.

Ergänzend hat der LfD darauf hingewiesen, dass eine Beteiligung der Personalvertretung vor der Einführung dieses Verfahrens erforderlich ist. Das Beteiligungsverfahren wurde zwischenzeitlich eingeleitet.

5.9 Abhören von Mobiltelefonen mit einem Abhörgerät, bei dem Unbeteiligte erfasst werden

Nach Meldungen in den Medien nutzen deutsche Polizeibehörden ein nicht zugelassenes Gerät zur Überwachung der Mobilfunkkommunikation. Danach sollen Bundeskriminalamt und Bundesgrenzschutz in den vergangenen Jahren in mindestens 30 Fällen sog. „IMSI-Catcher" („IMSI" steht für „International Mobile Subscriber Identity") zur Feststellung der Verbindungsdaten von Handy-Nutzern eingesetzt haben.

Dieses Gerät fungiert in einem bestimmten räumlichen Umkreis als „Basisstation" oder „Funkvermittlungsstelle" und kann Signale von allen Mobiltelefonen auffangen, die aktiv geschaltet sind. Der Einsatz solcher Geräte ermöglicht, die Verbindungsdaten der jeweiligen aktivierten Telefongeräte aufzuzeichnen. Er ermöglicht darüber hinaus aber auch grundsätzlich, die geführten Gespräche im Klartext abzuhören.

Der Einsatz entsprechender Geräte ist bereits im Jahr 1997 im Land erörtert worden. Damals hatte das Innenministerium erklärt, dass nach geltender Rechtslage der Einsatz der seinerzeitigen Geräteversionen sowohl gegen das Fernmeldeanlagengesetz als auch gegen das Telekommunikationsgesetz (§ 47 TKG) verstoßen würde. Außerdem wurde festgestellt, dass im Zuständigkeitsbereich des Ministeriums des Innern und für Sport entsprechende Geräte bisher weder vorgestellt noch erprobt worden seien.

Zwischenzeitlich wurde mitgeteilt, dass auch in unserem Bundesland diese Technik – allerdings nur in wenigen Fällen – eingesetzt wurde. Eine vorherige Mitteilung an den LfD war nicht erfolgt. Der LfD erörtert derzeit die Zulässigkeit des Einsatzes dieser Technik mit den zuständigen Ressorts.

5.10 Wahllichtbildvorlage

In polizeilichen Ermittlungsverfahren kann es zu Beweiszwecken erforderlich sein, bei Vorliegen eines Tatverdachtes gegen eine bestimmte Person einem Zeugen ein Lichtbild des Verdächtigen vorzulegen. Um eine Erkennung des Verdächtigen zu erschweren und dadurch deren Beweiskraft zu erhöhen, werden außer dem Bild des Verdächtigen gleichzeitig mehrere Bilder von Unverdächtigen vorgelegt. Für den Fall, dass der Zeuge unter den Bildern der Unverdächtigen eine ihm bekannte Person erkennt, kann er den Rückschluss ziehen, dass diese Person bereits als Beschuldigter in einem Strafverfahren erkennungsdienstlich behandelt wurde.

Diese Informationsübermittlung ist nach Auffassung des LfD nicht zulässig. Er forderte deshalb schon mehrfach, für diese Zwecke einen Vorrat anonymisierter Lichtbilder zu schaffen. Seitens des Ministeriums des Innern und für Sport wurde nun mitgeteilt, dass die Fertigung von synthetischen Bildern im Rahmen der Ausstattung des polizeilichen Erkennungsdienstes mit digitalen Fotogeräten beabsichtigt sei. Da diese Technik in einem relativ kurzen Zeitraum – bis Ende 2001 – eingeführt werden soll, erklärte der LfD seine Bereitschaft, seine bisher geäußerten Bedenken zur gegenwärtigen Form der Wahllichtbildvorlage zurückzustellen.

5.11 Konzeption zur Intensivierung der Zielfahndung

Mit dem Ziel einer klareren Regelung und effektiveren Gestaltung der Zielfahndung, welche nur in einzelnen ausgewählten Fällen nach besonders gefährlichen Straftätern ausschließlich vom LKA betrieben wird, wurde eine neue Konzeption erstellt. Hiergegen bestanden keine grundsätzlichen datenschutzrechtlichen Bedenken.

Nach dieser Konzeption waren zu Fahndungszwecken Anfragen an die Krankenkassen und die Sozialämter vorgesehen. Vom LfD wurde in diesem Zusammenhang darauf hingewiesen, dass diese Anfragen den besonderen Regelungen des SGB X unterliegen. Hiernach können Auskünfte an die Polizei verweigert werden, wenn die Informationen auf andere Weise beschafft werden können. Auch bedürfen Auskünfte, die über bestimmte Personaldaten hinausgehen, der richterlichen Anordnung.

Auf Anregung des LfD wurden in die Konzeption Ergänzungen aufgenommen, die diese Anforderungen deutlich herausstellen.

5.12 Übermittlung von Daten aus Gewerbeanzeigen durch die Kommunalbehörden an die Polizei

Zwei Polizeidienststellen richteten Ersuchen an eine Kommunalbehörde, ihnen monatlich Aufstellungen von ortsansässigen Gewerbebetrieben zu übermitteln. Die Erforderlichkeit der Nutzung dieser Informationen wurde von der Polizei damit begründet, dass die Polizeidienststellen außerhalb der allgemeinen Dienstzeiten der Kommunalverwaltung auch ortspolizeiliche Aufgaben wahrnähmen und hierzu die Informationen über die Gewerbebetriebe erforderlich seien.

Die betreffende Kommunalbehörde fragte beim LfD an, ob die Übermittlung der erbetenen Daten an die Polizei rechtmäßig sei. Er übersandte der Kommune folgende Stellungnahme:

Wird die Polizei bei ordnungspolizeilichen Aufgaben tätig, so geschieht dies im Rahmen von § 1 Abs. 6 POG. Nach dieser Bestimmung ist die Abwehr von Gefahren für andere Behörden, wenn deren Tätigwerden nicht oder nicht rechtzeitig möglich erscheint, Aufgabe der Polizei.

Hat die Polizei jedoch, wie in diesem Fall von ihr geschildert wird, Gefahren anlässlich von Straftaten oder Bränden zu beseitigen, so ist sie hierzu originär nach § 1 Abs. 1 POG zuständig. Die Übermittlung von Informationen aus der Gewerbeanzeige an öffentliche Stellen – wie hier die Polizei – ist in § 14 Abs. 6 GewO geregelt. Nach § 14 Abs. 6 Satz 1 GewO ist eine fallweise Übermittlung bestimmter Daten, nämlich Name, betriebliche Anschrift und angezeigte Tätigkeit im Rahmen der Erforderlichkeit zulässig. „Fallweise“ ist hierbei nicht im Sinn von einzelnen Fällen zu verstehen, sondern schließt auch einzelne Fallgruppen ein. Dabei wären auch z. B. die einmalige Übermittlung bestimmter Gewerbebetriebe aus besonderem Anlass oder die faktisch regelmäßige Übermittlung von Daten einer bestimmten Art von Gewerbebetrieben möglich; entscheidend ist die für diese „Fälle“ zu begründende Erforderlichkeit (siehe hierzu Tettinger/Wank, Kommentar zur GewO, 6. Auflage, Randziffer 113 zu § 14).

Daraus ergibt sich aus der Sicht des LfD, dass der Polizei keine Auflistung aller Gewerbebetriebe regelmäßig übermittelt werden darf, sondern eine Auswahl nach der Erforderlichkeit getroffen werden muss, da sicher ausgeschlossen werden kann, dass ausnahmslos alle Gewerbetreibende in gleichem Maß potentielle Adressaten von Maßnahmen zum Zweck der Gefahrenabwehr sind. Insbesondere im Bereich des nichtproduzierenden Gewerbes und des Dienstleistungssektors (z. B. Schreibbüros, Buchführungsstellen, Händler ohne eigenes Lager und Ladenlokal etc.) gibt es sicher zahlreiche Gewerbetreibende, dren Identität für die Polizei unter dem Gesichtspunkt der oben angesprochenen Eilkompetenz nicht von Interesse ist.

Weitere Daten, wie zum Beispiel die im Schreiben der Polizei aufgeführte Privatadresse, dürfen nach § 14 Abs. 6 Satz 2 GewO nur übermittelt werden, wenn

- dies zur Abwehr erheblicher Nachteile für das Gemeinwohl oder einer sonst unmittelbar drohenden Gefahr für die öffentliche Sicherheit erforderlich ist oder
- die Empfänger die Daten beim betreffenden Gewerbetreibenden nur mit unverhältnismäßig hohem Aufwand erheben könnten oder von einer solchen Datenerhebung nach der Art der Aufgabe, zu der die Daten erforderlich sind, abgesehen werden muss und kein Grund zur Annahme besteht, dass das schutzwürdige Interesse des Gewerbetreibenden überwiegt.

Erhebliche Nachteile für das Gemeinwohl dürften zu befürchten sein, wenn z. B. im Falle eines Brandes eine erhöhte Gefährdung von Personen oder Sachen von bedeutendem Wert anzunehmen ist oder wenn in dem Gewerbebetrieb Stoffe gelagert werden, die im Falle eines unkontrollierten Austrittes Umweltschädigungen größeren Ausmaßes verursachen können. Bei Betrieben dieser Art hält der LfD die Übermittlung weiterer Daten an die Polizei im Rahmen der Erforderlichkeit für zulässig. Ein überwiegendes schutzwürdiges Interesse des Gewerbetreibenden, das der Übermittlung dieser Daten an die Polizei entgegenstehen könnte, ist im Vergleich zur Verhinderung erheblicher Nachteile für das Gemeinwohl nicht zu erkennen.

In anderen Fällen der Gefahrenabwehr ist für die Übermittlung weiterer Daten das Vorliegen einer konkreten Gefahr gefordert, die jedoch bei den genannten Sachverhalten nicht gegeben ist.

Auch dürfte es für die Polizei leicht möglich sein, wenn ihr Name und Anschrift eines Gewerbebetriebes bereits mitgeteilt worden sind, ggf. weitere für ihre Aufgabenerfüllung erforderliche Daten bei dem Gewerbetreibenden selbst zu erheben. Somit wäre kein unverhältnismäßig hoher Aufwand erforderlich und eine Übermittlung weiterer Daten aus diesem Grund nicht zulässig.

In Bezug auf die Übermittlung von Daten aus den Gewerbeanzeigen an die Polizei ist zusammenfassend festzustellen, dass Meldungen mit dem Namen und der Adresse des Gewerbebetriebes sowie der Tätigkeit übermittelt werden dürfen, sofern dies wegen der Art des Betriebes für die Erfüllung der polizeilichen Aufgaben erforderlich ist.

Die Übermittlung weiterer Daten an die Polizei ist nur zulässig, wenn von dem Betrieb ausgehende erhebliche Nachteile für das Gemeinwohl zu befürchten sind und die Datenübermittlung zur Abwehr dieser Nachteile erforderlich ist.

Das Ministerium des Innern und für Sport hat sich dieser Auffassung angeschlossen.

5.13 Datenübermittlung der Polizei zur Ausführung von § 11 Gewerbeordnung

Aus der polizeilichen Praxis wurde folgende Frage an den LfD gerichtet:

Dürfen Daten, die aus Anlass von Straftaten, die in einer Gaststätte begangen wurden, von der Polizei zum Zwecke der Gefahrenabwehr verarbeitet wurden, an die für die Ausführung des Gaststättengesetzes zuständigen Stellen übermittelt werden, ohne dass ein entsprechendes Ersuchen vorliegt?

Diese Frage beantwortete der LfD aus datenschutzrechtlicher Sicht wie folgt:

Wenn Straftaten in Gaststätten begangen wurden, kann Zweck der polizeilichen Datenverarbeitung neben der Strafverfolgung auch die vorbeugende Bekämpfung von Straftaten sein. Rechtsgrundlage hierfür ist § 25 a Abs. 1 Nr. 2 POG. Demzufolge darf die Polizei diese Daten aus den polizeilichen Sammlungen im weiteren Sinne an die für die Ausführung des Gaststättengesetzes zuständige Stelle übermitteln, wenn dies zur Erreichung des Zwecks „vorbeugende Bekämpfung von Straftaten“ oder eines anderen zulässigen polizeilichen Zwecks erforderlich ist. Das Ziel der Übermittlung ist Teil des Aufgabenbereichs der Polizei; ein Ersuchen der datenempfangenden Stelle ist nicht erforderlich.

Voraussetzung für die Rechtmäßigkeit der Übermittlung ist außerdem noch, dass die empfangende Stelle zur Verarbeitung dieser Daten berechtigt ist. Dies ist im vorliegenden Fall gegeben (§§ 25 a Abs. 1 a POG, 31 GaststättenG, 11 Abs. 1 Nr. 1 GewO).

Für die Rechtmäßigkeit der Datenübermittlung ist grundsätzlich unerheblich, welche zusätzlichen oder alternativen Zwecke die empfangende Stelle mit den Daten verfolgt, sofern diese eigenen Zwecke zulässig sind und nicht im Widerspruch zu den polizeilichen Zwecken stehen.

5.14 Dienstanweisung der Polizei zum Datenschutz

Aufgrund der Änderung des Landesdatenschutzgesetzes vom 5. Juli 1994 war eine Neufassung der vom 23. März 1989 stammenden Dienstanweisung über den Datenschutz und die Datensicherheit bei der Polizei erforderlich geworden. Dieses Erfordernis ergab sich insbesondere aus § 9 Abs. 1 und 5 LDSG, wonach technisch-organisatorische Maßnahmen zum Schutz personenbezogener Daten bei deren Verarbeitung zu treffen und diese Sicherungsmaßnahmen durch Dienstanweisungen festzulegen sind.

Nach mehreren Entwurfsvorlagen, die im Wesentlichen durch die fortschreitende Entwicklung im technischen Bereich bedingt waren, trat am 15. September 2000 eine Rahmendienstanweisung in Kraft (Rundschreiben des Ministeriums des Innern und für Sport an die Polizeipräsidien, das LKA sowie die sonstigen polizeilichen Einrichtungen vom 16. August 2000, Az.: 346/08610). Die vom LfD gegebenen Anregungen wurden dabei berücksichtigt.

5.15 Richtlinie über Auskünfte der Polizei an Ordnungsbehörden

Das Anliegen des LfD, eine Richtlinie über Auskünfte der Polizei an Ordnungsbehörden im Rahmen von Zuverlässigkeits- bzw. Eignungsprüfungen zu erstellen, wurde vom Innenministerium bisher noch nicht umgesetzt.

Dem LfD wurde bisher lediglich eine Regelung übermittelt, wonach nur im Rahmen eines waffenrechtlichen Erlaubnisverfahrens und nur in begründeten Einzelfällen die Staatsanwaltschaften von den Waffenbehörden um Auskunft ersucht werden können.

Der LfD begrüßt diese restriktive Verfahrensweise, teilte dem Ministerium aber mit, dass er keine grundsätzlichen Bedenken gegen eine weniger einschränkende Regelung habe. Des Weiteren übermittelte er erneut seine Auffassung, dass er Regelungen oder zumindest klarstellende Hinweise über Auskünfte in anderen Bereichen, wie z. B. im Verkehrs-, Gaststätten-, Gewerbe-, Fischerei-, Jagd- und Sprengstoffrecht, weiterhin für erforderlich hält.

5.16 Presserichtlinie

Wie bereits im 17. Tb. unter Tz. 5.6 aufgeführt, hält der LfD die Regelung der Presse- und Öffentlichkeitsarbeit der Polizei durch eine Richtlinie für erforderlich. Eine solche Richtlinie wurde nunmehr geschaffen und trat mit Beginn des Jahres 2000 in Kraft. Zuvor wurden im Stadium des Entwurfs der Richtlinie Anregungen durch den LfD gegeben. Insbesondere ging es hierbei um den Schutz von Betroffenen bei der Mitwirkung der Polizei an Fernsehproduktionen. Nach der endgültigen Fassung der Richtlinie ist die Zustimmung von Bürgern und Bürgerinnen erforderlich, bevor sie Objekt solcher Fernsehaufzeichnungen werden. Damit wurde den Anregungen des LfD entsprochen.

5.17 Aufbewahrung von beschlagnahmten Patientenunterlagen bei der Polizei

Eine Ärztin beschwerte sich beim LfD darüber, dass Patientenunterlagen, die im Rahmen eines Ermittlungsverfahrens in ihrer Praxis beschlagnahmt worden waren, bei der Polizei in einem Raum gelagert seien, in dem Publikumsverkehr stattfinde und dass darüber hinaus die Behältnisse, in denen sich die Unterlagen befänden, von weitem für die Besucher erkennbar mit dem Namen der Ärztin versehen seien.

Bei einer nicht angekündigten Überprüfung durch den LfD wurde dann festgestellt, dass die Akten in einem Raum lagerten, der grundsätzlich nicht für Publikum zugänglich ist, in dem sich aber im Anschluss an Durchsuchungen beschuldigte Ärzte aufhalten. Auch waren die Behauptungen über die Beschriftung der Unterlagen zutreffend.

Auf seine Anregung hin wurde dem LfD von der Polizeidienststelle zugesichert, dass die Beschriftung der Akten nunmehr in anonymisierter Form erfolge.

5.18 Datenschutzverstöße durch einzelne Polizeibeamte

Dem LfD wurde bekannt, dass ein Polizeibeamter im Auftrag einer Privatperson eine Abfrage in ZEVIS getätigt und die dadurch gewonnene Information über den Halter eines Kraftfahrzeuges seinem Auftraggeber übermittelt hatte.

Von der Polizeibehörde war bereits die Staatsanwaltschaft über den Vorfall informiert worden, die zunächst Ermittlungen wegen eines Vergehens nach § 203 StGB (Verletzung von Privatgeheimnissen) einleitete, dann aber das Verfahren nach § 170 Abs. 2 StPO einstellte. In der Einstellungsverfügung wies die Staatsanwaltschaft auf eine Entscheidung des Hanseatischen Oberlandesgerichtes Hamburg vom 22. Januar 1998 hin, wonach Daten aus dem Informationssystem ZEVIS als offenkundige Tatsachen angesehen werden, die weder geheim noch geheimhaltungsbedürftig sind. Demnach, so führt die Staatsanwaltschaft aus, fallen die vorgenannten Daten auch nicht unter den Schutzzweck des § 35 LDSG, der sich auf nicht offenkundige Daten bezieht.

In allen rechtshängig werdenden vergleichbaren Fällen beruft sich die Staatsanwaltschaft zur Begründung der regelmäßig erfolgenden Einstellungen des Strafverfahrens auf die o. g. Rechtsprechung, die allerdings aus der Sicht der Datenschutzbeauftragten unzutreffend ist. Diese haben angeregt, das Strafgesetzbuch klarstellend in dem Sinn zu ändern, dass auch unzulässige Datenabrufe durch grundsätzlich zum Abruf befugte Personen aus nicht öffentlich zugänglichen Dateien unter Strafe gestellt werden.

Nachdem das Strafverfahren eingestellt war, wurde dem Polizeibeamten von seiner Behörde durch die Verhängung einer Disziplinarmaßnahme seine dienstliche Verfehlung verdeutlicht.

In einem anderen Fall offenbarte ein Polizeibeamter seiner Lebensgefährtin Einwohnermeldedaten von deren Angehörigen. Die Daten hatte er, ohne dass ein dienstlicher Anlass gegeben war, aus EWOIS abgefragt. Dieses Vorgehen wurde von der Behörde im Rahmen einer Disziplinarmaßnahme geahndet.

Ein weiterer Datenschutzverstoß wurde auf einer Polizeiwache durch einen Besucher festgestellt, der dort sein eigenes Foto im Aushang entdeckte. Dieses Foto war zum Zweck der dienstlichen Information der dort tätigen Beamten ausgehängt, konnte aber auch von allen Besuchern der Wache wahrgenommen werden. Nach datenschutzrechtlicher Prüfung hatte der LfD keine Bedenken gegen den Aushang des Fotos zur Information der Beamten, wohl aber gegen die Einsichtnahme durch das Publikum. Nach Auskunft der Polizeidienststelle war das Lichtbild durch ein Versehen an dieser Stelle angebracht worden, was umgehend korrigiert wurde.

Dem LfD wurde bekannt, dass in wenigen weiteren Fällen Datenschutzverstöße durch Polizeibeamte begangen worden sind. Mit einer Ausnahme wurden diese Beamten namentlich festgestellt. Es erfolgten strafrechtliche oder dienstordnungsrechtliche Sanktionen, wobei in einem Fall die Entscheidung der Behörde über das Verhalten des Beamten noch aussteht.

6. Verfassungsschutz

Schwerpunkte der Tätigkeit des LfD im Bereich des Verfassungsschutzes waren die Überprüfung von Errichtungsanordnungen und internen Arbeitsanweisungen sowie die Bearbeitung von Bürgereingaben.

6.1 Auskunftsansprüche gegenüber dem Verfassungsschutz

Es ist hervorzuheben, dass die Zahl von Eingaben, die diesen Bereich betrafen, im Berichtszeitraum gegenüber den Vorjahren deutlich zurückgegangen ist. Die Eingaben betrafen ausnahmslos Auskunftsbegehren gegenüber dem Verfassungsschutz. Nach dem Landesverfassungsschutzgesetz besteht ein Anspruch auf Auskunft über die beim Landesverfassungsschutz in Dateien oder Akten gespeicherten Informationen (§ 18 Abs. 1 LVerfSchG). Die Auskunftsverpflichtung erstreckt sich allerdings nicht auf die Herkunft der Daten und auf die empfangende Stelle bei Übermittlungen. Über personenbezogene Daten in nichtautomatisierten Dateien und Akten, die nicht zur Person von Betroffenen geführt werden, ist Auskunft nur zu erteilen, soweit Angaben gemacht werden, die ein Auffinden der personenbezogenen Daten mit angemessenem Aufwand ermöglichen. Ein Recht auf Akteneinsicht besteht nicht.

Die Auskunftserteilung unterbleibt, soweit

- durch sie eine Gefährdung der Aufgabenerfüllung zu besorgen ist,
- durch sie Nachrichtenzugänge gefährdet sein können oder die Ausforschung des Erkenntnisstandes oder der Arbeitsweise der Verfassungsschutzbehörde zu befürchten ist,
- sie die öffentliche Sicherheit gefährden oder sonst dem Wohl des Bundes oder eines Landes Nachteile bereiten würde oder
- die Daten oder die Tatsache der Speicherung nach einer Rechtsvorschrift oder wegen der überwiegenden berechtigten Interessen Dritter geheim gehalten werden müssen (§ 18 Abs. 2 LVerfSchG).

Die Ablehnung einer Erteilung von Auskünften bedarf keiner Begründung. Eine solche Regelung verstößt nicht gegen das Grundrecht auf informationelle Selbstbestimmung (so jedenfalls das Urteil des Bayerischen Verfassungsgerichtshofs vom 11. November 1997 zu einer insoweit vergleichbaren bayerischen Landesregelung).

Praktische Schwierigkeiten sind nicht aufgetreten. Die Verfassungsschutzbehörde hat im Regelfall die erbetenen Auskünfte erteilt (die ausnahmslos zum Inhalt hatten, dass Speicherungen nicht vorlagen).

6.2 Anforderungen an eine Novellierung des Landesverfassungsschutzgesetzes im Bereich der Telekommunikationsüberwachung

In seinem Urteil vom 14. Juli 1999 zu Abhörmaßnahmen des Bundesnachrichtendienstes hat das Bundesverfassungsgericht Anforderungen an das staatliche Handeln im Bereich von Telekommunikationsüberwachungsmaßnahmen getroffen, die über den entschiedenen Fall hinaus bedeutsam sind: Immer dann, wenn das Fernmeldegeheimnis im öffentlichen Interesse eingeschränkt wird, hat der Gesetzgeber nach den Ausführungen des Bundesverfassungsgerichts flankierende verfahrenssichernde Maßnahmen vorzusehen, die dem Persönlichkeitsschutz dienen. Dazu gehören:

- Eine ausreichende externe Kontrolle von Eingriffen in das Fernmeldegeheimnis durch eine unabhängige Instanz. Wenn eine justizielle Kontrolle nicht möglich ist, hat an deren Stelle eine effiziente andere Institution zu treten, die auch die Überwachung der gesetzeskonformen Durchführung solcher Maßnahmen zu ihren Aufgaben zählt. Dies sind die parlamentarischen Gremien derzeit nicht. Angemessen wäre insoweit die gesetzliche Beauftragung des unabhängigen Datenschutzbeauftragten mit dieser Aufgabe.

- Es muss nach der Datenerfassung erkennbar bleiben, dass es sich um Daten handelt, die aus Eingriffen in das Fernmeldegeheimnis stammen. Von Verfassungs wegen ist daher eine entsprechende Kennzeichnung geboten. Diesbezügliche Regelungen sind in erster Linie in die Strafprozessordnung, aber auch etwa in das Landesverfassungsschutzgesetz aufzunehmen.

- Das Bundesverfassungsgericht hat weiter festgestellt, dass die Übermittlung der betreffenden Daten zu protokollieren ist, um eine hinreichende Kontrolle solcher Übermittlungen zu ermöglichen. Auch hier ist insbesondere das Landesverfassungsschutzgesetz zu ergänzen.

- Schließlich gilt bezüglich der Vernichtung und Löschung derartiger Daten eine Protokollierungspflicht. Auch diese ist im Landesverfassungsschutzgesetz vorzusehen. Der Landesgesetzgeber ist hier zum Tätigwerden aufgefordert.

Die Datenschutzbeauftragten des Bundes und der Länder haben hierzu eine gemeinsame Entschließung verfasst (s. Anlage 8), die der LfD auch den zuständigen Ressorts der Landesregierung übersandt hat. Eine Äußerung zu diesen Anliegen steht allerdings noch aus.

6.3 Video- und Tonaufzeichnungen von Veranstaltungen in geschlossenen Räumen

Gegenüber dem Verfassungsschutz wurde schließlich die Frage problematisiert, ob und in welchem Umfang eine Aufzeichnung extremistischer Aktivitäten bei Veranstaltungen in geschlossenen Räumen zulässig ist. Da diese Frage gegenwärtig noch in einem Rechtsstreit vor einem Verwaltungsgericht anhängig ist, hat der LfD es zunächst bei einem Austausch von Rechtsstandpunkten mit dem Verfassungsschutz des Landes belassen. Nach Abschluss des gerichtlichen Verfahrens wird er die Angelegenheit aber erneut aufgreifen und ggf. Änderungen der Praxis des Verfassungsschutzes in diesem Zusammenhang anregen.

6.4 Regelanfrage von Ausländerbehörden an den Verfassungsschutz vor Einbürgerungen

Hinsichtlich der Regelanfrage von Ausländerbehörden an den Verfassungsschutz vor Einbürgerungen hat der LfD eine Anfrage an das Ministerium des Innern und für Sport gestellt, die in dem Sinne beantwortet wurde, dass solche Regelanfragen nicht erfolgen würden. Nur bei Anhaltspunkten für verfassungsfeindliche oder extremistische Tätigkeiten des Einzubürgernden würden solche Anfragen erfolgen. Aus datenschutzrechtlicher Sicht ist dies eine angemessene Verfahrensweise.

7. Justiz

7.1 Kontrollbefugnis des Landesbeauftragten für den Datenschutz bei Gerichten

In Rheinland-Pfalz ist das Verhältnis des LfD zur Justiz in der Frage seiner Kontrollbefugnis bei Gerichten nach wie vor kontrovers. Es gibt seit langem einen offenen Dissens in der Frage, wie weit der Bereich der „Verwaltung der Gerichte“ im Sinne der Kompetenznormen des Landesdatenschutzgesetzes reicht, und dementsprechend, in welchem Umfang dem LfD Kontrollbefugnisse zustehen und Beratungspflichten obliegen (s. 16. Tb., Tz. 7; s. auch Tz. 7.9, Elektronisches Grundbuch, in diesem Tb.). Vergleichbare Probleme bestehen derzeit auch in den meisten anderen Bundesländern.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat zu dieser Grundsatzfrage eine einheitliche Auffassung formuliert, die mit der des LfD übereinstimmt (Entschließung der 56. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 5./6. Oktober 1998: Prüfungskompetenz der Datenschutzbeauftragten bei den Gerichten). Dort heißt es:

„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.“

Im 17. Tb. vom 18. Oktober 1999 hat der LfD ausgeführt: „Aus der Sicht des Landesbeauftragten für den Datenschutz sollte die anstehende Novellierung des Landesdatenschutzgesetzes dazu genutzt werden, Klarstellungen im Sinne des Grundrechts auf informationelle Selbstbestimmung und im Sinne der Bürger in das Gesetz aufzunehmen.“

Auch in Rheinland-Pfalz sollte also der in den Ländern Hamburg, Berlin und Schleswig-Holstein bereits erreichte datenschutzgesetzliche Standard in diesem Bereich übernommen werden. In diesen Ländern ist gesetzlich klargestellt, dass es zum Aufgabenbereich des LfD gehört, zumindest auch die Einhaltung des technisch-organisatorischen Datenschutzes bei den richterlichen Hilfsdiensten (z. B. den Geschäftsstellen der Gerichte) zu überwachen, insbesondere, wenn dort die EDV eingesetzt wird.

Der LfD bemüht sich darum, dass der Gesetzgeber in das zur Novellierung anstehende Landesdatenschutzgesetz eine klarstellende Formulierung aufnimmt.

Unabhängig von der ungeklärten und schwierigen juristischen Situation versucht er in der Praxis, möglichst umfassende Einblicke in die Automationsvorhaben der Gerichte zu erhalten. Dies wird im Allgemeinen auch durch das Justizministerium dadurch ermöglicht, dass es sich bereit erklärt, Informationsbesuche des LfD zu unterstützen. Konkrete Kontrollen auch im Bereich des

technisch-organisatorischen Datenschutzes in Gerichten konnten demgegenüber bislang nur in Randbereichen erfolgen. So hat eine entsprechende Kontrolle beispielsweise beim automatisierten Schuldnerverzeichnis in einem Amtsgericht stattgefunden (s. unter Tz. 7.10).

7.2 Parlamentarische Kontrolle von Lauschangriffen in den Bundesländern

Der sog. „große Lauschangriff", also das Abhören des gesprochenen Worts von Verdächtigen zu Zwecken der Strafverfolgung in Wohnungen, hat die Datenschutzbeauftragten lange und intensiv beschäftigt. Zuletzt war umstritten, wem gegenüber, in welcher Form (ob nicht öffentlich oder öffentlich) und wie intensiv die zuständigen Regierungen jeweils den Parlamenten über die Durchführung und den Erfolg solcher Maßnahmen berichten sollten (vgl. 17. Tb., Tz. 7.4, S. 41).

Aus datenschutzrechtlicher Sicht sehr zu begrüßen ist es, dass die Konferenz der Präsidentinnen und Präsidenten der deutschen Landesparlamente (in ihrer Sitzung vom 21. bis 23. Mai 2000 in Heringsdorf, Landtagsdrucksache 13/6466) folgenden Beschluss zu diesem Thema gefasst hat:

„Berichtspflicht der Landesregierungen zur akustischen Wohnraumüberwachung im Bereich der Strafverfolgung:

1. Die Konferenz der Präsidentinnen und Präsidenten der deutschen Landesparlamente ist der Auffassung, dass die Berichtspflicht der Landesregierungen zur akustischen Wohnraumüberwachung sowohl den präventiven Bereich polizeilicher Tätigkeit als auch den repressiven Bereich der Strafverfolgung umfasst. Artikel 13 Abs. 6 Satz 3 GG, wonach die Länder eine an den verfassungsrechtlichen Vorgaben für den Bund orientierte gleichwertige parlamentarische Kontrolle zu gewährleisten haben, ist als umfassender Regelungsauftrag an die Länder zu verstehen.
2. Die Präsidentenkonferenz empfiehlt, dass die Landesparlamente auf gesetzlicher Grundlage eine regelmäßige Berichtspflicht der Landesregierungen für präventiv-polizeiliche und repressive Maßnahmen der akustischen Wohnraumüberwachung vorsehen sollten. Sie hält eine Regelung in der parlamentarischen Geschäftsordnung nicht für ausreichend, weil diese keine Pflichten der Landesregierung begründen könnte.
3. Die Präsidentinnen und Präsidenten der deutschen Landesparlamente begrüßen es, dass auch die Datenschutzbeauftragten des Bundes und der Länder in einer Entschließung die Auffassung vertreten haben, die Kontrollkompetenz der Landtage erfasse sowohl den präventiven polizeilichen als auch den repressiven Bereich der Strafverfolgung.

Begründung:

Nach Artikel 13 Abs. 6 Satz 3 GG haben die Länder bei Maßnahmen der akustischen Wohnraumüberwachung eine dem Bund gleichwertige parlamentarische Kontrolle zu gewährleisten. Dabei geht es nicht allein um eine Beobachtung der Normeffizienz durch den Gesetzgeber, sondern um eine besondere Form parlamentarischer Kontrolle. Denn für die Einführung einer überkommenen parlamentarischen Kontrolle hätte es keiner gesonderten verfassungsrechtlichen Regelung bedurft. Vielmehr hat Artikel 13 Abs. 6 Satz 3 GG eine besondere (gesteigerte) Form der Kontrolle des Gesetzesvollzugs im Blick. Diese Kontrolle hat zwar nicht die Funktion, die Rechtmäßigkeit jeder einzelnen Vollzugsmaßnahme zu überprüfen. Denn insoweit sieht Artikel 13 GG – anders als Artikel 10 GG – im Regelfall eine richterliche Überprüfung vor. Gleichwohl beruht Artikel 13 Abs. 6 Satz 3 GG auf der Überlegung, dass die allgemeine parlamentarische Kontrolle, wie sie etwa durch parlamentarische Anfragen allgemein rückblickend oder auf einzelne Fälle bezogen möglich ist, nicht ausreichen würde. Artikel 13 Abs. 6 GG sieht daher – weiter gehend – eine anlassunabhängige und umfassende Kontrolle der Verwaltungspraxis anhand von regelmäßigen Berichten der Exekutive vor.

Diese Kontrolle kann aber effektiv nur gegenüber dem insoweit parlamentarisch verantwortlichen Minister ausgeübt werden. Die durch Artikel 13 Abs. 6 GG und § 100 e Abs. 1 StPO vorgesehene Unterrichtung des Bundestages kann, soweit die Länder für den Vollzug zuständig sind, keine effektive Kontrolle in diesem Sinne sein. Sie kann daher auch keinen Anlass geben, die Kontrolle auf Länderebene ausschließlich auf den präventiven Bereich zu beschränken."

Eine entsprechende gesetzliche Regelung in Rheinland-Pfalz steht derzeit noch aus.

Bislang liegen drei Berichte der Bundesregierung an den Bundestag über den Einsatz der „akustischen Wohnraumüberwachung" durch Strafverfolgungsbehörden insbesondere der Länder vor (vom 27. Dezember 1999, Bundestagsdrucksache 14/2452, vom 17. August 2000, Bundestagsdrucksache 14/3998 sowie vom 6. August 2001, Bundestagsdrucksache 14/6778). Aus den Berichten ergibt sich, dass in Rheinland-Pfalz in den Jahren 1998 und 1999 keine, im Jahr 2000 allerdings vier entsprechende Maßnahmen durchgeführt wurden. In zwei Fällen handelte es sich um Verfahren wegen Verstoßes gegen das Betäubungsmittelgesetz, in zwei Fällen wegen des Verdachts eines Tötungsdelikts. Betroffen war jeweils eine Wohnung, wobei in zwei Fällen nur Beschuldigte belauscht wurden, in einem Fall – jeweils neben einem Beschuldigten – neun Nichtbeschuldigte, in einem anderen Fall sieben Nichtbeschuldigte. Die Dauer der Maßnahmen variierte von vier Tagen bis zu 20 Tagen. In drei Fällen ergab sich nichts Verwertbares, in einem Fall allerdings war die Maßnahme erfolgreich.

Insgesamt ist erkennbar, dass die Strafverfolgungsbehörden von diesem neuen Instrument zurückhaltend Gebrauch machen. So waren im Jahr 1998 insgesamt bundesweit neun Verfahren betroffen, im Jahr 1999 waren es 26, im Jahr 2000 waren es 32 Verfahren.

Der LfD wird die Entwicklung weiter aufmerksam beobachten.

7.3 Telefonüberwachungen

Im Jahr 1998 wurden in Rheinland-Pfalz 118 Telefonüberwachungsmaßnahmen angeordnet; im Jahr 1999 waren es 157 und im Jahr 2000 194 strafrechtliche Ermittlungsverfahren (die Angaben beruhen auf Mitteilungen des Ministeriums der Justiz, zuletzt Pressemitteilung vom 15. März 2001). Gegenüber dem Vorjahr ist also im Jahr 2000 eine Steigerung um ca. 23 % festzustellen.

Die Zahl der Betroffenen stieg ebenfalls:
1998 waren es 195 Personen, 1999 254 und 2000 309, prozentual also eine Steigerung von 1999 auf 2000 von ca. 22 %.

Die Zunahme beruht erneut im Wesentlichen auf der gestiegenen Zahl von Telefonüberwachungen in Verfahren nach dem Betäubungsmittelgesetz. Auf diesen Bereich entfallen 144 Verfahren im Jahr 2000 (74,22 %), 116 Verfahren im Jahr 1999 (73,88 %) und 82 Fälle im Jahr 1998 (69,5 %). Die restlichen 51 Fälle verteilen sich im Wesentlichen auf die gewerbsmäßige Hehlerei/Bandenhehlerei sowie Waffendelikte (jeweils neun Fälle im Jahr 2000), auf Verfahren wegen Mord oder Totschlag (acht Fälle im Jahr 2000) sowie den Bandendiebstahl (sieben Fälle im Jahr 2000).

Die einzelnen Staatsanwaltschaften sind unterschiedlich betroffen: In Bad Kreuznach gab es 13, in Frankenthal 24, in Kaiserslautern 26, in Koblenz 37, in Landau 22, in Mainz 29, in Trier 24 und in Zweibrücken 19 Verfahren.

Es hat sich auch angesichts dieser Zahlen kein Anlass ergeben, an der Rechtmäßigkeit und Verhältnismäßigkeit der durchgeführten Maßnahmen zu zweifeln. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat allerdings angesichts des Befundes einer sich ständig ausweitenden Nutzung der elektronischen Kommunikation an die aus der Sicht des Datenschutzes bei Abhörmaßnahmen zu beachtenden Grundsätze erinnert (s. Anlage 14).

7.4 Zugriff von Polizei und Staatsanwälten auf Verbindungsdaten der Telekommunikation

Der LfD hat zu einem Gesetzentwurf der Bundesregierung Stellung genommen, mit dem die Nutzung von Verbindungsdaten aus der Telekommunikation für Strafverfolgungszwecke neu geregelt werden soll (Nachfolgeregelung für § 12 FAG). Der LfD hat begrüßt, dass beabsichtigt ist, diese Materie in der Strafprozessordnung (insbes. in einem neuen § 100 h) zu regeln. Zu begrüßen ist auch die erkennbare Tendenz des Entwurfs, grundrechtssichernde, dem Verhältnismäßigkeitsgrundsatz entsprechende Schranken zu statuieren.

Der LfD hat allerdings das Justizministerium gebeten, noch folgende Gesichtspunkte im Rahmen seiner Stellungnahme gegenüber dem Bundesgesetzgeber zu berücksichtigen:

§ 100 h Abs. 2 StPO in der Fassung des vorliegenden Entwurfs sieht vor, dass die durch die Auskunft erlangten personenbezogenen Informationen in anderen Strafverfahren zu Beweiszwecken verwendet werden dürfen, soweit der Beschuldigte zustimmt.

Eine solche Regelung hält der LfD für problematisch: Bei Verbindungsdaten sind regelmäßig der Beschuldigte und mindestens eine andere Person betroffen. Es wäre also eine unzulässige Verkürzung, hier nur auf die Einwilligung des Beschuldigten abzustellen. Möglicherweise liegen gerade bei anderen Betroffenen schutzwürdige Belange vor. Es kommt hinzu, dass es in der Strafprozessordnung systemfremd ist, die Frage ausdrücklich zu regeln, wann eine Einwilligung des Betroffenen als ausreichende Legitimation für die Durchführung strafprozessualer Eingriffe anzusehen ist. Aus einer solchen Regelungstechnik könnten in anderen Zusammenhängen Probleme entstehen; aus einem entsprechenden Schweigen des Gesetzgebers könnten Schlüsse gezogen werden, die nicht sachgerecht sind.

Schließlich hat der LfD auf einen Gesichtspunkt hingewiesen, den das Bundesverfassungsgericht im Zusammenhang mit Telekommunikationsüberwachungsmaßnahmen betont hat (in seiner Entscheidung zu den Befugnissen des BND im Rahmen der strategischen Überwachung des Fernmeldeverkehrs, NJW 2000, 55 ff., 64, 67): Es ist sachgerecht, aus Telefonüberwachungsmaßnahmen stammende Daten, die einem besonderen Verwendungszweck und besonderen Löschungsvorgaben unterliegen, im Strafverfahren gesondert zu kennzeichnen und Übermittlungen zu anderen Zwecken an andere Stellen besonders zu protokollieren. Dies sind verfahrenstechnische Vorkehrungen, um das hier in Rede stehende zu schützende Grundrecht auch in der Praxis zu gewährleisten.

In diesem Sinn hat sich auch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder ausgesprochen (s. Anlage 7).

7.5 Das Rückmeldeverfahren von der Justiz an die Polizei

In den zurückliegenden Tätigkeitsberichten wurde wiederholt darauf hingewiesen, dass es für die Polizei und ihre Entscheidung über Datenspeicherungen in ihren Informationssystemen durchaus von Bedeutung ist, über den Ausgang von Strafverfahren informiert zu werden.

Der LfD hat deshalb Anlass gesehen zu untersuchen, ob das gesetzlich (in Art. 32 Justizmitteilungsgesetz) vorgeschriebene Meldeverfahren tatsächlich in der Praxis umgesetzt wird. Zu diesem Zweck hat er bei einer großen Staatsanwaltschaft des Landes örtliche Feststellungen und eine repräsentative Stichprobe von Akten darauf hin durchgeführt, ob die jeweils gebotene Rückmeldung an

die Polizei verfügt war. In den Fällen, in denen dies zweifelhaft war bzw. in denen sich Zweifel aufdrängten, ob die entsprechende Verfügung vollzogen worden war, hat er ergänzend die kriminalpolizeilichen Akten eingesehen und das polizeiliche Informationssystem abgefragt.

Das Ergebnis war durchaus zufrieden stellend: Es gab eine – sehr geringe – Zahl von Fällen, in denen nicht aufklärbar war, ob eine Meldung erfolgt war. In keinem Fall aber war festzustellen, dass eine polizeiliche Datenspeicherung wegen einer möglicherweise unterbliebenen Meldung zu Unrecht aufrechterhalten worden ist. Dies entweder, weil gar keine polizeiliche Datenspeicherung vorhanden war oder weil nachfolgende Straftaten und diesbezügliche Meldungen zu einer Berichtigung bzw. Aktualisierung führten.

7.6 Täter-Opfer-Ausgleich und Datenschutz

Im 17. Tb. wurde das seinerzeit noch nicht abgeschlossene Gesetzgebungsverfahren zum Täter-Opfer-Ausgleich beschrieben (vgl. Tz. 7.6). Es wurde auf die aus datenschutzrechtlicher Sicht entscheidende Frage hingewiesen, ob auch ohne den Willen des Opfers seine Daten an privatrechtliche Aufsichtsstellen übermittelt werden dürfen.

Das Gesetz ist zwischenzeitlich in Kraft getreten (Gesetz zur strafverfahrensrechtlichen Verankerung des Täter-Opfer-Ausgleichs vom 20. Dezember 1999, BGBl. I S. 2491). Den datenschutzrechtlichen Anforderungen entspricht es, dass dort eine enge Zweckbindung und eine Vernichtungsregelung für die Daten der Ausgleichsstelle sowie eine anlassunabhängige Datenschutzkontrolle durch die jeweils zuständige Stelle vorgesehen ist. Bei privaten Stellen, um die es sich häufig handeln wird, ist dies in Rheinland-Pfalz die Aufsichts- und Dienstleistungsdirektion in Trier. Die Aktenzuleitung an die mit der Durchführung des Ausgleichs beauftragte Stelle wurde jedoch auch ohne Einwilligung des Verletzten zugelassen. Dies ist aus datenschutzrechtlicher Sicht zu bedauern. Prüferfahrungen in anderen Bundesländern (die Erfahrungen aus Niedersachsen sind hier bekannt geworden) haben zudem gezeigt, dass der Datenschutz bei diesen Stellen nicht immer in den besten Händen liegen dürfte.

7.7 DNA-Analyse in Strafverfahren

Im 17. Tb. (Tz. 7.5) wurde die Rechtslage ausführlich dargestellt, die für die Durchführung von DNA-Analysen in Strafverfahren maßgeblich ist.

Zwischenzeitlich handelt es sich bei solchen Analysemaßnahmen um Routinemaßnahmen der Strafverfolgungsbehörden, vergleichbar einer erkennungsdienstlichen Behandlung. Beim BKA werden derzeit ca. 300 Datensätze pro Arbeitstag in die Bundes-DNA-Datei eingespeichert (s. Bundestagsdrucksache 14/6025 vom 11. Mai 2001).

Auch in Rheinland-Pfalz sind solche Analysen keineswegs selten. Mit zunehmendem Zeitablauf seit In-Kraft-Treten der entsprechenden Rechtsgrundlagen (September 1998 bzw. Juni 1999) verliert die sog. „retrograde" Erfassung von verurteilten Straftätern in der DNA-Datei (gem. § 2 IFG) an Bedeutung. Zunehmend wichtiger und häufiger werden die Fälle, in denen DNA-Untersuchungen richterlich allein zur Aufklärung einer konkreten Straftat bzw. eines konkreten Tatverdachts gem. § 81 e StPO angeordnet worden sind und in denen anschließend entschieden werden muss, ob die entsprechenden Informationen (die DNA-Verformelung) in die DNA-Datei des Bundes eingestellt werden darf. Hier spricht man von einer „Umwidmung" der DNA-Informationen, die für ein laufendes Strafverfahren gewonnen worden sind, die dann aber für die vorbeugende Straftatenbekämpfung dauerhaft gespeichert werden sollen. Das Problem dieser Umwidmung wurde bereits im 17. Tb. (Tz. 7.5) angesprochen: Zwar bedarf es für die molekulargenetische Untersuchung auch in diesem Fall eines richterlichen Beschlusses. Über die Einstellung in die BKA-Datei entscheiden dann aber allein die Polizeibehörden. Das Ministerium der Justiz ist – ebenso wie der LfD – der Auffassung, dass hier eine gesetzliche Klarstellung erfolgen sollte, wonach auch diese Umwidmung und die daran anschließende Dateispeicherung von einem richterlichen Beschluss abhängig sein sollte.

Das Landgericht Hamburg hat sich mit der Frage auseinander gesetzt, ob diese gesetzliche Regelung verfassungskonform ist oder ob ergänzende, nicht ausdrücklich im Gesetz formulierte Schranken beachtet werden müssen (Beschluss vom 7. Juni 2001, Az.: 631 Qs 20/01, NJW 2001, S. 2563 f.). Es hat insbesondere Folgendes festgestellt:
Die Entscheidung durch einen Richter sei keineswegs das einzige Mittel, um Eingriffe in das Grundrecht auf informationelle Selbstbestimmung – seien sie auch schwer wiegender Art – zu legitimieren. Auch die Prüfung und Entscheidung durch eine Polizeibehörde könne vom Gesetzgeber zulässigerweise zur Voraussetzung eines solchen Eingriffs gemacht werden. Soweit die Gewährung rechtlichen Gehörs und die Informationspflicht über eine erfolgte Speicherung aus dem Grundrecht abgeleitet werde, so könnten diese Verfahrensrechte den Betroffenen auch in einem Verwaltungsverfahren gewährt werden. Die von einer Verwaltungsbehörde getroffene Entscheidung unterliege der gerichtlichen Kontrolle.

Insbesondere der Gedanke, dass dem Betroffenen rechtliches Gehör zu gewähren ist sowie eine Informationspflicht über die erfolgte Datenspeicherung bestehen muss, ist aus datenschutzrechtlicher Sicht zu unterstützen. In diesem Sinne hat der LfD das Ministerium der Justiz und das Ministerium des Innern und für Sport unterrichtet. Eine Reaktion steht noch aus.

Einem Schreiben des Ministeriums der Justiz an die Justizministerien der anderen Bundesländer war zu entnehmen, dass dieses die Auffassung vertrat, es würden in Rheinland-Pfalz in zu vielen Fällen, also eher leichtfertig und nicht entsprechend den gesetzlichen Vorgaben, die DNA-Testergebnisse aus laufenden Strafverfahren zur vorbeugenden Straftatenbekämpfung umgewidmet und in die DNA-Datei des Bundes überführt.

Die genannte Aussage des Ministeriums der Justiz bestärkte den LfD darin, diesbezüglich örtliche Feststellungen durchzuführen. Folgendes Ergebnis ist zu berichten:

Im Jahr 2000 wurden in 134 Fällen in Rheinland-Pfalz solche Umwidmungen aufgrund polizeilicher Entscheidungen durchgeführt. Der LfD überprüfte 44 Verfahren, die im Wege der Zufallsstichprobe ausgewählt worden sind und in denen die Analysedaten von 59 Personen umgewidmet worden sind. Folgende Probleme ergaben sich:

Häufig hatte die molekulargenetische Untersuchung und der Abgleich mit Spuren im konkreten Strafverfahren nicht zur Überführung des Verdächtigen geführt. Das Strafverfahren musste wegen mangelnden Tatverdachts eingestellt werden (gem. § 170 Abs. 2 StPO). Dennoch war die Polizeibehörde von der Täterschaft des Verdächtigen überzeugt. Dementsprechend entschied sie in diesen Fällen, den genetischen Fingerabdruck des Verdächtigen in die BKA-Datei einzuspeichern. Dies hat der LfD grundsätzlich für ausreichend gehalten. Eine Umwidmung war auch in diesen Fällen zulässig (gem. § 80 e Abs. 2 Satz 2 i. V. m. § 81 a Abs. 3 erster Halbsatz StPO). In drei Fällen allerdings war der LfD der Überzeugung, dass die Speichervoraussetzungen nicht vorgelegen hätten. Hierauf hat er das Ministerium des Innern und für Sport hingewiesen. Es ist zu erwarten, dass die entsprechenden Speicherungen gelöscht werden.

Ob die richterliche Tätigkeit in diesem Zusammenhang wirklich eine bessere Gewähr für eine datenschutzgerechte Verfahrensweise bieten würde, ist für den LfD allerdings zweifelhaft. Mit Beschluss vom 15. März 2001, Az.: 2 BvR 1841/00 u. a., hat die Dritte Kammer des 2. Senats des Bundesverfassungsgerichts entschieden, dass vier Verfassungsbeschwerden von betroffenen Straftätern stattgegeben wurde, die sich gegen eine Speicherung ihres genetischen Fingerabdrucks in der BKA-Datei gewehrt hatten. In diesen Fällen war die Entnahme von Körperzellen durch den Richter jeweils zum Zweck der Aufnahme der Daten in die BKA-Datei (gem. § 81 g StPO) angeordnet worden. Das Verfassungsgericht bemängelte bei allen vier richterlichen Beschlüssen, die jeweils durch das zuständige Landgericht in der Beschwerdeinstanz bestätigt worden waren, dass nicht gründlich genug geprüft, nicht angemessen gewertet und nicht ausreichend begründet worden ist. Einer dieser vier Fälle ereignete sich in Rheinland-Pfalz. Nach dieser Entscheidung des Bundesverfassungsgerichts dürften viele der entsprechenden richterlichen Beschlüsse den verfassungsgerichtlichen Vorgaben in diesem Zusammenhang bislang jedenfalls nicht entsprochen haben.

7.8 Internetveröffentlichungen justizieller Daten, insbesondere aus Insolvenzverfahren

Die Bestrebungen, das Internet zur kostengünstigen Bekanntmachung von unterschiedlichen Informationen auch aus dem Justizbereich zu nutzen, werden immer deutlicher. Dies betrifft nicht nur Schuldnerdaten im Insolvenzverfahren, sondern auch Veröffentlichungspflichten im Gesellschaftsrecht, öffentliche Bekanntmachungen von Gerichtsterminen u. Ä.

Die besondere Qualität der Internetveröffentlichungen, die gekennzeichnet wird durch

- weltweite Zugriffsmöglichkeiten,
- Unkontrollierbarkeit der Weiterverwendung durch das Erstellen von Kopien,
- Gefährdung der Integrität der veröffentlichten Daten bei unzureichenden technischen Sicherungsmaßnahmen,

rechtfertigt es, gesetzlich besondere Hürden zu errichten. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat hierzu einen Beschluss gefasst, der vom LfD unterstützt wird (Umlaufentschließung vom 24. April 2001, Anlage 27).

7.9 Einführung des elektronischen Grundbuchs

Künftig sollen alle Informationen, die bislang in Papierform in den Grundbüchern verzeichnet sind, elektronisch auf Datenträgern gespeichert werden. Die bisher verwendeten Papiergrundbücher werden schrittweise elektronisch erfasst und danach geschlossen. In Rheinland-Pfalz soll hierfür das Siemens-Verfahren SOLUM STAR eingeführt werden, das in Bayern bereits seit dem Juni 1994 verwendet wird. SOLUM-STAR löst das in den Jahren 1981 bis 1990 eingeführte „Mainzer Automationsunterstützte Grundbuchverfahren – MAGB –“ ab, das als Textverarbeitungssystem den Eintragungsvorgang vereinfachte, nicht aber zur dauerhaften Datenspeicherung vorgesehen war. Der bayerische Landesbeauftragte hat in seinem 16. Tätigkeitsbericht (S. 60) eine Darstellung und grundlegende Einschätzung dieses Verfahrens vorgelegt, wonach gegen die Konzeption des EDV-Grundbuchs SOLUM STAR keine grundsätzlichen datenschutzrechtlichen Bedenken bestehen. Die Erfahrungen im laufenden Betrieb blieben aber abzuwarten.

In Rheinland-Pfalz ist ein zentrales Grundbuchrechenzentrum beim DIZ aufgebaut worden, das für alle 47 rheinland-pfälzischen Grundbuchämter Daten speichern soll. Grundbuchinformationen stehen dann überall zur Verfügung. So sollen etwa berechtigte Behörden, Notare, Banken oder Sparkassen Grundbuchinformationen jedes rheinland-pfälzischen Amtsgerichts anfordern können.

Ab 1. November 2000 ist beim Amtsgericht Alzey das maschinelle Grundbuch als Pilotprojekt eingeführt worden. Bis zum Ende des Jahres 2004 soll diese Form der Grundbuchführung landesweit eingerichtet werden.

Zu diesem Zweck hat das Ministerium der Justiz eine Landesverordnung über das maschinell geführte Grundbuch erlassen. Den Entwurf hatte es mit folgender Anmerkung übersandt: „Wenngleich es sich um gerichtliche Tätigkeiten handelt, übersende ich Ihnen den anliegenden Entwurf der Landesverordnung zur informatorischen Kenntnisnahme.“

Der zitierte Passus des Zuleitungsschreibens lässt das grundlegende Missverständnis erkennen, dass der LfD auch im Bereich abstrakt genereller Regelungen mit datenschutzrechtlicher Bedeutung dann keine Zuständigkeit hätte, wenn diese Regelungen für den gerichtlichen Bereich gelten würden. Selbstverständlich hat der LfD im Zusammenhang mit solchen Regelungen aber auch dann Beratungsbefugnisse, wenn sie sich auf die gerichtliche Tätigkeit beziehen. Unabhängig davon bleibt festzuhalten, dass die Grundbuchführung – wie überhaupt die „freiwillige Gerichtsbarkeit", soweit es sich nicht um richterliche Entscheidungen handelt, d. h. soweit auch die Justizverwaltung Kompetenzen besitzt – und insbesondere auch die Art der Gestaltung des Grundbuches nicht als gerichtliche Tätigkeit, sondern als eine Verwaltungstätigkeit, die den Gerichten gesetzlich übertragen ist, anzusehen ist.

Der Zugang zu diesem automatisierten Abrufverfahren soll durch ein mehrstufiges System gesichert werden. Für die zugelassenen Teilnehmer soll ein geschlossener Benutzerkreis eingerichtet werden, so dass nur legitimierte Anschlüsse mit dem Grundbuchrechenzentrum verbunden werden können. Ferner sollen besondere Berechtigungen vergeben und vom Programm kontrolliert werden. Für die Bürgerinnen und Bürger sollen bei den Grundbuchämtern Auskunftsbildschirme zur Verfügung gestellt werden. Mit der Einrichtung des Abrufverfahrens soll im Jahr 2002 begonnen werden.

Der LfD hat beim Amtsgericht Alzey örtliche Feststellungen in diesem Zusammenhang getroffen. Angesichts des Systems der geschlossenen Benutzergruppe hat er in Übereinstimmung mit dem Ministerium der Justiz für entbehrlich gehalten, die Standards der qualifizierten elektronischen Signatur nach dem Signaturgesetz für Datenveränderungen im elektronischen Grundbuch vorauszusetzen. Die vorgesehene Protokollierung der Änderungen entspricht den datenschutzrechtlichen Anforderungen.

Soweit das Auskunftsverfahren an Dritte (Behörden, Notare, Banken, Sparkassen, Bürgerinnen und Bürger) betroffen ist, waren im Zeitpunkt der örtlichen Feststellungen noch keine konkreten Planungen vorhanden. Dieser Bereich wird Gegenstand besonderer Aufmerksamkeit im nächsten Berichtszeitraum werden.

7.10 Automatisierte Führung des Schuldnerverzeichnisses; unterlassene Unterrichtung der Bezieher von Abdrucken über eine Löschung

Ein Amtsgericht hatte einen Haftbefehl in einem Vollstreckungsverfahren zur Erzwingung der Abgabe der eidesstattlichen Versicherung gegen einen Schuldner erlassen. Dieser Haftbefehl wurde aufgrund eines gerichtlichen Beschlusses gelöscht. Dennoch hat mindestens eine private Kreditauskunftei eine entsprechende Negativauskunft über den betroffenen Petenten noch etwa sechs Monate nach der Löschung an die Fa. Neckermann erteilt.

Der betroffene Schuldner beschwerte sich darüber beim LfD. Dieser bat das Amtsgericht um Überprüfung, ob die entsprechende Löschung im Schuldnerverzeichnis ordnungsgemäß eingetragen war sowie ob die Bezieher der Schuldnerverzeichnis-Listen seinerzeit die Löschungsmitteilung erhalten hatten.

Es ergab sich, dass die Unterrichtung der Bezieher dieser Listen versehentlich unterblieben war. Der Grund ließe sich – so der Amtsgerichtsdirektor – nicht mehr feststellen. Die Unterrichtung wurde aufgrund der Anfrage des LfD nachgeholt.

Daraufhin wurde das automatisierte Verfahren zur Führung des Schuldnerverzeichnisses beim Amtsgericht in Augenschein genommen; es wurden verschiedene Vorschläge zu organisatorischen und technischen Verbesserungen des Verfahrens gemacht, zu deren Umsetzung Bereitschaft besteht.

7.11 Löschung von Haftdaten eines lange zurückliegenden Verfahrens aus der Gefangenenpersonalakte

Zwischen dem Justizministerium und dem LfD konnte in folgendem Fall leider keine Einigung über die datenschutzrechtlich zutreffende Beurteilung erzielt werden:

Zu entscheiden war, ob eine übereinstimmend als unzulässig beurteilte Eintragung einer lange zurückliegenden Vorstrafe in der Gefangenenpersonalakte zu vernichten ist oder ob es ausreicht, Informationen über die Vorstrafe in der Akte zu schwärzen, aber den gesamten Vorgang, insbesondere auch die Schriftstücke, die sich mit der Löschung dieser Information selbst befassen, in der Gefangenenpersonalakte zu belassen.

Aus Sicht des LfD ist Ausgangspunkt der hier anzustellenden Überlegungen die Regelung des § 51 Abs. 1 BZRG. Danach dürfen eine Straftat und die entsprechende Verurteilung dem Betroffenen im Rechtsverkehr nicht mehr vorgehalten und nicht zu seinem Nachteil verwertet werden, wenn die Eintragung über eine Verurteilung im Register getilgt worden ist.

Die Vorstrafe des Beschwerdeführers war im Bundeszentralregister getilgt. Sie hat ihren Eingang in die Gefangenenpersonalakte (den A-Bogen) gefunden, weil ein JVA-Bediensteter den Beschwerdeführer bei seiner erneuten Inhaftierung erkannte und ihn auf seine alte Haftzeit ansprach. Daraufhin habe der Beschwerdeführer erklärt – wohl auch, um den Sachverhalt klarzustellen und um nicht zu belastenden Spekulationen Anlass zu geben –, welche Dauer seine Vorstrafe hatte und wegen welcher Straftat sie verhängt worden war. Diese Angaben übernahm die Verwaltung der JVA in den sog. „A-Bogen".

Diese Information ist nach Auffassung des LfD unter Verstoß gegen § 51 Abs. 1 BZRG in die Gefangenenpersonalakte aufgenommen worden.

Nachdem der Beschwerdeführer den Eindruck erhalten hatte, dass bestimmte Resozialisierungsmaßnahmen bei ihm deshalb abgelehnt werden, weil die in Rede stehende Vorstrafe der JVA bekannt ist, bemühte er sich um die Entfernung dieser Information aus der Gefangenenpersonalakte. Nach Intervention des LfD erfolgte durch die JVA eine Schwärzung. Erkennbar blieb aber, dass ein Vorstrafeneintrag vorhanden war, der nunmehr geschwärzt worden ist. Auch der Schriftverkehr über diesen Vorgang dürfte sich noch in der Gefangenenpersonalakte befinden.

Damit wird weder dem Regelungsgehalt des § 51 Abs. 1 BRZG noch dem des § 184 Abs. 1 StVollzG ausreichend Rechnung getragen.

In der Kommentarliteratur wird einhellig die Auffassung vertreten (unter Bezugnahme auf die Rechtsprechung, insbesondere OVG Koblenz, ZfStrVo 89, 182; BVerfG NJW 83, 2135; BVerwG NVwZ 88, 621; BVerwG NJW 89, 1942; Hess. VGH RDV 93, 246), dass in vergleichbaren Fällen auch Aktenteile zu vernichten seien. Wenn es sich um besonders sensitive Daten handele, die nicht mehr benötigt werden oder die sich in einer rechtswidrig angelegten Akte befinden oder rechtswidrig in eine ordnungsgemäße Akte gelangt seien, habe der Grundsatz der Aktenvollständigkeit zurückzustehen (s. hierzu insbesondere Schmid in Schwind-Böhm, Kommentar zum Strafvollzugsgesetz, 3. Auflage 1999, Anmerkung 10 zu § 184).

Trotz mehrfacher Versuche des LfD, das Justizministerium zum Einlenken zu bewegen, beharrte dieses auf seiner abweichenden Auffassung. Eine förmliche Beanstandung des Verhaltens der JVA und der Aufsichtsbehörde in diesem Zusammenhang konnte deshalb nicht vermieden werden.

7.12 Eurojust

7.12.1 Pro Eurojust

Seit dem 1. März 2001 arbeitet in Brüssel eine neue Behörde, „Pro Eurojust", in der unter dem Vorsitz eines schwedischen Staatsanwaltes derzeit 16 Staatsanwälte aus allen Mitgliedstaaten der Europäischen Union tätig sind. Für Deutschland ist dies ein Bundesanwalt sowie ein Staatsanwalt des nordrhein-westfälischen Justizdienstes. Rechtsgrundlage für die Tätigkeit von Pro Eurojust ist der Ratsbeschluss vom 14. Dezember 2000, ABl. L 324, 21/12/2000, S. 2. Danach soll die „vorläufige Stelle zur justiziellen Zusammenarbeit", wie Pro Eurojust offiziell heißt, die Koordinierung von Ermittlungs- und Strafverfolgungsmaßnahmen im Bereich der schweren grenzüberschreitenden Kriminalität erleichtern und die Zusammenarbeit der Strafverfolgungsbehörden in diesem Bereich verbessern (Erwägungsgrund 1 des zitierten Ratsbeschlusses, Art. 2 a und b). Die Befugnisse der Mitarbeiter von Pro Eurojust werden in diesem Beschluss nicht angesprochen, sie bestimmen sich allein nach dem Recht des jeweiligen Entsendestaates. Dies bedeutet, dass jeder beteiligte Staatsanwalt in konkreten grenzüberschreitenden Ermittlungsverfahren seine nationalen Möglichkeiten zur Unterstützung nutzen soll und auch seit Anfang März 2001 in einer Vielzahl von Fällen bereits konkret genutzt hat: Zur Beschleunigung von Ermittlungsmaßnahmen und des Erlasses von für solche Maßnahmen erforderlichen Beschlüssen, zum Informationsaustausch über Verdächtige, Zeugen oder relevante Sachverhalte etc.

7.12.2 Eurojust

Pro Eurojust ist die Keimzelle einer künftigen großen europäischen Behörde namens Eurojust (Erwägungsgründe 4 und 5 des zitierten Ratsbeschlusses), deren Ziel es sein soll, die Bekämpfung der grenzüberschreitenden Kriminalität qualitativ entscheidend zu verbessern (Schlussfolgerungen der Tagung des Europäischen Rates vom 15. und 16. Oktober 1999 in Tampere, Nummer 46). Der Europäische Rat von Tampere hat vereinbart, dass vor Ablauf des Jahres 2001 eine Stelle eingerichtet werden soll, in der von den einzelnen Mitgliedstaaten nach Maßgabe ihrer Rechtsordnung entsandte Staatsanwälte, Richter oder Polizeibeamte mit gleichwertigen Befugnissen vertreten sind. Diese Stelle soll eine sachgerechte Koordinierung der nationalen Staatsanwaltschaften erleichtern und die strafrechtlichen Ermittlungen unterstützen. Dabei soll sie insbesondere auf die Europol-Analysen zurückgreifen können (Mitteilung der Kommission zur Einrichtung von Eurojust vom 22. November 2000, Com [2000] 746 endgültig).

Die Europäische Kommission unterstützt dieses Konzept.

Bislang gibt es zu folgenden Fragen über Aufgaben und Befugnisse von Eurojust einen Konsens: Eurojust soll

- Informationen über einzelstaatliche Rechtsvorschriften bereithalten und eine entsprechende Dokumentationsdatenbank aufbauen,
- Kontakte zwischen einzelstaatlichen Ermittlungsbehörden herstellen,
- Informationen über den Stand von Gerichtsverfahren oder über Urteile übermitteln,
- Erfahrungen austauschen und
- bis zu einem gewissen Grad Rechtsberatung leisten.

Zunächst wird Eurojust – wie Pro Eurojust derzeit bereits – ein zentraler runder Tisch für Verbindungsbeamte bzw. Verbindungsrichter und Staatsanwälte sein, die gemeinsam arbeiten und leichter miteinander kommunizieren können als dezentrale Kontaktstellen in den Mitgliedstaaten, wie dies gegenwärtig beim europäischen justiziellen Netz (EJN) der Fall ist. Eine zentrale Stelle bietet den Vorteil einer höheren Effizienz, erleichtert den Aufbau einer Sammlung relevanter Unterlagen und gewährleistet, dass jederzeit Sachverständige mit Fachkenntnissen im Bereich der justiziellen Zusammenarbeit verfügbar sind.

Darüber hinaus beabsichtigt die Kommission, Eurojust mit folgenden Kompetenzen auszustatten (vgl. die vorgenannte Mitteilung der Kommission zur Einrichtung von Eurojust):

- Direkte Beteiligung an konkreten strafrechtlichen Ermittlungen; aktive effiziente Koordination bei der Strafverfolgung in einzelnen Fällen; die Mitarbeiter von Eurojust sollen selbst aktiv an den Ermittlungen teilnehmen.
- Vermittlung zwischen den einzelstaatlichen Strafverfolgungsbehörden.
- Außerdem soll Eurojust die Kompetenz haben, gemeinsame Stellungnahmen und formelle Empfehlungen an einzelstaatliche Behörden im Bereich der Strafverfolgung zu richten. Gegenstand solcher Empfehlungen sollen insbesondere die Einsetzung gemeinsamer Ermittlungsgruppen, Fragen der gerichtlichen Zuständigkeit, der Informationsaustausch zwischen den einzelstaatlichen Behörden einschließlich der Gewährung von Akteneinsicht, der Inhalt von Rechtshilfeersuchen sowie die Beweisaufnahme oder der Zeugenschutz sein.
- Jede einzelstaatliche Behörde, die einer Eurojust-Empfehlung nicht nachkommt, soll gehalten werden, dieses Vorgehen innerhalb eines angemessenen Zeitraums zu begründen.
- Eurojust soll außerdem Strafanzeige erstatten können und Informationen an einzelstaatliche Strafverfolgungsbehörden im Hoheitsgebiet der Mitgliedstaaten weiterleiten. Wenn die Strafverfolgungsbehörden in solchen Fällen keine strafrechtlichen Ermittlungen einleiten, soll die Verpflichtung geschaffen werden, dass Eurojust eine begründete Antwort zu erhalten hat.
- Eurojust soll weiter die Kompetenz erhalten, verbindliche Auskunftsersuchen an einzelstaatliche Strafverfolgungsbehörden zu richten.
- Eurojust soll Zugang zu den nationalen Verfahrens- und Strafregistern haben.
- Auch ohne ausdrückliche Anfrage soll Eurojust über den Stand wichtiger grenzüberschreitender Verfahren informiert werden.
- Außerdem soll diese Stelle Einsicht in Akten von Strafsachen haben, die einen Bezug zu zwei oder mehr Mitgliedstaaten aufweisen.

7.12.3 Verhältnis von Eurojust zu EUROPOL

Eurojust soll EUROPOL durch Rechtsberatung unterstützen. Eurojust soll sich aber auf justizielle Aspekte beschränken. Eurojust soll im Rahmen geeigneter Datenschutz- und Geheimhaltungsvorschriften uneingeschränkt Zugang zu den Datenbanken von EUROPOL erhalten. Umgekehrt soll auch EUROPOL Daten von Eurojust erhalten können. Deutschland hat angeregt, dass Eurojust zusätzlich die Aufgabe erhalten solle, EUROPOL justiziell zu kontrollieren, allerdings unter dem vorsichtigen Stichwort der „justiziellen Begleitung" von EUROPOL (Bericht der Arbeitsgruppe Europa des Strafrechtsausschusses der Justizministerkonferenz vom 26. Oktober 2000). Abgesehen davon, dass diese zusätzliche Aufgabe nichts an der Relevanz und datenschutzrechtlichen Brisanz der Hauptaufgaben von Eurojust ändern würde: Diese deutschen Bestrebungen sind bislang von den anderen europäischen Partnern nicht aufgegriffen worden.

7.12.4 Datenschutzrechtliche Bewertungen

Damit wird das Bild einer zusätzlichen auf europäischer Ebene agierenden Strafverfolgungsbehörde deutlich.

Wichtig ist, dass die Mitarbeiter von Eurojust nach den Vorstellungen der Kommission auch die Befugnis erhalten sollen, nach dem nationalen Recht des Entsendestaates unmittelbare Eingriffe in die Rechte von Verdächtigen vornehmen zu lassen, dass sie insbesondere auch alle nationalen Datenbestände im Strafverfolgungsbereich abrufen können und eigene Datenbestände über Verdächtige aufbauen sollen. Gedacht ist beispielsweise auch daran, dass die Mitarbeiter von Eurojust die Sperrung von Bankguthaben veranlassen können sollen, dass sie zumindest entsprechende Anträge bei dem zuständigen nationalen Richter stellen können sollen. Zu diesem Zweck sollen ggf. die einzelstaatlichen Rechtsordnungen noch geändert werden.

Eurojust soll eine eigenständige Rechtspersönlichkeit zuerkannt erhalten, wie dies bereits bei EUROPOL der Fall ist.

Wie jedes Amt dieser Bedeutung auf der europäischen Ebene wird Eurojust eine effektive Infrastruktur erhalten: Für Dokumentation, EDV-Ausstattung und Übersetzung wird gesorgt werden; eine Managementstruktur, die die internen Regeln umsetzen soll und über Fragen der Verwaltung, über Ressourcen, Haushaltsmittel und Personalpolitik entscheidet, wird geschaffen werden. Ein entsprechendes Sekretariat wird also eingerichtet werden, das die Sitzungen und Beschlüsse des Lenkungsausschusses vorbereitet und das von einem geschäftsführenden Direktor geleitet werden soll. Zwei stellvertretende Direktoren sollen vorgesehen werden. Damit sind die Weichen gestellt für eine Behörde, deren Größenordnung sicher an EUROPOL heranreichen wird.

Diese wird sensibelste Daten über verdächtige Personen sammeln. Die Auskunftsansprüche von Bürgern haben also eine besondere Bedeutung. Entscheidungen von Eurojust selbst werden nicht justiziabel sein. Nur soweit nationale Stellen die Verantwortung für einzelne Maßnahmen übernehmen, werden diese Maßnahmen nach Maßgabe des nationalen Rechtes auch gerichtlich überprüfbar sein. Was Eurojust allerdings in seiner Position als eigenständige europäische Rechtspersönlichkeit tun wird, wird der unabhängigen richterlichen Überprüfung entzogen sein. Vor diesem Hintergrund fordern die Datenschutzbeauftragten insbesondere die Einrichtung einer effektiven Kontrollinstitution, die als Ersatz einer justiziellen Kontrolle angesehen werden kann.

Die Datenschutzbeauftragten des Bundes und der Länder erarbeiten derzeit eine gemeinsame Position mit konkreten datenschutzrechtlichen Anforderungen an die Rechtsakte, die Eurojust begründen werden. Bei aller Unterstützung von Institutionen, die das organisierte Verbrechen bekämpfen: Europa sollte schnellstens daran gehen, Institutionen wie EUROPOL und Eurojust in eine justizielle Struktur einzubinden, die es erlaubt, dass unabhängige Richter über Eingriffsmaßnahmen entscheiden. Nur dies würde dem Anspruch der Europäischen Union gerecht und könnte die Besorgnis der Bürger vor unkontrollierbaren Bürokratien mindern.

7.13 Bezeichnung strafrechtlicher Ermittlungsverfahren gegen mehrere Beschuldigte nach Verfahrenseinstellung gegen einen Namensgeber

Aufgrund einer Eingabe ist deutlich geworden, dass bei der Namensvergabe von Strafverfahren gegen mehrere Beschuldigte eine datenschutzrechtlich unbefriedigende Verfahrensgestaltung üblich war. In den Fällen, in denen gegen mehrere Beschuldigte ein Ermittlungsverfahren durchgeführt wurde und einige dieser Beschuldigten (üblicherweise wohl mindestens zwei) als Namensgeber des Verfahrens genutzt wurden und wenn gegen diese Namensgeber das Verfahren eingestellt wurde, das Verfahren gegen andere Beteiligte aber weiterlief, so war keine Änderung der Verfahrensbezeichnung in der Aktenordnung vorgeschrieben. Sie wurde dementsprechend in der Praxis also wohl auch nicht vorgenommen. Dies galt mindestens bis zum Abschluss des Ermittlungsverfahrens gegen alle Beschuldigten. Erst nach Erhebung einer Anklage wurden nur noch die Namen der Personen genannt, die in der Anklageschrift enthalten sind.

Für den Zeitraum, der zwischen der Einstellung des Verfahrens gegen einen Beschuldigten und dem Abschluss der Ermittlungen gegen alle Beschuldigten liegt, wurde also der Name derjenigen Personen, gegen die die Ermittlungen eingestellt wurden, weiter als Bestandteil der Verfahrensbezeichnung verwandt. Dies bedeutet, dass durchaus dritte Personen erstmals davon Kenntnis erhalten konnten, wer Beschuldigter gewesen ist, ohne dass dafür ein sachlicher, geschweige denn ein zwingender Grund vorgelegen hätte. Insbesondere bei Zeugenladungen konnte dies der Fall gewesen sein. Aber auch im sonstigen Schriftverkehr im Ermittlungsverfahren erhielten Dritte zwangsläufig (beispielsweise Sachverständige oder um Auskunft ersuchte öffentliche/private Stellen) diese Information.

Vor diesem Hintergrund hat der LfD gegenüber dem Ministerium der Justiz angeregt, in Fällen der beschriebenen Art nach Einstellung des Verfahrens den Namen der von der Einstellung betroffenen Personen aus der Verfahrensbezeichnung zu streichen, da die Datenübermittlung an Dritte über die Tatsache, dass gegen bestimmte Personen ein Ermittlungsverfahren geführt worden ist, einen durchaus erheblichen Eingriff in deren informationelles Selbstbestimmungsrecht darstellt. Wenn also entsprechende Fälle auch nur ausnahmsweise bedeutsam sein werden, so lohnt es sich aus der Sicht des LfD doch, im Interesse eines effektiven Grundrechtsschutzes hierfür eine adäquate Regelung zu schaffen.

Das Ministerium der Justiz hat den Generalstaatsanwälten die Entscheidung überlassen. Der Koblenzer Generalstaatsanwalt hat sich den obigen Argumenten gegenüber aufgeschlossen gezeigt und für seinen Geschäftsbereich eine entsprechende Anordnung getroffen. Die Entscheidung der Zweibrücker Generalstaatsanwältin steht noch aus.

8. Schulen, Hochschulen, Wissenschaft

8.1 Schulen

8.1.1 MARKUS tanzt WALZER im IGLU

MARKUS (Mathematik-Gesamterhebung Rheinland-Pfalz: Kompetenzen, Unterrichtsmerkmale, Schulkontext) war die erste landesweite externe Evaluation von schulischen Mathematikleistungen durch das Ministerium für Bildung, Wissenschaft und Weiterbildung. Dabei wurden im Jahr 2000 die achten Klassen an rheinland-pfälzischen Schulen auf ihre Leistungen im Fach Mathematik überprüft. Der LfD hielt die Befragung gem. § 54 a Abs. 1 SchulG für zulässig, wonach personenbezogene Daten von Schülern durch die Schulbehörde erhoben und verarbeitet werden dürfen, wenn dies zur Erfüllung schulbezogener Aufgaben erforderlich ist. Die gewünschten Angaben beschränkten sich auf das für die Qualitätsmessung erforderliche Maß, auch wenn manche Fragen die häusliche Situation der Kinder betrafen. Fragen aus diesem Bereich berührten aber nicht in solch einer Weise den Privatbereich der Schüler und Eltern, dass die Erforderlichkeit für die schulbezogene Aufgabenerfüllung in Zweifel zu ziehen gewesen wäre. Damit war eine Einwilligung der Eltern und Schüler entbehrlich.

WALZER (Wirkungsanalyse der Leistungsevaluation: Zielerreichung, Ertrag für die Bildungsqualität der Schule und die Rückmeldung von Evaluationsergebnissen) ist Bestandteil des auf sechs Jahre angelegten Schwerpunktprogramms „Bildungsqualität der Schule“ der Deutschen Forschungsgemeinschaft. Es richtet sich an die Mathematiklehrkräfte, die bereits im Rahmen von

MARKUS befragt worden sind. Dabei soll von der Universität Koblenz-Landau der Frage nachgegangen werden, wie dieses Projekt in den Schulen und bei den Lehrkräften aufgenommen wurde und welche Anstöße es für die Schulentwicklung geliefert hat. Die Beteiligung an dieser Untersuchung soll für die Lehrkräfte freiwillig sein. Der LfD hat Hinweise gegeben, was bei einer Aufklärung der Beteiligten zu beachten ist.

IGLU (Internationale Grundschul-Lese-Untersuchung) erfasste im Jahre 2001 mit einer im internationalen Vergleich für Deutschland repräsentativen Stichprobe die Lesekompetenz von Schülerinnen und Schülern der 4. Jahrgangsstufe. Die Ergebnisse wurden unter Einbeziehung der Sozialstruktur der Schülerschaft und unter Berücksichtigung des schulischen Umfeldes ausgewertet. Die Studie wurde international von der „International Association for the Evaluation of Educational Achievement" (IEA, Amsterdam) unter der Federführung des Boston College, USA, durchgeführt. Die Bundesrepublik beteiligte sich an dieser Studie aufgrund eines Beschlusses der Ständigen Konferenz der Kultusminister der Länder (KMK) und einer Vereinbarung zwischen der KMK und dem Bundesministerium für Bildung, Wissenschaft, Forschung und Technologie. Verantwortlich für die Durchführung der Studie war ein nationales Konsortium mehrerer Universitäten und Forschungseinrichtungen unter der wissenschaftlichen Federführung der Universität Hamburg. Durchgeführt wurde die Studie durch das Data Processing Center (DPC) in Hamburg. Wie bei der PISA-Studie (vgl. 17. Tb. Tz. 8.3.3) wurden auch hier Testleiter und Schulkoordinatoren eingesetzt. Das Verfahren war ähnlich. Weiterhin sollten Eltern, Schulleitung, Deutschlehrer und Fachbereichsleiter Deutsch Fragebögen ausfüllen. Da man sich an die gleiche Verfahrensweise wie bei PISA hielt, bestanden auch gegen diese Untersuchung keine datenschutzrechtlichen Bedenken.

8.1.2 Umfrage des Landeselternbeirats über Unterrichtsausfälle an Schulen

Ein vom Landeselternbeirat entwickelter Fragebogen, mit dem Unterrichtsausfälle an rheinland-pfälzischen Schulen erfasst werden sollten, war bei Lehrerinnen und Lehrern auf datenschutzrechtliche Bedenken gestoßen. Insbesondere die Gewerkschaft Erziehung und Wissenschaft Rheinland-Pfalz hielt die Erhebung teilweise aus Datenschutzgründen für unzulässig.

Der LfD sah in der Befragungsaktion keinen Verstoß gegen Datenschutzrecht. Der Fragebogen sollte in erster Linie dazu dienen, den Eltern einen Überblick über die Unterrichtssituation an der eigenen Schule zu verschaffen. Daher sollte im Erhebungsbogen zum einen eingetragen werden, wie viele Unterrichtsstunden an der Schule vorgesehen sind und wie viele tatsächlich stattgefunden haben. Dieser Soll-Ist-Vergleich betraf lediglich das strukturelle Lehrerstundendefizit. Er war in keiner Form personenbeziehbar. Zudem sollte über einen Zeitraum von vier Wochen festgehalten werden, wann und aus welchem Grund in einer Klasse eine Unterrichtsstunde ausgefallen ist. Insbesondere zu diesem Teil der Erhebung bestanden seitens der Betroffenen Bedenken. Es wurde befürchtet, dass aus diesen Informationen auf die Person des einzelnen Lehrers geschlossen werden konnte. Diese Bedenken teilte der LfD nicht. In der Regel sollten die Elternsprecher einer Klasse den Unterrichtsausfall festhalten. Diesen wurde aber ohnehin bekannt, bei welchem Lehrer der Unterricht ausgefallen war. Denn diese Information hätten sie bereits von ihren Kindern erhalten können. Die Eltern, die die Aufzeichnung vornahmen, gewannen hierdurch keine neuen personenbeziehbaren Erkenntnisse. Dem Landeselternbeirat wäre es nur mit der Beschaffung von Zusatzwissen möglich gewesen, einen Personenbezug zu einzelnen Lehrern herzustellen. Der Aufwand, sich dieses Zusatzwissen zu beschaffen, stand aber nach Ansicht des LfD außer Verhältnis zur Bedeutung und zur Sensitivität der zu gewinnenden Informationen.

Schließlich war zu berücksichtigen, dass der Landeselternbeirat eine entsprechende Befragung auch in personenbezogener Form hätte durchführen dürfen. Der Landeselternbeirat als Vertretungsorgan der Eltern ist Teil der Institution Schule. Als solche darf er Lehrerdaten erheben, soweit dies zu seiner Aufgabenerfüllung erforderlich ist.

8.1.3 Das schwarze Brett

Die Aufsichts- und Dienstleistungsdirektion teilte einem Lehrer an einer rheinland-pfälzischen Schule die Ermäßigung seiner Wochenstunden mit. Daraufhin wurde umgehend der Stundenplan geändert und am schwarzen Brett unmittelbar am Eingang zum Lehrerzimmer ausgehängt. Des Weiteren veröffentlichte der Personalrat ein von ihm verfasstes Schreiben an die Aufsichts- und Dienstleistungsdirektion ebenfalls am schwarzen Brett. Diesem Schreiben war zu entnehmen, dass der betreffende Lehrer einen Antrag auf Arbeitszeitermäßigung bei vollen Bezügen gestellt hatte, gleichzeitig aber eine nicht genehmigte Nebentätigkeit ausübe. Zum schwarzen Brett hatten außer dem Kollegium zumindest auch der Hausmeister Zugang. Der Brief des Personalrates war ausgehängt worden, da bei einer Personalversammlung, in der über diese Angelegenheit informiert wurde, nicht alle Kollegen anwesend waren.

Das Aushängen der Stundenplanänderung am schwarzen Brett stieß nicht auf datenschutzrechtliche Bedenken, da dies eine notwendige organisatorische Maßnahme war, die den Mitgliedern der Schule bekannt gegeben werden musste. Es handelte sich dabei um eine für die schulische Aufgabenerfüllung erforderliche Datenübermittlung.

Die Veröffentlichung des Briefes hielt der LfD dagegen für die schulische Aufgabenerfüllung im Sinne von § 54 a Abs. 1 SchulG nicht für erforderlich. Die Tatsache, dass ein Antrag auf Stundenermäßigung gestellt wurde, war zwar zum Zeitpunkt des Aushangs des Briefes ohnehin durch die Mitteilung über die Stundenplanänderung bekannt. Eine gleich lautende Information stellte daher keine Datenschutzverletzung dar. Es war jedoch davon auszugehen, dass die Mitteilung über die Nebentätigkeit des Lehrers eine Information war, die nicht für alle, die das schwarze Brett lesen konnten, erforderlich war. Vielmehr handelte es sich dabei um eine

Information, die lediglich im Verhältnis zwischen Personalrat und den von ihm Vertretenen eine Rolle spielte. Es war Aufgabe des Personalrates, die Interessen der Bediensteten zu vertreten. Wenn der Verdacht bestand, ein Kollege erhalte eine Stundenreduzierung zu Lasten der anderen, um eine Nebentätigkeit ausüben zu können, gehörte es zu den Obliegenheiten des Personalrates, die Betroffenen zu informieren und entsprechende Maßnahmen – wie eine Stellungnahme an die Schulaufsicht – zu ergreifen. Jedoch wäre es aus datenschutzrechtlicher Sicht nicht erforderlich gewesen, die Informationen so zu veröffentlichen, dass andere als die Lehrer des Kollegiums ebenfalls Zugang hatten. Aus der Verpflichtung des Hausmeisters der Schule zur Wahrung des Datengeheimnisses folgte nicht, dass er automatisch zu allen in der Schule verfügbaren personenbezogenen Daten Zugang hatte. Durch die Verpflichtung zur Wahrung des Datengeheimnisses kommt lediglich zum Ausdruck, dass er die ihm rechtmäßig zur Kenntnis gelangten Informationen vertraulich behandeln muss. Eine unmittelbare Mitteilung nur an die Betroffenen – nämlich die Kollegen und allenfalls die Elternvertreter – hätte ausgereicht. Das Aushängen des kompletten Briefes war daher aus datenschutzrechtlicher Sicht nicht zulässig.

8.1.4 Schulen im Internet

Sehr viele Schulen in Rheinland-Pfalz sind bereits mit einer eigenen Homepage im Internet vertreten oder im Begriff, eine entsprechende Präsentation vorzubereiten. Das führte häufig zu Anfragen der an der Schule Verantwortlichen oder auch besorgter Eltern, welche personenbezogenen Daten im Internet veröffentlicht werden dürfen. Hierzu ist auf die Ausführungen im 17. Tb., Tz. 8.1.7 zu verweisen. Es hat sich gezeigt, dass in der Regel ein datenschutzbewusster Umgang mit dem neuen Medium Internet erfolgt.

8.2 Hochschulen

8.2.1 Anmeldeverfahren für Lehrveranstaltungen

Studenten hatten im Institut für Informatik an einer rheinland-pfälzischen Hochschule die Möglichkeit, sich zu Beginn des Semesters für Lehrveranstaltungen an PCs im Institut anzumelden. Das zugrunde liegende EDV-System war während dieser Zeit öffentlich zugänglich, im Übrigen konnte es nur von besonders berechtigten Personen gestartet werden. Diese Form der Anmeldung war freiwillig, die Studenten konnten sich auch im Sekretariat anmelden. Fraglich war allerdings, inwieweit die dort vorgenommenen Anmeldungen auch auf den öffentlich zugänglichen Rechnern vorhanden waren. Es war davon auszugehen, dass die Anmeldedaten im Sekretariat ebenfalls in das System, an das auch die vorübergehend öffentlich zugänglichen Rechner angeschlossen waren, eingegeben wurden. Folglich machte es keinen Unterschied, ob der Betroffene die Daten selbst eingab oder das im Sekretariat zu der Zeit erledigt wurde, zu der das System für alle öffentlich zugänglich war. Um von einer echten Wahlmöglichkeit bei der Anmeldeform auszugehen, musste sichergestellt werden, dass bei einer Anmeldung über das Sekretariat auf diese Daten nicht über die beiden kurzzeitig öffentlich zugänglichen Rechner zugegriffen werden konnte.

Weiterhin war es beim Anmeldeverfahren ausreichend, die Matrikelnummer bei der Anmeldung in den PC einzugeben. Sodann wurden die dazugehörigen persönlichen Daten wie Name und Anschrift aus dem Datenbestand der Zentralen Studentenverwaltung automatisch ergänzt, wenn zuvor noch keine Anmeldung erfolgte. Wenn diese persönlichen Daten dem Betroffenen angezeigt wurden, weil er sie bestätigen oder ändern sollte, hätte auch ein Dritter durch Eingabe einer Matrikelnummer im Rahmen einer fingierten Anmeldung Kenntnis von persönlichen Daten eines anderen erlangen können. Die Matrikelnummer hätte z. B. einem Aushang am schwarzen Brett entnommen werden können, wenn dort Informationen unter Angabe der Matrikelnummer veröffentlicht worden wären. Der LfD hat daher empfohlen, zusätzlich zur Matrikelnummer stets ein weiteres persönliches Datum wie den Nachnamen eingeben zu lassen. Dadurch würde die Gefahr, dass Dritte sich lediglich unter Angabe einer Matrikelnummer weitere Informationen verschaffen können, wesentlich verringert.

Die Hochschule hat daraufhin das Anmeldeverfahren entsprechend den Empfehlungen geändert.

8.2.2 Datenschutzbeauftragter an der Hochschule

Bei einer rheinland-pfälzischen Hochschule gab es über den Zeitraum von einem halben Jahr keinen behördlichen Datenschutzbeauftragten, da der Amtsinhaber ausgeschieden war und die Position nicht neu besetzt wurde. Der LfD hat die Hochschule darauf hingewiesen, dass gem. § 11 LDSG öffentliche Stellen mit mindestens zehn Beschäftigten, die personenbezogene Daten verarbeiten, einen behördlichen Datenschutzbeauftragten zu bestellen haben. Scheidet der Amtsinhaber aus, ist die Stelle unverzüglich wieder zu besetzen. Die Vakanz der Stelle seit einem halben Jahr war nicht mit der gesetzlichen Regelung vereinbar. Daraufhin hat die Hochschule unverzüglich einen neuen Datenschutzbeauftragten bestellt und damit die rechtswidrige Situation behoben.

8.2.3 Forschungsdatenbank des Landes Rheinland-Pfalz

Das Ministerium für Bildung, Wissenschaft und Weiterbildung unterhält im Internet die Seiten „Forschungsbericht des Landes Rheinland-Pfalz“ und „Who's Who der Hochschulen des Landes Rheinland-Pfalz“. Im Forschungsbericht sind die Rubriken Institution, Wissenschaftler, Forschungsgebiet und Forschungsprojekt vorgesehen. Dies entspricht den Informationen im Forschungsbericht, den die Hochschulen nach dem Universitätsgesetz vorlegen müssen. Im „Who's Who“ werden die Rubriken Wissenschaftler, Fachgebiet, Forschungsgebiet, Lehrgebiet, (wissenschaftlicher) Werdegang, sonstige Kommunikationsadressen, Anschrift

und Besucheradresse, Publikationen sowie Forschungsprojekte dargestellt. Die Veröffentlichung von Informationen über den beruflichen Werdegang ist nicht mehr von der Verpflichtung zur Veröffentlichung eines Forschungsberichts gem. § 11 Abs. 2 UG gedeckt. Es handelt sich dabei vielmehr um Personaldaten, die nur unter bestimmten Voraussetzungen an Dritte übermittelt, aber nicht automatisch der Öffentlichkeit zur Verfügung gestellt werden dürfen. Zur Veröffentlichung der Informationen des Werdegangs im Internet bedarf es somit der Einwilligung der Betroffenen. Im Internet-Formular ist daher ein entsprechender Hinweis anzubringen, der insbesondere auch über die Freiwilligkeit der Datenpreisgabe informiert (vgl. § 5 Abs. 3 LDSG). Das Ministerium hat zugesagt, dies bei der nächsten Überarbeitung zu beachten.

8.2.4 Datenschutz in der Landesverfassung und Personaldatenverarbeitung in der Hochschule

Am 18. Mai 2000 ist Art. 4 a LV in Kraft getreten. Dieser besagt u. a., dass jeder Mensch das Recht hat, über die Erhebung und weitere Verarbeitung seiner personenbezogenen Daten selbst zu bestimmen, sofern diese Rechte nicht durch Gesetz oder aufgrund eines Gesetzes eingeschränkt werden. In diesem Zusammenhang warf eine rheinland-pfälzische Hochschule die Frage auf, ob diese Vorschrift die bisher geltende Rechtslage in Bezug auf die Personaldatenverarbeitung ändere.

Der LfD hat hierzu die Auffassung vertreten, dass die Einführung des Art. 4 a LV die bestehende Rechtslage nicht verändert. Das Recht auf informationelle Selbstbestimmung ist ein Grundrecht, das seinen Ausdruck im allgemeinen Persönlichkeitsrecht des Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG findet. Dieses wiederum ist umgesetzt im Landesdatenschutzgesetz sowie in Vorschriften allgemeiner Gesetze. Art. 4 a LV bestätigt dieses Grundrecht jetzt ausdrücklich auch in der Landesverfassung.

Das Recht auf informationelle Selbstbestimmung ist jedoch bei öffentlich Bediensteten eingeschränkt. Eine solche Einschränkung ist gem. Art. 4 a Abs. 2 LV zulässig. Die Erhebung und Speicherung von Personaldaten ist für Angestellte gem. § 31 Abs. 1 LDSG zulässig, soweit dies zur Abwicklung des Dienstverhältnisses oder zur Durchführung bestimmter Maßnahmen erforderlich ist. Dies trifft insbesondere auf die Verarbeitung von Urlaubs- oder Krankheitsdaten zu. Diese Daten sind jedoch zu löschen, sobald sie im Sinne der o. g. Vorschrift nicht mehr erforderlich sind. Auch das Einstellen der Bedienstetennamen und deren Erreichbarkeit ins Intranet oder Vorlesungsverzeichnis hält sich im Rahmen einer notwendigen organisatorischen Maßnahme, da sich diese Medien nur an eine beschränkte Öffentlichkeit wenden. Für Beamte gilt gem. § 102 g Abs. 1 LBG das Gleiche.

Auch dürfen im Rahmen der sog. Amtsträgertheorie Name, Funktion sowie dienstliche Erreichbarkeit von Bediensteten, die die Institution nach außen vertreten, veröffentlicht werden. Als Medium kann dabei auch das Internet dienen. Dies wurde im 16. Tb. (Tz. 17.3) für Personaldaten im Allgemeinen und im 17. Tb. (Tz. 8.1.7) für Daten von Schulangehörigen ausführlich dargelegt.

Durch die Einfügung des Art. 4 a LV wurden die Rechte der Bediensteten demnach nicht erweitert, sondern bleiben im bisherigen Rahmen bestehen.

8.2.5 Übermittlung von Personalakten durch die Fachhochschule an das Ministerium

Die an den LfD herangetragene Frage, ob das Ministerium für Bildung, Wissenschaft und Weiterbildung Personalakten über Professoren von Fachhochschulen nur schriftlich unter Angabe von Gründen anfordern durfte, wurde wie folgt beantwortet:

Nach § 102 d Abs. 1 LBG dürfen Personalakten ohne Einwilligung des Beamten für Zwecke der Personalverwaltung oder Personalwirtschaft der obersten Dienstbehörde oder der im Rahmen der Dienstaufsicht weisungsbefugten Behörde vorgelegt werden. Das Vorlageersuchen wäre nach dieser Vorschrift schriftlich zu begründen und die Erforderlichkeit von den Fachhochschulen zu prüfen.

Jedoch ist Dienstvorgesetzter der Professoren gem. § 37 Abs. 1 FHG das fachlich zuständige Ministerium und muss damit über alle personalrechtlichen Angelegenheiten informiert sein. Die Personalverwaltung wird von den Fachhochschulen gem. § 7 Abs. 1 Nr. 1 FHG lediglich im Auftrag durchgeführt. Herr der Daten bleibt aber nach wie vor das Ministerium für Bildung, Wissenschaft und Weiterbildung als Dienstvorgesetzter. Ein entsprechendes Ersuchen durch dieses erfolgt damit nicht gem. § 102 d LBG zur Vorlage an die oberste Dienstbehörde oder der im Rahmen der Dienstaufsicht weisungsbefugten Behörde, sondern an den unmittelbaren Dienstvorgesetzten.

Der LfD ging daher davon aus, dass § 102 d LBG keine Anwendung findet und daher eine schriftliche Anfrage unter Darlegung von Gründen nicht erforderlich war.

8.2.6 Big Brother an der Hochschule? – Datenschutzrechtliche Aspekte von Webcams

Einige Hochschulen des Landes haben sich an den LfD mit der Frage gewandt, ob die Installation von Videokameras oder Webcams auf dem Hochschulgelände aus datenschutzrechtlicher Sicht zulässig ist. Dazu hat der LfD unter Hinweis auf die Entschließung der 59. Konferenz der Datenschutzbeauftragten des Bundes und der Länder „Risiken und Grenzen der Videoüberwachung“ (vgl. Anlage 13) Folgendes ausgeführt:

Die Installation von Webcams oder Videokameras zur Überwachung von Plätzen und Räumen einer Hochschule stellt einen Eingriff in das informationelle Selbstbestimmungsrecht der Studierenden, der Bediensteten und der sonstigen Nutzer der Einrichtungen der Hochschule dar. Ein solcher Eingriff ist nur dann gerechtfertigt, wenn er dazu dient, die Betroffenen vor Straftaten zu schützen und verhältnismäßig ist.

Soweit durch die Videoaufzeichnungen erreicht werden soll, Störungen auf dem Hochschulgelände bzw. Beschädigungen an Hochschuleigentum zu vermeiden bzw. einzuschränken (Maßnahmen zur Gebäudesicherung), kann die Hochschule aufgrund ihres Hausrechts zu entsprechenden Maßnahmen befugt sein. Diese müssen sich allerdings im Rahmen der verfassungsmäßigen Ordnung, insbesondere auch der Verhältnismäßigkeit, halten, wenn dadurch Rechte von Bürgern beeinträchtigt werden können. Dies ist vorliegend der Fall: Durch die Videoaufzeichnungen können auch Unbeteiligte auf dem Hochschulgelände erfasst und in ihrem Verhalten registriert werden. Die Videoaufzeichnungen halten sich nur dann im Rahmen der Verhältnismäßigkeit, wenn sie geeignet, angemessen und erforderlich sind, das angestrebte Ziel zu erreichen.

Die Fertigung von Videoaufzeichnungen ist grundsätzlich geeignet, künftige Störungen, wie Sachbeschädigungen und Diebstähle, zu verhindern: Falls der oder die Täter mit Hilfe der Aufzeichnungen identifiziert werden können, kann ihnen ein Hausverbot erteilt werden. Außerdem können Schadensersatzansprüche geltend gemacht und strafrechtliche Sanktionen eingeleitet werden. Zudem hat die erkennbare Existenz von Videokameras einen entsprechenden Abschreckungseffekt.

Die Maßnahme muss auch angemessen sein. Der Eingriff in die Rechte Dritter (Aufzeichnen des Verhaltens Unbeteiligter) ist gegen den voraussichtlichen Erfolg der Maßnahmen (Gebäudesicherung) abzuwägen. Wenn die Aufzeichnungen nur kurze Zeit gespeichert und nach Auswertung durch einen beschränkten Personenkreis gelöscht werden, soweit sie nicht zur Beweissicherung bei besonderen Vorkommnissen benötigt werden, hält der LfD die Maßnahmen insoweit für verhältnismäßig und damit für angemessen. Es ist jedoch erforderlich, dass die Aufzeichnung für die Betroffenen erkennbar ist.

Fraglich ist schließlich, ob die Maßnahmen zur Gebäudesicherung erforderlich sind. Dies ist nur dann der Fall, wenn es in der Vergangenheit schon an den geplanten oder vergleichbaren Standpunkten der Webcams oder Videokameras zu Vorfällen gekommen ist.

Teilweise sollte das Aufstellen von Webcams der Einbindung der Aufzeichnungen in die Homepage der Hochschule dienen, um Studierende zu werben. Dadurch könnte § 22 KunsturhG verletzt werden, wenn Personen auf den Aufzeichnungen zu erkennen sind. Danach dürfen Bildnisse nur mit Einwilligung des Abgebildeten verbreitet oder öffentlich zur Schau gestellt werden. Die Kameras könnten so installiert werden, dass einzelne Personen nicht mehr erkennbar sind. Andernfalls wäre die Einwilligung der Betroffenen einzuholen. Dies könnte dadurch erfolgen, dass nur ein bestimmter Teil der Räumlichkeiten von den Webcams aufgezeichnet und die Betroffenen darauf entsprechend hingewiesen werden. Wer keine Aufzeichnung zur Veröffentlichung im Internet wünscht, kann diesen Teil der Räumlichkeiten meiden. Für Maßnahmen der Gebäudesicherung wären dann evtl. gesonderte Webcams oder Videokameras aufzustellen und die o. g. Ausführungen zu beachten.

8.2.7 Chipkarte als Studierendenausweis

Nach der Universität Trier plant nun auch die Universität Koblenz-Landau die Einführung einer Chipkarte als Studierendenausweis. Dieser soll erstmals für die Rückmeldung zum Sommersemester 2002 eingesetzt werden. Mit der Karte sollen folgende Anwendungen durchgeführt werden:

- Rückmeldung ohne Änderung von Studiengängen und Studienfächern
- Ausdruck der Studienbescheinigungen
- Nachweis für das Semesterticket bei den Verkehrsbetrieben (optischer Nachweis)
- Nutzung für die Kopiersysteme
- Bibliotheksausweis (Auslesen der Matrikelnummer aus dem Chip).

Eine Geldkartenfunktion soll der Studierendenausweis nicht enthalten.

Es ist beabsichtigt, in der Einschreibeordnung eine entsprechende Rechtsgrundlage für die Einführung der Chipkarte zu schaffen. Die Universität hat das überarbeitete Sicherheitskonzept vorgelegt. Dessen Umsetzung wird der LfD durch entsprechende örtliche Feststellungen überprüfen, sobald ein Testlauf möglich ist. Dies wird voraussichtlich im Winter 2001 sein.

8.2.8 Verwertung von Internet-Verbindungsdaten zum Zweck der Strafverfolgung

Der LfD hatte sich mit folgendem Fall zu beschäftigen:

Auf einer Homepage wurden u. a. kinderpornographische Bilddateien für die private Nutzung angeboten. Die Strafverfolgungsbehörden ermittelten, dass Internet-Teilnehmer einer Hochschule auf diese Bilddateien zugegriffen hätten. Man bat nunmehr um Angabe der vollständigen Bestandsdaten der Kunden der Hochschule, da der Verdacht einer Straftat bestünde.

Beim Auskunftsersuchen der Strafverfolgungsbehörden war zwischen der Übermittlung von Bestandsdaten und der Übermittlung von Verbindungsdaten zu unterscheiden. Bestandsdaten sind gem. § 89 Abs. 2 Nr. 1 lit. a TKG die Angaben, die zur betrieblichen Abwicklung von geschäftsmäßigen Telekommunikationsdiensten durch Unternehmen oder Personen für das Begründen, inhaltliche Ausgestalten und Ändern eines Vertragsverhältnisses erforderlich sind. Das Angebot einer Universität an ihre Studenten und das wissenschaftliche Personal, das Internet nutzen zu dürfen, ist als geschäftsmäßig anzusehen, weil es auf eine wiederkehrende Leistung gerichtet ist. Als nicht geschäftsmäßig anzusehen wäre dagegen die Internet-Nutzung dann, wenn sie Bediensteten zu dienstlichen Zwecken zur Verfügung gestellt wird, da hier die Nutzung durch die Universität selbst (in Person ihrer Mitarbeiter) erfolgt. Da sich der fragliche Rechner, über den auf die kinderpornographischen Dateien zugegriffen wurde, offensichtlich nicht im Verwaltungsgebrauch befand, sondern von einem Fachbereich eingesetzt wurde, war hier von einer Nutzung zu Lehr- und Forschungszwecken auszugehen. Diese war aber nicht als Nutzung zu dienstlichen Zwecken zu werten, da die Ergebnisse nicht der Verwaltungsarbeit der Universität dienten.

Bestandsdaten sind insbesondere Name und Anschrift des Kunden, die Art des kontrahierten Dienstes und die dem Kunden zum Gebrauch überlassenen Einrichtungen. Diese Daten sind gem. § 89 Abs. 6 TKG im Einzelfall auf Ersuchen an die zuständigen Stellen zu übermitteln, soweit dies für die Verfolgung von Straftaten erforderlich ist. Im vorliegenden Fall hatte die Hochschule daher die Bestandsdaten der Kunden der Universität zu übermitteln, da der Verdacht einer Straftat bestand.

Etwas anderes gilt für die Verbindungsdaten der konkreten fraglichen Nutzung. Hierbei handelt es sich um die Rufnummer des Anrufers und die Zielrufnummer, Datum, Uhrzeit und Dauer der Verbindung sowie die Art der vom Kunden in Anspruch genommenen Telekommunikationsleistung ebenso wie deren Inhalt. Diese unterliegen gem. 85 Abs. 1 TKG dem Telekommunikationsgeheimnis, wenn sie – wie hier – im Rahmen eines geschäftsmäßigen Angebots von Internet-Dienstleistungen entstanden sind. Die Internet-Nutzungsdaten sind als dem Telekommunikationsgeheimnis unterliegende Verbindungsdaten daher grundsätzlich nur auf Grundlage eines richterlichen Beschlusses im Rahmen des § 12 FAG herauszugeben. Dann dürften bzw. müssten (siehe § 161 StPO) aber sämtliche erbetenen Daten übermittelt werden. Bei dem geschilderten Sachverhalt war jedoch davon auszugehen, dass die Universitätsverwaltung die konkreten Verbindungsdaten weder kannte noch ermitteln konnte, so dass eine Übermittlung nur durch den betreffenden Fachbereich hätte vorgenommen werden können. Auch dieses durfte die Daten nur aufgrund eines richterlichen Beschlusses herausgeben.

8.3 Wissenschaft

8.3.1 Online-Befragung über Internet-Nutzung in Schulen

Die Universität Mainz plante eine Online-Befragung über die Internet-Nutzung in der Sekundarstufe I in Mainzer Schulen. Dazu war die informierte Einwilligung der Betroffenen einzuholen. Da die Befragung via Internet erfolgen sollte, konnte aus datenschutzrechtlicher Sicht auch die Information der Betroffenen über dieses Medium vorgenommen werden. Zusätzlich war in diesem Fall auf die Gefahren einer unverschlüsselten Rücksendung des Fragebogens über das Internet und darauf aufmerksam zu machen, dass hierdurch eine klare Zuordnung des Fragebogens zur absendenden Stelle möglich ist. Die Forscher wurden durch den LfD auf diese Anforderungen hingewiesen.

8.3.2 Gentechnik

Die Diskussion um die Gentechnik beschäftigte im Berichtszeitraum auch den LfD. Das Fortschreiten der Entschlüsselung des menschlichen Genoms hat erheblichen datenschutzrechtlichen Bezug. Das hat die 60. Konferenz der Datenschutzbeauftragten dazu veranlasst, eine Entschließung zu den „Datenschutzrechtlichen Konsequenzen aus der Entschlüsselung des menschlichen Genoms“ (vgl. Anlage 15) zu verabschieden. Dort werden die datenschutzrechtlichen Anforderungen an den Umgang mit genetischen Daten formuliert. Die Datenschutzbeauftragten sind sich einig, dass es zum Umgang mit diesen hoch sensiblen Daten einer gesetzlichen Grundlage bedarf, die die näheren Voraussetzungen regelt. Die Datenschutzbeauftragten haben eine Ad-hoc-Arbeitsgruppe gebildet, die zurzeit konkrete Anforderungen an eine mögliche Regelung formuliert.

8.4 Verarbeitung personenbezogener Daten von Bibliotheksbenutzern

Ein Bibliotheksbenutzer trug vor, in einer städtischen Bibliothek sei ein Vermerk über ihn gespeichert, der ihn als Verschmutzer von entliehenen Büchern bezeichne. Er begehrte die Löschung oder Sperrung dieses Vermerks, da dieser nicht zutreffend sei.

Auf Nachfrage bei der Bibliothek stellte sich heraus, dass es dort üblich war, bei Benutzern mit entsprechenden Vorkommnissen interne Bearbeitungsvermerke einzutragen, um auf Besonderheiten angemessen reagieren zu können. Der Vermerk im vorliegenden Fall lautete „Bücher gut kontrollieren“, was sich sowohl auf eine Kontrolle unmittelbar vor der Buchausgabe als auch direkt nach der Buchrückgabe beziehen sollte. Da es beim Petenten schon mehrmals Anlass zu Beanstandungen gegeben habe, hielt die Bibliothek einen solchen Vermerk für wichtig zur Sicherung der Beweislage im beiderseitigen Interesse. Die Speicherung erfolgte aufgrund der Benutzungsordnung für die Bibliothek.

Der Vermerk „Bücher gut kontrollieren“ wurde als Hinweis bei einem bestimmten Bibliotheksbenutzer zu dessen Datensatz gespeichert und war damit ein personenbezogenes Datum gem. § 3 Abs. 1 LDSG. Durch diesen Vermerk wurde nicht festgestellt, dass der Benutzer Bücher verschmutzte. Vielmehr sollte ein bestehender Verdacht, dass dies so sein könnte, überprüft werden. Dieser Verdacht konnte durch die besondere Prüfung entweder bestätigt oder entkräftet werden.

Der LfD hielt die Speicherung dieses Datums gem. § 13 Abs. 1 LDSG in Verbindung mit der Benutzungsordnung der Bibliothek für zulässig. Nach § 13 Abs. 1 LDSG ist das Speichern personenbezogener Daten zulässig, wenn dies zur rechtmäßigen Erfüllung der in der Zuständigkeit der Daten verarbeitenden Stelle liegenden Aufgaben erforderlich ist und für Zwecke erfolgt, für die die Daten erhoben worden sind. Nach der Benutzungsordnung hatten sich die Benutzer bei der Übergabe vom Zustand der Medien zu überzeugen und etwaige Mängel sofort zu melden. Wurde eine Verschmutzung oder Beschädigung während der Ausleihfrist festgestellt, waren diese bei Rückgabe unaufgefordert anzuzeigen. Um in besonderen unklaren Fällen die Einhaltung dieser Pflichten nachprüfen und auch entsprechende weitere Maßnahmen durchführen zu können, war ein Hinweis auf einen besonderen Kontrollbedarf bei Ausleihe und Rückgabe erforderlich.

Eine Sperrung der Daten gem. § 19 Abs. 3 Nr. 1 LDSG kam nicht in Betracht. Dies hätte vorausgesetzt, dass die Richtigkeit personenbezogener Daten vom Betroffenen bestritten wurde und sich weder die Richtigkeit noch die Unrichtigkeit feststellen ließ. Im vorliegenden Fall ging es nicht um das Bestreiten der Tatsache, dass Bücher verschmutzt oder beschädigt worden seien, sondern lediglich um das Bestreiten des Verdachts verbunden mit einer erhöhten Prüfungstätigkeit des Bibliothekspersonals. Für den Verdacht lagen aber Anhaltspunkte vor: Das Bibliothekspersonal hatte wiederholt den Eindruck, dass ausgeliehene Bücher verschmutzt worden sein könnten. Der Widerspruch des Petenten konnte daher nicht zum Bezweifeln des Verdachts führen, sondern sich nur auf die Urheberschaft an Verschmutzungen beziehen. Letzteres war aber nicht Gegenstand der Eintragung.

8.5 Verwendung von Daten ehemaliger Zwangsarbeiter für eine Ortschronik

Eine rheinland-pfälzische Gemeinde hatte die Erstellung einer Ortschronik in Auftrag gegeben. Dort sollten sowohl personenbezogene Daten ehemaliger Zwangsarbeiter als auch deren Arbeitgeber veröffentlicht werden. Die Informationen sollten aus archivierten polizeilichen Anmeldungen entnommen werden. Der Chronist bat den LfD vorab um seine Stellungnahme, ob dies in der vorgesehenen Form zulässig sei.

Hier waren die Vorschriften des Landesarchivgesetzes zu prüfen. Nach § 3 Abs. 1 LArchG hat jeder, der ein berechtigtes Interesse darlegt, das Recht, öffentliches Archivgut zu nutzen. Archivgut, das sich auf natürliche Personen bezieht, darf gem. Abs. 3 dieser Vorschrift jedoch erst 30 Jahre nach deren Tod oder, wenn das Todesjahr dem Archiv nicht bekannt ist, erst 110 Jahre nach der Geburt der Betroffenen benutzt werden. Es war davon auszugehen, dass im vorliegenden Fall diese Fristen noch nicht abgelaufen waren, so dass eine Veröffentlichung in der vorgesehenen Form unzulässig gewesen wäre. Es wäre jedoch nicht zu beanstanden gewesen, wenn die Informationen über ehemalige Zwangsarbeiter und ihre Arbeitgeber in anonymisierter Form veröffentlicht worden wären, also man z. B. lediglich Angaben zur Zahl oder Herkunft gemacht hätte.

9. Umwelt

9.1 Umweltinformationsgesetz

9.1.1 Anzahl der Parkplätze als Umweltinformation?

Das Umweltinformationsgesetz sieht vor, dass jeder Anspruch auf freien Zugang zu Informationen über die Umwelt hat, die bei einer Behörde oder einer öffentlich-rechtliche Aufgaben wahrnehmenden Person des Privatrechts vorhanden sind. Dieser Anspruch ist beschränkt oder ausgeschlossen zum Schutz öffentlicher oder auch privater Belange. Er ist u. a. dann ausgeschlossen, wenn durch das Bekanntwerden der Informationen personenbezogene Daten offenbart und dadurch schutzwürdige Interessen der Betroffenen beeinträchtigt würden (vgl. dazu die Darstellung im 17. Tb., Tz. 9.1).

Nach diesen Vorschriften stand einem Bürger einer rheinland-pfälzischen Gemeinde ein Anspruch auf Informationen über ein größeres Bauvorhaben zu. Konkret ging es um die Erweiterung eines Seniorenwohnheims. Der Petent war Eigentümer eines Hauses im angrenzenden Wohngebiet und befürchtete durch die Erweiterung ein erhöhtes Verkehrsaufkommen, das die Ausweisung als verkehrsberuhigte Zone gefährden könne. Er wollte aus diesem Grund ein Verkehrsgutachten erstellen lassen, für das er die Anzahl und die Zuordnung der Stellplätze zu den einzelnen Gebäudekomplexen des Seniorenzentrums benötigte. Diese Auskunft wurde ihm von der Kreisverwaltung unter Berufung auf Datenschutzgründe versagt.

Das Seniorenzentrum stand im Eigentum einer privaten Person, so dass Datenschutzrecht bei einer Entscheidung über die gewünschte Auskunft grundsätzlich zu berücksichtigen war. Bei den Auskünften über die Stellplatzsituation am Seniorenzentrum handelte es sich um Umweltinformationen, da sich die Zahl der bei einem Bauvorhaben zu schaffenden Stellplätze nach dem zu erwartenden Zugangs- oder Abgangsverkehr, also nach Art und Zahl der vorhandenen und zu erwartenden Kraftfahrzeuge der Benutzer sowie der Besucher der Anlage richtete. Folglich bestand grundsätzlich ein Informationsanspruch nach dem Umweltinformationsgesetz. Fraglich war nur, ob durch die Information datenschutzrechtliche Belange der Betroffenen hätten verletzt werden können. Da die Entscheidung über die Stellplätze im baurechtlichen Verfahren in erster Linie auf verkehrsrechtlichen Aspekten beruht und daher weniger die individuellen Interessen des Bauherrn als vielmehr die der Allgemeinheit im Vordergrund stehen, war nicht zu erkennen, dass die Interessen des Eigentümers des Seniorenwohnheims an der Geheimhaltung der Informationen über die Stellplatzsituation die Interessen an deren Offenbarung überwogen. Die Kreisverwaltung hat daraufhin die entsprechenden Informationen herausgegeben.

9.1.2 Kein freier Zugang zu Umweltinformationen während eines strafrechtlichen Ermittlungsverfahrens

Hinsichtlich der Bearbeitung von Eingaben im Bereich des Umweltinformationsgesetzes war auch die einschlägige Rechtsprechung des Bundesverwaltungsgerichts von Bedeutung. Es hat in einem am 28. Oktober 1999 verkündeten Urteil (Az: 7 C 32/98) entschieden, dass der freie Zugang zu Umweltinformationen während eines strafrechtlichen Ermittlungsverfahrens hinsichtlich aller Informationen ausgeschlossen ist, die Gegenstand des laufenden Verfahrens sind. Die Vorschrift des § 7 Nr. 2 UIG wolle den ungestörten Ablauf des strafrechtlichen Ermittlungsverfahrens sichern und verhindern, dass Umweltdaten, die für das Verfahren bedeutsam seien, der Öffentlichkeit außerhalb des Verfahrens bekannt würden.

9.2 Beachtung datenschutzrechtlicher Bestimmungen bei Anfragen nach Datenmaterial in Bezug auf Altlasten

Wenn sich die Altlast auf einem Grundstück einer natürlichen Person befindet, handelt es sich bei den Angaben über die genaue Lage und die Flurstücksnummer der betroffenen Grundstücke regelmäßig um personenbezogene Daten im Sinne des Landesdatenschutzgesetzes, bei deren Weitergabe das verfassungsmäßig geschützte Recht auf informationelle Selbstbestimmung zu beachten ist.

Im Prinzip geht es immer wieder um die gleiche Frage, nämlich, ob und ggf. in welchem Umfang der Inhalt von Registern oder Archiven mit Aufzeichnungen über (z. B.) Altablagerungen an andere Behörden oder private Interessenten übermittelt oder sogar veröffentlicht werden darf. Die datenschutzrechtliche Problematik liegt darin begründet, dass einerseits ein starkes öffentliches und privates Interesse an möglichst breiter Information über die Aufzeichnungen in solchen Registern oder Katastern besteht; andererseits kann die Offenbarung grundstücksbezogener – und damit personenbeziehbarer – Daten zu gravierenden Beeinträchtigungen schutzwürdiger Belange von Grundstückseigentümern führen. Für die datenschutzrechtliche Beurteilung ist u. a. von Bedeutung, dass eine Fläche mit Altablagerungen erst dann als Altlast eingestuft wird, wenn feststeht, dass von ihr nachweislich Gefahren für die Allgemeinheit ausgehen.

Für das Verdachtsflächenkataster und das Altlastenkataster sind im Landesabfallwirtschafts- und Altlastengesetz entsprechende Regelungen in § 21 vorhanden. Danach wird der Inhalt des Verdachtsflächenkatasters und des Altlastenkatasters von der zuständigen Behörde auf Verlangen anderer Behörden und Einrichtungen des Landes, der Gemeinden, der Landkreise und kreisfreien Städte zur Wahrnehmung der diesen Stellen auf dem Gebiet der Gefahrenermittlung, Gefahrenabwehr, Überwachung oder Planung gesetzlich obliegender Aufgaben übermittelt. Soweit die zuständige Behörde Angaben über altlastverdächtige Flächen der Öffentlichkeit zugänglich macht, darf die Bekanntgabe keine personenbezogenen Daten enthalten. Dies gilt nicht, wenn solche Angaben offenkundig sind oder ihre Bekanntgabe zur Abwehr von Gefahren oder aus anderen überwiegenden Gründen des Wohls der Allgemeinheit erforderlich ist.

9.3 Haushaltserklärungen für die Gebührenerhebung bei der Abfallentsorgung

Aufgrund des Hinweises eines Betroffenen wurde bekannt, dass der Abfallwirtschaftsbetrieb eines Landkreises recht eigenwillig gestaltete Vordrucke zur Gebührenerhebung bei der Abfallentsorgung an Grundstückseigentümer bzw. an von diesen beauftragte Hausverwaltungen verschickte. Sie sollten ihre Angaben in der „Haushaltserklärung" – z. B. hinsichtlich der Anzahl der Kochgelegenheit der Mieter je Haushalt – an Eides statt versichern und wurden darauf hingewiesen, dass die Abgabe einer falschen eidesstattlichen Versicherung gerichtlich verfolgt werden kann. Diese Verfahrensweise konnte keinen Bestand haben; denn gem. § 27 Abs. 1 VwVfG darf die Behörde bei der Ermittlung des Sachverhalts eine Versicherung an Eides statt nur verlangen und abnehmen, wenn die Abnahme der Versicherung über den betreffenden Gegenstand und in den betreffenden Verfahren durch Gesetz oder Rechtsverordnung vorgesehen und die Behörde durch Rechtsvorschrift für zuständig erklärt worden ist. An diesen rechtlichen Voraussetzungen fehlte es im vorliegenden Fall. (Zudem soll eine Versicherung an Eidesstatt nur gefordert werden, wenn andere Mittel zur Erforschung der Wahrheit nicht vorhanden sind, zu keinem Ergebnis geführt haben oder einen unverhältnismäßigen Aufwand erfordern; vgl. § 27 Abs. 1 Satz 2 VwVfG.)

Die Datenerhebung bei der Abfallentsorgung ist ein Thema, das den LfD immer wieder beschäftigt. So banal die Verarbeitung personenbezogener Daten in diesem Bereich auf den ersten Blick scheinen mag, die dahinter stehende Problemlage ist durchaus komplex. Bereits im November 1998 hat sich der LfD in einer Pressemitteilung an die Öffentlichkeit gewandt, indem er auf ein für viele Bürger kostspieliges Datenschutzproblem hinwies. Betroffen sind Personen, die 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 diese verheiratet sind oder wenn Kinder bei den Eltern oder einem Elternteil leben. Personen, die z. B. in einer nichtehelichen Lebensgemeinschaft zusammenleben, werden als mehrere Einpersonenhaushalte gemeldet und, sofern den für die Festsetzung der Müllabfuhrgebühren zuständigen Behörden nichts anderes bekannt wird, als Einpersonenhaushalte veranlagt.

Betroffene Mieter merken diesen Veranlagungsfehler 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 würde 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. Der LfD weist darauf hin, dass alle Bürgerinnen und Bürger nach den Bestimmungen des Landesdatenschutzgesetzes das Recht haben, bei den zuständigen Behörden (Landkreise, kreisfreie Städte) zu erfragen, ob sie als Einpersonenhaushalt oder Mehrpersonenhaushalt veranlagt werden, und erforderlichenfalls eine Berichtigung zu verlangen. Die Wahrnehmung dieser Datenschutzrechte kann zu erheblichen Gebühreneinsparungen führen.

Es ist verständlich, dass die für die Abfallentsorgung verantwortlichen Körperschaften nach Möglichkeiten suchen, die fehlenden Informationen durch andere Quellen zu gewinnen. Entsorgungspflichtige Körperschaften sind gem. § 3 LAbfWAG die Landkreise und kreisfreien Städte. Sie können durch Satzung nach § 5 LAbfWAG festlegen, wie ihnen die Abfälle zu überlassen sind und erheben als Gegenleistung für die Inanspruchnahme ihrer öffentlichen Einrichtung Benutzungsgebühren nach den Vorschriften des Kommunalabgabengesetzes. Regelmäßig werden in den Abfall- und Abfallgebührensatzungen als Adressaten und Auskunftspflichtige die Grundstückseigentümer bestimmt. Wohl aufgrund des im Kreislaufwirtschafts- und Abfallgesetz verwendeten Begriffes „private Haushaltungen“ stellen die (meisten) Satzungen bei der Berechnung von Gebühren z. B. statt auf den Eigentümer/Mieter auf „Haushalte“ ab. Es fehlt aber jeweils eine für die Betroffenen nachvollziehbare eindeutige Definition für den Begriff des „Haushaltes“. Dies stellt sich jedoch häufig erst in der Praxis heraus, wenn sich die Angaben von Eigentümern (bzw. Verwaltern) und Mietern widersprechen, was beispielsweise zu einer Problemlage bei nichtehelichen Lebensgemeinschaften führt.

Im Berichtszeitraum ist eine Zunahme von Anfragen betroffener Bürgerinnen und Bürger hinsichtlich der Datenerhebung und -verarbeitung im Rahmen der Umsetzung von Abfallsatzungen und Abfallgebührensatzungen festzustellen. Als Ursachen haben sich insbesondere missverständliche Regelungen oder fehlende Definitionen in den Satzungen sowie mangelhafte Information der Betroffenen herausgestellt. Im Übrigen werden mitunter – wie im eingangs geschilderten Fall – Bestimmungen in Vordrucke aufgenommen, bei denen sich mangels einer vorherigen Prüfung erst später bei der praktischen Umsetzung datenschutzrechtliche Probleme ergeben.

Grundsätzlich rät der LfD, die betroffenen Grundstückseigentümer – z. B. auf der Rückseite des Vordrucks – über die Grundlage der Datenerhebung zu informieren, indem auszugsweise die Regelungen der Abfallsatzung, insbesondere hinsichtlich der Auskunftspflicht, und in der Gebührensatzung bezüglich der Haushaltsbezogenheit aufzunehmen sind. Auch eine deutliche Klarstellung, wonach in Fällen, in denen keine Angaben zur Haushaltszugehörigkeit erfolgen, bei unterschiedlichen Namen getrennte Haushalte veranlagt werden, hält er angesichts der geschilderten Problemlage für sinnvoll.

10. Gesundheitswesen

10.1 Auskunft und Akteneinsicht im Gesundheitswesen

In einer Vielzahl von Fällen musste im Berichtszeitraum zum Auskunfts- bzw. Akteneinsichtsrecht der Betroffenen Stellung genommen werden, meist weil die öffentliche Stelle derartige Ansprüche aus den verschiedensten Gründen abgelehnt hatte. Häufig kann nur ein Blick in die betreffende Akte selbst klären, ob seitens der Verwaltung Auskunft oder Einsicht zu Recht abgelehnt wurden oder nicht. Dem LfD ist es dabei freilich verwehrt, die Informationen selbst zu erteilen, er kann jedoch – bei Feststellung der Rechtswidrigkeit der Auskunftsverweigerung – nach § 25 LDSG eine formelle Beanstandung aussprechen, die zuständige Aufsichtsbehörde einschalten und dem Betroffenen damit die Entscheidung, ob er den Verwaltungsrechtsweg beschreiten möchte, erleichtern.

Nach Art. 4 a Abs. 1 Satz 2 LV hat jeder das Recht auf Auskunft über ihn betreffende Daten und auf Einsicht in amtliche Unterlagen, soweit diese solche Daten enthalten. Im Bereich des Gesundheitswesens ist dieses Grundrecht etwa in § 36 Abs. 4 LKG, § 32 Abs. 2 PsychKG oder § 10 LKRG einfachgesetzlich konkretisiert worden. Diese Regelungen enthalten auch Aussagen darüber, ob und unter welchen Voraussetzungen dem Betroffenen medizinische Informationen zu vermitteln sind (Stichwort „Therapeutisches Privileg“ – Schutz des Patienten vor Auskünften, die ihn schädigen könnten). Umso erstaunlicher ist es, dass sich im Landesgesetz über den öffentlichen Gesundheitsdienst überhaupt keine Vorschrift zum Auskunfts- und Einsichtsrecht findet. Gem. § 11 Abs. 1 ÖGdG kommt vielmehr das Landesdatenschutzgesetz zur Anwendung. Da aber auch hier spezifische Bestimmungen zur Einsichtnahme in medizinische Unterlagen fehlen, kommt man nur über eine analoge Anwendung von § 25 Abs. 2 SGB X oder § 36 Abs. 5 LKG zu sachgerechten Lösungen. Der LfD wird sich bei der nächsten Novellierung des ÖGdG für eine entsprechende Ergänzung einsetzen.

Wie in den übrigen Verwaltungsbereichen ging es auch im Gesundheitswesen in erster Linie um die Frage, ob Auskunft und Einsicht aufgrund überwiegender schutzwürdiger Interessen Dritter zu unterbleiben hatten (vgl. § 18 Abs. 3 Ziff. 3 LDSG, § 36 Abs. 5 Satz 3 LKG, § 32 Abs. 3 Satz 1 2. HS PsychKG). Als „Dritte“ sind auch private Hinweisgeber und Informanten anzusehen, deren

Identität von der Verwaltung vertraulich zu behandeln ist. Gegenüber Auskunfts- und Akteneinsichtsansprüchen des Betroffenen ist das Geheimhaltungsinteresse der Hinweisgeber daher grundsätzlich vorrangig (vgl. hierzu die vom LfD herausgegebene Orientierungshilfe „Grundsätze für den Umgang mit Daten von Hinweisgebern bzw. Informanten in der allgemeinen öffentlichen Verwaltung"). Dies bedeutet aber nicht, dass in diesen Fällen ein Akteneinsichtsrecht des Betroffenen überhaupt nicht in Betracht kommt. Informationen über Hinweisgeber können nämlich unkenntlich gemacht oder aus der Akte entfernt werden, auch wenn dies für die Daten verarbeitende Stelle mit einem gewissen Aufwand verbunden ist.

Eine Eingabe hatte u. a. die Frage zum Gegenstand, ob auch die Personen Informantenschutz genießen, welche in amtlicher Funktion im Anwendungsbereich des PsychKG – hier: Prüfung der Unterbringungsvoraussetzungen – tätig geworden sind (Bsp.: Mitarbeiter der Unterbringungsbehörde, des Ordnungsamtes oder des Gesundheitsamtes). Der LfD hat dies im konkreten Fall verneint. Würde man auch hier überwiegende schutzwürdige Interessen Dritter annehmen, würde das Akteneinsichtsrecht des Betroffenen im Ergebnis leer laufen und die Rechtsverteidigung gegen Maßnahmen nach dem PsychKG erheblich einschränken. Der VGH München hat hierzu festgestellt, dass bereits die Einleitung eines entsprechenden Verfahrens einen so gravierenden Eingriff in das Leben des Betroffenen darstellt, dass es ihm möglich sein muss, die Einzelheiten zu erfahren und zu würdigen, die mit den Amtshandlungen des Gesundheitsamtes verbunden sind (NVwZ 1990, 775 ff.).

Der LfD kam nach eingehender Prüfung zu dem Ergebnis, dass dem Einsichtsrecht zumindest teilweise zu entsprechen ist. Das Gesundheitsamt sah dies jedoch anders, so dass die Einschaltung der zuständigen Fachaufsichtsbehörde, nämlich des Landesamtes für Soziales, Jugend und Versorgung, angezeigt war. Auch nach zwei Weisungen des Landesamtes weigerte sich das Gesundheitsamt, dem Betroffenen in eingeschränkter Form Akteneinsicht zu gewähren. Es schaltete das Gesundheitsministerium ein und es entstand eine weitere Form des behördlichen Kreisverkehrs, über den bereits im 17. Tb. unter Tz. 11.2.1 berichtet wurde und der im Berichtszeitraum noch nicht sein Ende gefunden hatte.

10.2 Ärztliche Untersuchung von Beschäftigten der Kreisverwaltungen und ihren Angehörigen

In einer Eingabe an den LfD wurde auf Folgendes hingewiesen: Mitarbeiterinnen und Mitarbeiter von Kreisverwaltungen hätten keine Möglichkeit zu verhindern, dass bei dienstrechtlich veranlassten ärztlichen Untersuchungen oder bei sonstigen ärztlichen Untersuchungen – auch von Angehörigen – Kolleginnen und Kollegen der gleichen Behörde personenbezogene medizinische Daten zur Kenntnis nehmen können. Es gehe zum einen um Kolleginnen und Kollegen der Gesundheitsämter, zum anderen aber, je nachdem, wie der Postlauf organisiert sei, auch um Kolleginnen und Kollegen, die in der Kreisverwaltung außerhalb des Gesundheitsamtes beschäftigt sind.

Dieses Problem ist sicherlich nicht ganz neu; auch vor der Übertragung der Aufgaben der unteren Gesundheitsbehörden auf die Kreisverwaltungen war nicht auszuschließen, dass eine persönliche Nähe zwischen Bediensteten verschiedener Behörden bestand und die Kenntnisnahme der Befunde usw. von den Betroffenen als unangenehm empfunden wurde. Mit der Eingliederung der Gesundheitsämter ist es aber noch deutlicher zutage getreten.

Da sich bei der Bearbeitung der Steuerangelegenheiten von Amtsangehörigen der Finanzämter ähnliche Probleme ergeben können, hatte das Ministerium der Finanzen verfügt, dass Mitarbeiter, deren Beschäftigungsfinanzamt gleichzeitig das für ihre steuerlichen Angelegenheiten zuständige Finanzamt ist, die Besteuerung durch ein anderes Finanzamt beantragen können. Auf gesetzlicher Ebene existieren indessen nur Regelungen, die zuvörderst auf die Vermeidung von Interessenkollisionen zielen (z. B. § 102 a LBG, § 35 Abs. 1 SGB I).

Der LfD wandte sich in der Sache an den Landkreistag, um eine mit der Finanzverwaltung vergleichbare Lösung auch für die Beschäftigten der Kreisverwaltungen und ihre Angehörigen zu erreichen. Dieser zeigte sich hinsichtlich der Problematik aufgeschlossen. In einem Schreiben an die Mitglieder des Sozial- und Gesundheitsausschusses wies die Geschäftsstelle des Landkreistages darauf hin, dass es die Betroffenen zwar hinzunehmen haben, wenn im Rahmen von amtsärztlichen Untersuchungen den damit notwendigerweise befassten Behördenmitarbeitern medizinische Daten im erforderlichen Umfang bekannt werden. Eine Lösung sei jedoch dergestalt vorstellbar, dass dem berechtigten Wunsch eines Betroffenen auf Untersuchung durch den Amtsarzt eines anderen Gesundheitsamtsbezirkes in begründeten Einzelfällen dann entsprochen wird, wenn er die entstehenden Mehrkosten trägt. Diese Lösung wurde von dem Ausschuss akzeptiert; für die Beschäftigten der Kreisverwaltungen und ihre Angehörigen wurde damit eine deutliche datenschutzrechtliche Verbesserung erreicht.

10.3 Einschaltung einer „Medizinischen Verbindungsstelle" bei Inruhestandsversetzung von Beamtinnen und Beamten

Seit dem 1. März 2001 ist beim Landesamt für Soziales, Jugend und Versorgung eine „Medizinische Verbindungsstelle" eingerichtet, die bei allen nach §§ 56 ff. LBG beantragten amtsärztlichen Beurteilungen der Dienstfähigkeit staatlicher Beamtinnen und Beamten zu beteiligen ist. Die Verbindungsstelle nimmt qualitätssichernde Aufgaben, namentlich die Prüfung der Plausibilität der von den Amtsärztinnen und Amtsärzten erstellten medizinischen Gutachten, wahr. Bestehen nach Auffassung der „Medizinischen Verbindungsstelle" insoweit Zweifel, kann sie diese durch Rückfragen beim Gesundheitsamt oder durch Einholung zusätzlicher Informationen klären und ggf. eine Ergänzung, Klarstellung oder Abänderung der amtsärztlichen Beurteilung anregen, ohne jedoch

fachlich weisungsbefugt zu sein. Bei Fortbestehen der Zweifel ist sie berechtigt, dies der personalbewirtschaftenden Dienststelle mitzuteilen. Nach Abschluss des Verfahrens werden bei der „Medizinischen Verbindungsstelle“ nur noch anonymisierte Daten zu statistischen Zwecken vorgehalten.

Der LfD, der vom Gesundheitsministerium beteiligt wurde, wies darauf hin, dass gesetzliche Bestimmungen zum Datenschutz bei amtsärztlichen Untersuchungen nur insoweit vorhanden sind, als nach §§ 56, 81 und 210 LBG der Amtsarzt dem Dienstherrn die für die Feststellung der Dienstunfähigkeit erforderlichen Untersuchungsergebnisse mitteilt. Die mit dem neuen Verfahren einhergehenden Datenverarbeitungsprozesse konnten daher nur auf der Basis einer informierten Einwilligungserklärung der betroffenen Beamtinnen und Beamten erfolgen.

Einem mit dem LfD abgestimmten Rundschreiben des Ministeriums an die Kreisverwaltungen wurde ein Mustertext für eine entsprechende Einverständniserklärung beigefügt. Die Betroffenen werden hierin über Einschaltung und Aufgaben der „Medizinischen Verbindungsstelle“ einschließlich der Datenverarbeitungsprozesse, die Freiwilligkeit der Einwilligung, das Nichtbestehen von Nachteilen bei einer Weigerung sowie über Akteneinsichts- und Auskunftsansprüche unterrichtet. Die Erklärung genügt damit den Anforderungen, die an eine datenschutzrechtliche Einwilligungserklärung sowie an eine wirksame Befreiung von der ärztlichen Schweigepflicht zu stellen sind.

Erste Untersuchungen des Gesundheitsministeriums haben indessen ergeben, dass von der Widerspruchsmöglichkeit in etwa der Hälfte der Fälle Gebrauch gemacht wird. Vor diesem Hintergrund bestehen Bestrebungen, durch eine Änderung des Landesbeamtengesetzes die Einschaltung der „Medizinischen Verbindungsstelle“ in jedem Einzelfall ohne Widerspruchsmöglichkeit der Betroffenen verbindlich festzuschreiben. Der LfD wird diese Entwicklung kritisch begleiten und darauf achten, dass durch diese Gesetzesänderung die Datenschutzrechte der Betroffenen nicht in unverhältnismäßigerweise Weise eingeschränkt werden.

10.4 Datenschutz im Rahmen der Aufnahmekonferenz innerhalb der Gemeindepsychiatrischen Wohnverbünde

Das PsychKG sieht die Bildung von Gemeindepsychiatrischen Verbünden vor und weist den Landkreisen und kreisfreien Städten die Planung und Koordination der psychischen Hilfen in diesem Zusammenhang zu (§ 7 PsychKG). Durch eine Vernetzung der Hilfen vor Ort (Bsp.: Tagesstätten mit Kontaktstellenfunktion, beratende und aufsuchende Dienste und Angebote des Betreuten Wohnens) soll gewährleistet werden, dass die psychisch behinderten Menschen die für sie notwendigen Hilfen dort erhalten, wo sie leben. Im Kontext hierzu sind die neuen Regelungen in §§ 93 ff. BSHG zu sehen, welche die Träger der Sozialhilfe verpflichten, vor der Schaffung eigener neuer Einrichtungen und Dienste Vereinbarungen mit anderen Trägern über die Inanspruchnahme deren Einrichtungen abzuschließen.

In Umsetzung dieser Bestimmungen wurde für den Gemeindepsychiatrischen Wohnverbund im Landkreis Trier-Saarburg und in der Stadt Trier in Zusammenarbeit mit dem Sozialministerium eine Aufnahmekonferenz eingerichtet. Diese setzt sich aus Vertretern verschiedener Einrichtungen, die im Rahmen der Eingliederungshilfe für seelisch Behinderte Leistungen erbringen, zusammen (Bsp.: Kliniken, Sozialpsychiatrischer Dienst, Psychiatrie-Koordinatoren, Sozialhilfeträger). Sie hat die Aufgabe, zu Art, Inhalt, Ziel und Umfang der Hilfen, die im Rahmen der Eingliederungshilfe nach §§ 39, 40 BSHG für seelisch behinderte Personen aus dem Einzugsbereich beantragt oder erbracht werden, gegenüber dem Kostenträger eine Stellungnahme in Form einer Empfehlung abzugeben.

Die Einschaltung der Aufnahmekonferenz ist auch von datenschutzrechtlicher Relevanz, da in den Sitzungen sensible Informationen über das Hilfeplanverfahren des Antragstellers bekannt werden. Dies basiert zwar auf einer Einwilligungserklärung der Betroffenen, gleichwohl ergaben sich in der konkreten Umsetzung eine ganze Reihe von datenschutzrechtlichen Fragen, etwa in Bezug auf die Einwilligungsfähigkeit, die Personenbeziehbarkeit sowie die Erhebung und Verarbeitung von Drittdaten (Bsp.: Angehöriger). Die Einwilligungserklärung wurde in Zusammenarbeit mit dem Ministerium dergestalt modifiziert, dass dem Betroffenen drei verschiedene Möglichkeiten offeriert werden: Er kann sich mit der Weitergabe personenbezogener Daten einverstanden erklären, alternativ kann er in die Weitergabe anonymisierter Daten einwilligen oder einer Übermittlung, in welcher Form auch immer, insgesamt widersprechen. Auch zu den weiteren aufgeworfenen Fragen wurden sachgerechte Lösungen gefunden, so dass das Verfahren insgesamt datenschutzverträglich ausgestaltet werden konnte.

10.5 Weitergabe von Patientendaten an den Betreuer

Die Psychiatrische Abteilung eines Krankenhauses bat um eine Stellungnahme zu der Frage, inwiefern ohne Einverständnis des betroffenen Patienten eine Befugnis bzw. Verpflichtung besteht, einem Betreuer medizinische Informationen über die von ihm zu betreuende Person zu übermitteln.

Im vorliegenden Fall war davon auszugehen, dass die Vorschriften des PsychKG, welches die Hilfen und Schutzmaßnahmen für psychisch kranke Personen einschließlich der freiheitsentziehenden Unterbringung regelt, zur Anwendung kommen. Als „psychisch krank“ im Sinne dieses Gesetzes gelten Personen, die an einer Psychose, an einer psychischen Störung, die in ihrer Auswirkung einer Psychose gleichkommt, oder an einer mit dem Verlust der Selbstkontrolle einhergehenden Abhängigkeit von Suchtstoffen leiden (§ 1 Abs. 2 PsychKG).

Bei Vorliegen dieser Voraussetzungen bestimmt sich die Zulässigkeit der Datenverarbeitung nach §§ 32 ff. PsychKG, und zwar unabhängig davon, ob die Person gem. § 11 ff. PsychKG untergebracht ist oder nicht.

Die Übermittlung personenbezogener Daten an Personen, denen die gesetzliche Vertretung obliegt, ist gem. § 34 Abs. 3 Ziff. 2 PsychKG nur zulässig, soweit dies für die Wahrnehmung der damit zusammenhängenden Aufgaben erforderlich ist.

Demnach besteht keine Verpflichtung, sondern lediglich eine Befugnis, personenbezogene Daten im erforderlichen Umfang an den Betreuer als gesetzlichen Vertreter weiterzugeben. Bei der Anforderung von Informationen, die der ärztlichen Schweigepflicht unterliegen, ist vom Behandler zu prüfen, ob die Voraussetzungen des § 34 Abs. 3 Ziff. 2 PsychKG und damit eine im Sinne des § 203 Abs. 1 StGB „befugte" Offenbarung von Patientendaten vorliegt. Ob und inwieweit von einer in diesem Sinne „erforderlichen" Datenübermittlung auszugehen ist, hängt entscheidend vom Aufgabenkreis und der insoweit bestehenden Vertretungs- und Handlungsvollmacht des Betreuers ab:

Sind einem Betreuer sämtliche persönliche Angelegenheiten des Betreuten einschließlich der Gesundheitsfürsorge zugewiesen worden, gehört dazu auch die Befugnis, über die medizinische Behandlung – ggf. mit Genehmigung des Vormundschaftsgerichts (vgl. § 1904 BGB) – zu bestimmen. Dann steht der Betreuer im Verhältnis zum Arzt bzw. Krankenhaus an der Stelle des Betreuten und hat die gleichen Auskunftsansprüche wie dieser. Die bloße Befugnis zur Datenweitergabe kann sich in diesen Fällen zu einer Übermittlungsverpflichtung verdichten.

Sind dem Betreuer dagegen nur bestimmte Teilbereiche (z. B. Vermögensverwaltung) zugewiesen worden, kann die Erforderlichkeit einer Anforderung von Patientendaten fraglich sein. Wegen seiner persönlichen Verantwortlichkeit für die Rechtmäßigkeit der Übermittlung medizinischer Daten muss der Behandler im Zweifelsfalle vom Betreuer eine schlüssige und nachvollziehbare Begründung der Datenanforderung verlangen.
Die Personen, an die personenbezogene Daten übermittelt worden sind, haben diese in demselben Umfang geheim zu halten, wie die übermittelnde Person oder Stelle selbst (§ 34 Abs. 4 PsychKG).

Das Krankenhaus wurde in diesem Sinne unterrichtet.

10.6 Zeugnisverweigerungsrechte im Erbscheinverfahren

Ein Mitarbeiter des Sozialpsychiatrischen Dienstes der Kreisverwaltung Altenkirchen erhielt vom LG Koblenz eine Zeugenladung in einem Verfahren zur Erteilung eines Erbscheins. Der Erblasser, der wegen seiner Alkoholerkrankung in der Betreuung des Gesundheitsamtes stand, hatte mehrere letztwillige Verfügungen zu Gunsten seiner Lebensgefährtin getroffen, die nach seinem Tod von der Witwe angefochten wurden. Das Gericht beabsichtigte, auch anhand der Zeugenaussage des Mitarbeiters des Sozialpsychiatrischen Dienstes Beweis darüber zu erheben, ob der Verstorbene zurzeit der Errichtung des Testaments testierfähig war.

Das Problem bestand nach Auffassung der Kreisverwaltung in der Regelung des § 203 StGB, der die unbefugte Offenbarung von Geheimnissen durch sog. Berufsgeheimnisträger, zu denen auch der Mitarbeiter des Sozialpsychiatrischen Dienstes zu zählen war, unter Strafe stellt. Die Schweigepflicht besteht nach Abs. 4 dieser Vorschrift auch über den Tod des Betroffenen hinaus.

Da für Fälle der dargestellten Art keine ausdrückliche gesetzliche Übermittlungsvorschrift existiert, darf ein Mitarbeiter des Sozialpsychiatrischen Dienstes im Zivilprozess nur dann aussagen, wenn davon auszugehen ist, dass diese Aussage dem tatsächlichen bzw. dem mutmaßlichen Willen des Verstorbenen entspricht.

Eine positive Willensäußerung des Verstorbenen lag jedoch nicht vor und ob eine Zeugenaussage dem mutmaßlichen Willen des Verstorbenen entspricht, ist auf den ersten Blick nicht leicht zu beantworten. In einem vergleichbaren Fall, in dem es um die Zeugenaussage eines Arztes zur Frage der Testierfähigkeit im Rahmen eines Erbscheinverfahrens ging, hat der BGH zur mutmaßlichen Einwilligung aber ausgeführt, dass das Interesse des Erblassers im Allgemeinen dahin gehe, aufkommende Zweifel über seine Testierfähigkeit nach Möglichkeit auszuräumen. Sein wohlverstandenes Interesse sei nicht darauf gerichtet zu verbergen, dass er testierunfähig sei. Dies schließe nicht aus, dass sich der Zeuge bei einzelnen Fragen auf sein Zeugnisverweigerungsrecht nach § 383 Abs. 1 Ziff. 6 ZPO berufen könne (BGH NJW 1984, 2893).

Vor dem Hintergrund dieser Rechtsprechung war davon auszugehen, dass im vorliegenden Fall eine Zeugnispflicht des Mitarbeiters des Sozialpsychiatrischen Dienstes dem Grunde nach besteht. Die Kreisverwaltung wurde entsprechend unterrichtet.

10.7 Datenschutzfragen in Zusammenhang mit der Bestellung von Transplantationsbeauftragten

Das Landesgesetz zur Ausführung des Transplantationsgesetzes (AGTPG) sieht vor, dass jedes Krankenhaus mit Intensiv- oder Beatmungsbetten einen Arzt oder eine Ärztin als Transplantationsbeauftragten zu bestellen hat (§ 5 AGTPG). Dieser berät und unterstützt die Beschäftigten der Krankenhäuser und Patienten in Fragen der Transplantationsmedizin und ist insbesondere dafür verantwortlich, dass die Krankenhäuser den Hirntod eines Patienten dem zuständigen Transplantationszentrum mitteilen.

Aufgrund der Anfrage einer Fraktion im Landtag hatte sich der LfD mit der datenschutzrechtlichen Problematik im Zusammenhang mit der Bestellung von Transplantationsbeauftragten zu befassen. In seiner Stellungnahme wies der LfD darauf hin, dass das Landesgesetz vor dem Hintergrund des Transplantationsgesetzes des Bundes vom 5. November 1997 (BGBl. I S. 2631) zu sehen ist. Diese bundesrechtliche Vorgabe enthält in § 11 Abs. 4 TPG insoweit eine für die datenschutzrechtliche Beurteilung maßgebliche Regelung, als die Krankenhäuser hierin verpflichtet werden, dem zuständigen Transplantationszentrum potentielle Organspender einschließlich der hierfür erforderlichen personenbezogenen Daten mitzuteilen. Das AGTPG überträgt diese Mitteilungspflicht dem Transplantationsbeauftragten, schreibt ihm weitere Aufgaben zu und verpflichtet das Krankenhaus, ihm die hierfür erforderlichen Informationen zur Verfügung zu stellen. Die o. g. Vorschriften beinhalten somit eine auch von Datenschutzseite geforderte normenklare Regelung zur Durchbrechung der ärztlichen Schweigepflicht (vgl. § 203 Abs. 1 StGB).

Es stellt sich allerdings die Frage, ob durch die Datenerhebungsbefugnisse des Transplantationsbeauftragten im AGTPG zusätzlich in unverhältnismäßiger Weise in das informationelle Selbstbestimmungsrecht der Patienten oder Angehörigen eingegriffen wird. Dies ist nach Auffassung des LfD nicht der Fall:

§ 11 Abs. 4 TPG verpflichtet „die Krankenhäuser" insgesamt, nicht aber eine bestimmte Person innerhalb des Krankenhauses zu den o. g. Mitteilungen. Dass diese ausschließlich vom behandelnden Arzt vorgenommen werden dürfen, lässt sich aus § 11 Abs. 4 TPG nicht ableiten. Dem Landesgesetzgeber steht daher bei der Frage, wie die Mitteilungspflichten umzusetzen sind, ein Gestaltungsspielraum zu. Richtig ist, dass durch die Bestellung von Transplantationsbeauftragten der Kreis der Personen, die Zugang zu personenbezogenen medizinischen Daten haben, erweitert wird, was wiederum mit Informationseingriffen zu Lasten von Patienten und Angehörigen verbunden ist. Andererseits erscheint die klare Festlegung von Aufgaben und Befugnissen des zum Transplantationsbeauftragten bestellten Arztes gerade auch in Abgrenzung zum Aufgabenbereich des behandelnden Arztes durchaus als sachgerecht, die bundesrechtlich vorgegebene Verpflichtung zur Mitwirkung bei der Organtransplantation effektiv umzusetzen. Datenschutzrechtlich ist es nicht zu beanstanden, wenn der Gesetzgeber den ihm zustehenden Gestaltungsspielraum in der erfolgten Art ausfüllt und insoweit das informationelle Selbstbestimmungsrecht von Patienten und Angehörigen in geringem Maße beschränkt.

10.8 Chipkarten im Gesundheitswesen

Die Datenschutzbeauftragten des Bundes und der Länder haben bereits auf ihrer 47. Konferenz im März 1994 und auf ihrer 50. Konferenz im November 1995 (s. Anlage 28) zum Einsatz von Chipkarten im Gesundheitswesen Stellung genommen. Die hier formulierten datenschutzrechtlichen Anforderungen haben auch in Bezug auf aktuelle Chipkartenprojekte auf Bundes- und Landesebene nach wie vor Geltung. Zu erwähnen sind hier in erster Linie die vom Bundesgesundheitsministerium angekündigte Einführung eines elektronischen Arzneimittelpasses (s. hierzu Tz. 10.8.1), die Erweiterung der gesetzlichen Krankenversicherungskarte um ein Lichtbild (s. Tz. 10.8.2) oder das Bemühen des Gesundheitsministeriums, einmal mehr eine Patientenchipkarte modellhaft zu erproben (zum Modellversuch Neuwied/Rhein s. 15. Tb., Tz. 10.8; 16. Tb., Tz. 10.6.2 und 17. Tb., Tz. 10.9).

10.8.1 Einführung eines Arzneimittelpasses

Ausgelöst durch die Lipobay-Affaire plante das Bundesgesundheitsministerium die grundsätzlich „verpflichtende" Verwendung eines elektronischen Arzneimittelpasses. Dieser sollte einen möglichst lückenlosen Überblick über die Medikamententherapie eines Patienten bieten und so das Risiko unerwünschter Wechselwirkungen mit anderen Mitteln mindern.

Die Datenschutzbeauftragten des Bundes und der Länder haben hiergegen Bedenken erhoben. Aufgrund der verordneten Medikamente kann nämlich ohne weiteres auf die Erkrankung geschlossen werden. Wenn ein Patient gezwungen sei, bei jedem Arztbesuch seine Chipkarte vorzulegen, kann er damit nicht mehr selbst bestimmen, welche Informationen er dem Arzt mitteilen möchte, um etwa eine unvoreingenommene zweite Fachmeinung einzuholen.

Die Einführung eines Arzneimittelpasses kommt aus datenschutzrechtlicher Sicht daher nur auf freiwilliger Basis in Betracht. Die freie Entscheidung des Patienten darf in Bezug auf die Haftung nicht durch eine sachwidrige Risikoverlagerung auf den Patienten beeinflusst werden. Denn auch beim Einsatz eines Arzneimittelpasses bleibt es im Hinblick auf die Arzneimittelsicherheit bei der grundsätzlichen Verantwortung der Ärzte und Apotheker. Darüber hinaus ist im Vorfeld zu klären, ob das mit der Einführung der Medikamentenchipkarte verfolgte Ziel, nämlich unerwünschte Wechselwirkungen zu vermeiden, überhaupt erreicht werden kann. Angesichts der zahlreichen nicht verschreibungspflichtigen Medikamente, von denen ebenfalls Wechselwirkungen ausgehen können, sowie der Möglichkeit, Medikamente aus dem Ausland oder über das Internet zu beziehen, sind Zweifel im Hinblick auf die Geeignetheit angebracht.

Das Bundesgesundheitsministerium hat in der Zwischenzeit signalisiert, das weitere Verfahren mit dem BfD abzustimmen. Neben der freiwilligen Verwendung der Karte soll auch das rechtswidrige Auslesen der dort gespeicherten Daten unter Strafe gestellt werden.

10.8.2 Die Krankenversichertenkarte mit Lichtbild

Aus Marketing-Gründen, aber auch um eine missbräuchliche Verwendung der gesetzlichen Krankenversichertenkarte zu vermeiden, gehen einige Krankenkassen dazu über, ihren Versicherten auf freiwilliger Basis die gesetzliche Krankenversichertenkarte mit Lichtbild anzubieten.

Der LfD vertritt hierzu die Auffassung, dass aufgrund des abschließenden Datenkatalogs in §§ 15 Abs. 4 S. 2, 291 Abs. 2 SGB V Krankenkassen – auch mit einer Einwilligungserklärung des Versicherten – grundsätzlich gehindert sind, die gesetzlich zugelassenen Informationen auf der Krankenversichertenkarte um ein Lichtbild zu ergänzen (s. hierzu auch Entschließung der 47. DSB-Konferenz, Anlage 28). Auch nach Meinung des mit der Sache befassten Gesundheitsministeriums bestehen angesichts der gegenwärtigen Gesetzeslage rechtliche Bedenken, die Krankenversichertenkarte um ein Lichtbild zu ergänzen.

Bis zum Vorliegen einer gesetzlichen Änderung, für die sich die Krankenkassen und ihre Spitzenverbände einzusetzen haben, kommt der Einsatz der erweiterten Chipkarte auf freiwilliger Basis daher lediglich innerhalb eines Modellversuchs in Betracht. Innerhalb solcher Modellprojekte, bei denen in erster Linie die Akzeptanz der Lichtbild-Chipkarte bei den Versicherten getestet werden soll, muss allerdings die modellhafte Erprobung der Chipkarte im Vordergrund stehen, eine flächendeckende Vollversorgung aller Versicherten ausgeschlossen sein und den Anforderungen an eine informierte Einwilligungserklärung gem. § 67 b Abs. 2 SGB X Rechnung getragen werden. Bei Vorliegen dieser Mindestvoraussetzungen ist angesichts der als gering zu bewertenden Persönlichkeitsbeeinträchtigung der Betroffenen die Erweiterung der gesetzlichen Krankenversichertenkarte um ein Lichtbild datenschutzrechtlich hinnehmbar.

10.9 Studie „Risikofaktoren für sporadische EHEC-Infektionen“

Das Robert-Koch-Institut plante eine Studie über bestimmte Bakterien unter den Lebensmittelinfektionserregern (enterohämorrhagische Escherichia coli – EHEC). Erklärtes Ziel dieser Studie war es, Risikofaktoren für sporadische EHEC-Infektionen zu identifizieren, um nachfolgend geeignete Interventionsstrategien entwickeln zu können. Da diese Erkrankungen bei den Gesundheitsämtern meldepflichtig sind, sollten die dort vorliegenden Adressen für die Kontaktaufnahme mit den Betroffenen genutzt werden. Die Gesundheitsämter sollten sowohl Erkrankte als auch gesunde Kontrollpersonen telefonisch interviewen, nachdem diese ihr Einverständnis erklärt hatten. Nach Vorlage der Unterlagen konnte bestätigt werden, dass das Verfahren keinen datenschutzrechtlichen Bedenken begegnete.

10.10 Datenschutz in Kindertagesstätten

Ein Gesundheitsamt bot in den Kindergärten für 5- bis 6-Jährige Seh- bzw. Hörtests an, die auf freiwilliger Basis durchgeführt wurden. Die Kindergärten wurden telefonisch benachrichtigt, wann solche Tests stattfinden sollten. Es oblag dann den Kindergärten, die Eltern zu informieren und die Kinder zu dem Test zu schicken, deren Eltern in die Teilnahme eingewilligt hatten. Das Gesundheitsamt selbst überprüfte nicht, ob die vorgestellten Kinder tatsächlich mit Einwilligung der Eltern teilnahmen. Der Befund wurde üblicherweise in einem verschlossenen, mit dem Namen der Eltern versehenen Umschlag der Kindergärtnerin übergeben, die diesen dann an die Eltern weiterleiten sollte. Dazu erbat das Gesundheitsamt vom Kindergarten die Anschriften der Eltern der untersuchten Kinder. Dieser Wunsch nach Datenübermittlung stieß in den Kindergärten auf Bedenken.

Um das aus datenschutzrechtlicher Sicht beste Verfahren sicherzustellen, hat der LfD angeregt, dass die Gesundheitsämter selbst die Einholung der Einwilligung der Eltern übernehmen sollten. Dies konnte in Form eines kurzen Informationsschreibens an die Eltern geschehen, das über die Kindergärten an diese weitergeleitet wird. Darauf hätten die Eltern ihre schriftliche Einwilligung erklären können. Das Kind konnte diese Erklärung zur Untersuchung mitbringen, sodass aus dem Formular auch der Name der Eltern für die Mitteilung des Befundes entnommen werden konnte. Dadurch wäre sichergestellt gewesen, dass tatsächlich nur die Kinder an der Untersuchung teilnehmen, deren Eltern ihre Einwilligung erklärt haben.

Bei Beibehaltung des praktizierten Verfahrens hielt der LfD es für erforderlich, den Kindergärten eine Information über die Untersuchungen zur Verfügung zu stellen, in der Zweck und Inhalt der geplanten Datenerhebung sowie die weitere Datenverwendung erklärt wurden. Mit dieser Information hätten die Kindergärten die Eltern ausreichend im Sinne des Gesundheitsamtes über die beabsichtige Untersuchung informieren können.

Das Gesundheitsamt hat das Verfahren entsprechend den Empfehlungen des LfD geändert.

11. Sozialdatenschutz

11.1 Krankenkassen, Kassenärztliche Vereinigungen

11.1.1 Anforderung medizinischer Unterlagen durch Krankenkassen bei Krankenhäusern

Die Anforderung medizinischer Krankenunterlagen durch Krankenkassen gelangt immer wieder in die datenschutzrechtliche Diskussion (s. auch 14. Tb, Tz. 11.2.8). Und dabei ist die Rechtslage im Krankenhausbereich erfreulich normenklar geregelt: § 301 SGB V beinhaltet einen Katalog von Daten, die eine Krankenkasse für Abrechnungszwecke zulässigerweise anfordern darf. Die Krankenhäuser sind verpflichtet, den Krankenkassen diese Informationen zu übermitteln.

Obwohl der Katalog des § 301 SGB V umfangreich ist und auch sensible medizinische Informationen erfasst (Bsp: sämtliche Diagnosen, durchgeführte Operationen und sonstige Prozeduren, medizinische Begründung bei Überschreitung der voraussichtlichen Krankenhausverweildauer), wird er von einigen Krankenkassen offenbar als nicht ausreichend empfunden. Selbst angesichts der spezialgesetzlichen und damit im Grundsatz abschließenden Regelung sehen sie sich nicht gehindert, im Zusammenhang mit der Abrechnung der Krankenhausleistung – auch ohne Beteiligung des Patienten – medizinische Informationen anzufordern, die in § 301 SGB V nicht genannt sind (z. B. Arzt-, Operations- und Krankenhausentlassungsberichte).

Es wäre datenschutzrechtlich nicht zu beanstanden, wenn die Krankenhäuser entsprechende Anfragen der Krankenkassen unbeantwortet ließen, wenn nicht in der sozialgerichtlichen Rechtsprechung die Tendenz erkennbar wäre, den Krankenkassen in verstärktem Umfang medizinische Informationen zukommen zu lassen. Und dies, obwohl das Zusammenspiel der Regelungen im SGB V nicht nur eine andere Sichtweise ermöglicht, sondern – aus Sicht des LfD – sogar zwingend erfordert:

Dem Medizinischen Dienst der Krankenversicherung (MDK) ist nach den Vorschriften des SGB V im Zusammenhang mit der Krankenhausabrechnung die Rolle zugedacht, mit seinen gegenüber den Krankenkassen weiter gehenden Datenerhebungsbefugnissen Streitfälle zwischen diesen und den Krankenhäusern zu klären. Die Befugnis der Krankenkassen zur Datenübermittlung an den MDK (§ 276 Abs. 1 SGB V) bezieht sich nur auf solche Daten, die der Krankenkasse zulässigerweise (z. B. nach § 301 SGB V) übermittelt worden sind. Alle Informationen, die der MDK zusätzlich benötigt, kann er im Rahmen seiner ihm zustehenden Befugnisse (§§ 275 ff. SGB V) nach Maßgabe des § 276 Abs. 2 SGB V selbst erheben. Nur so ist verständlich, dass der MDK gegenüber den Krankenkassen wiederum nur über eingeschränkte Übermittlungsbefugnisse verfügt.

Daraus folgt: MDK und Krankenkasse nehmen innerhalb des Systems der gesetzlichen Krankenversicherung unterschiedliche Aufgaben wahr und bilden keinesfalls eine „speichernde Stelle" i. S. d. § 67 Abs. 9 SGB X. Vielmehr haben beide die für sie jeweils geltenden Datenschutzbestimmungen bei der Datenerhebung und -verarbeitung zu beachten. Die rechtliche Zulässigkeit der Anforderung von Patientendaten gegenüber Krankenhäusern hängt somit maßgeblich davon ab, ob diese durch den MDK (nach Maßgabe des § 276 Abs. 2 SGB V) oder durch die Krankenkasse (nach Maßgabe des § 301 SGB V) erfolgt – ein Umstand, der in der sozialgerichtlichen Rechtsprechung häufig keine hinreichende Berücksichtigung findet.

Gleiches gilt für die datenschutzrechtlich zwingend erforderliche Differenzierung zwischen der Befugnis zur Datenerhebung und der Befugnis zur Datenübermittlung. Selbst wenn Krankenkassen gem. § 284 SGB V Sozialdaten erheben dürfen, bedeutet dies nicht, dass die Stelle, bei der die Daten angefordert werden, ihrerseits zur Übermittlung befugt oder gar verpflichtet wäre (s. hierzu auch 17. Tb., Tz. 11.5.2). Hat ein Krankenhaus als übermittelnde Stelle die ärztliche Schweigepflicht zu beachten, bedarf eine i. S. d. § 203 Abs. 1 StGB „befugte" und damit straffreie Weitergabe von Patientendaten entweder der Einwilligungserklärung des Patienten oder einer normenklaren gesetzlichen Grundlage (Bsp.: § 301 SGB V). Das „allgemeine System der Ausgestaltung der Beziehungen zwischen den Krankenkassen und den Krankenhäusern" vermag – wie das Sozialgericht Speyer (Urteil vom 10. Juli 2000; Az.: S 3 K 181/98) meint, eine Durchbrechung der ärztlichen Schweigepflicht jedenfalls nicht zu legitimieren. Auch ein Rückgriff auf das Landeskrankenhausgesetz führt – unabhängig von der Frage, ob dieses im Hinblick auf die bundes- und spezialgesetzlichen Übermittlungsbestimmungen des SGB V überhaupt zur Anwendung kommen kann – nicht weiter, da § 36 Abs. 3 Ziff. 6 LKG die Übermittlung von Patientendaten an Sozialleistungsträger nur im erforderlichen Umfang zulässt. Welche Daten bei der Krankenhausabrechnung für Krankenkassen erforderlich sind, hat der Bundesgesetzgeber in § 301 SGB V konkretisiert. Aus diesem Grunde vermag auch die – noch nicht rechtskräftige – Entscheidung des Landessozialgerichts Rheinland-Pfalz (Urteil vom 1. März 2001; Az.: L 5 KR 55/00; DUD 2001, 489 f.) in zweiter Instanz, in der § 36 Abs. 3 Ziff. 6 LKG als einschlägige Rechtsgrundlage für die Weitergabe von Arzt-, Operations- und Krankenhausentlassungsberichten angesehen wurde, nicht zu überzeugen.

§ 301 SGB V stellt daher die grundsätzlich abschließende Regelung zulässiger Datenübermittlungen zu Abrechnungszwecken dar. Auf der Basis dieser Informationen ist die Krankenkasse in der Regel auch in der Lage zu prüfen, ob der MDK gem. §§ 275 Abs. 1 i. V. m. 284 Abs. 1 Ziff. 7 SGB V einzuschalten ist. Anhaltspunkte für eine Prüfung können sich beispielsweise aus unklaren oder mehreren sich widersprechenden Diagnosen oder mit der Diagnose nicht zu vereinbarenden Behandlungsmaßnahmen ergeben. Begehrt die Krankenkasse in begründeten Einzelfällen zur Vorprüfung, ob der MDK einzuschalten ist, über den Katalog des § 301 SGB V hinausgehende medizinische Angaben, dürfen diese an die Krankenkasse nur auf der Basis einer informierten Einwilligungserklärung des Patienten vom Krankenhaus herausgegeben werden.

Die AOK Rheinland-Pfalz als größte der Kontrollkompetenz des LfD unterliegende Krankenkasse vertritt auch angesichts der insoweit gegenteiligen Rechtsprechung die Auffassung, dass bei einem konsequent durchgeführten operativen Fallmanagement die Daten nach § 301 SGB V ausreichen, um ihre Aufgaben innerhalb des Systems der gesetzlichen Krankenversicherung erfüllen zu können. Sie sieht daher auch im Hinblick auf die o. g. Entscheidung des Landessozialgerichts Rheinland-Pfalz keine Veranlassung, künftig Arzt,- Operations- oder Entlassungsberichte von Krankenhäusern anzufordern.

Im Zusammenhang mit der Überprüfung der Behandlungsdauer gibt die AOK Rheinland-Pfalz allerdings unter bestimmten Voraussetzungen nur befristete Kostenübernahmeerklärungen ab. Dies ist dann der Fall, wenn das Krankenhaus eine unpräzise Schätzung der voraussichtlichen Behandlungsdauer vorgenommen hat. Bei Überschreitung der von der AOK gesetzten Frist wird eine medizinische Begründung verlangt.

Nach Auffassung der AOK Rheinland-Pfalz zählt es zu den Pflichten der Krankenhäuser, nach § 301 Abs. 1 Ziff. 3 SGB V eine auf den Einzelfall bezogene sorgfältige Prüfung der voraussichtlichen Krankenhausverweildauer vorzunehmen. Sofern das Krankenhaus dieser Verpflichtung nicht nachkomme, müsse die Krankenkasse mittels einer Befristung hierauf reagieren können. Ansonsten könnten Krankenhäuser durch die Angabe unpräziser Behandlungszeiten eine Überprüfung der Verweildauer durch die Krankenkasse im Ergebnis unmöglich machen. Das Verfahren habe sich bewährt; die Anzahl der Befristungen sei – da sich die Krankenhäuser mittlerweile hierauf eingestellt hätten – stetig weniger geworden.

Obwohl der Wortlaut der Vorschrift des § 301 SGB V die Krankenkassen erst bei Überschreitung der vom Krankenhaus mitgeteilten voraussichtlichen Behandlungsdauer zur Anforderung der medizinischen Begründung legitimiert, war angesichts der vorgetragenen Argumente sowie des ansonsten weit gehenden Verzichtes auf medizinische Informationen diese Verfahrensweise der AOK Rheinland-Pfalz aus Sicht des LfD akzeptabel.

11.1.2 Sozialdaten auf dem Parkplatz

Wie zahlreichen Presseberichten und -anfragen auch bei der Behörde des LfD zu entnehmen war, hatte sich vor der Geschäftsstelle einer Krankenkasse ein – um im Sprachgebrauch zu bleiben – „Datenschutzskandal" ereignet. Tausende Arbeitsunfähigkeitsbescheinigungen (AU-Bescheinigungen) von niedergelassenen Ärzten lagen über einen Parkplatz verteilt, so dass die Personalien von Ärzten und Patienten einschließlich Diagnoseangaben, soweit diese nicht nach dem ICD-10-Code verschlüsselt waren, ohne weiteres von Unbefugten zur Kenntnis genommen werden konnten. Die verständigte Polizei stellte die teilweise verschmutzten, zerrissenen und regendurchnässten Unterlagen sicher. Die Recherchen des LfD ergaben zum Hintergrund Folgendes:

Die AU-Bescheinigungen der niedergelassenen Ärzte werden von der Kassenärztlichen Vereinigung gesammelt und an die Krankenkassen verteilt. Die Kassenärztliche Vereinigung stellt die Unterlagen nahezu täglich über einen Paketdienst der Krankenkasse zu. Dieser hat seinerseits einen Subunternehmer beauftragt, dessen Fahrer die Geschäftsstelle der Krankenkasse wegen eines Betriebsausflugs geschlossen vorfand. Daraufhin legte er das Paket im Bereich des Hintereingangs der Geschäftsstelle ab und quittierte sich selbst die Zustellung. Offenbar wurde diese Verfahrensweise zwischen Fahrer und Hausmeister der Geschäftsstelle für den Fall vereinbart, dass diese nicht besetzt ist. Der Hausmeister, so die Vereinbarung, würde das Paket später hereinholen. Spielende Kinder haben dann das Paket aufgerissen und die AU-Bescheinigungen über den Parkplatz und in diverse Briefkästen verteilt.

Zu diesem Vorfall konnte es in allererster Linie aufgrund des Fehlverhaltens des Zustellers kommen. Unabhängig vom Bestehen der o. g. Abrede wäre dieser verpflichtet gewesen, bei Nichtantreffen des Empfängers die Sendung zurück ins Depot zu nehmen. Der Kassenärztlichen Vereinigung war datenschutzrechtlich insoweit überhaupt kein Vorwurf zu machen, der Krankenkasse allenfalls wegen der Absprache ihres Hausmeisters mit dem Paketzusteller.

Der LfD wandte sich gleichwohl an die seiner Kontrollzuständigkeit unterliegenden Krankenkasse und Kassenärztliche Vereinigung mit dem Ziel, einen solchen Vorfall künftig möglichst auszuschließen. Er wies darauf hin, dass Absprachen zwischen dem Hausmeister der Geschäftsstelle und dem Fahrer des Transportunternehmens, die die unbeaufsichtigte Lagerung von Sozialdaten zum Gegenstand haben, künftig zu unterbleiben haben und die Mitarbeiter des Paketdienstes einschließlich die des Subunternehmers nachdrücklich darauf hingewiesen werden sollten, dass bei Nichtantreffen des Empfängers die Unterlagen ordnungsgemäß im Depot zu verwalten sind.

Aufgrund der Nachfrage der Kassenärztlichen Vereinigung teilte das Unternehmen mit, dass man dieses „unglückliche Ereignis" zum Anlass genommen habe, die Fahrer und Unternehmer noch einmal darauf hinzuweisen, dass die Pakete beim richtigen Empfänger gegen eine ordnungsgemäße Quittung abzuliefern sind. Man werde alles tun, um die „gewonnenen Qualitätsstandards" auch künftig unter Beweis zu stellen.

11.1.3 Datenschutz im sozialgerichtlichen Verfahren

Das Sozialgericht Mainz hatte in einem vom LfD zu beurteilenden Fall beim damaligen Versorgungsamt die Schwerbehindertenakte einer Petentin zur Durchführung eines Prozesses, den diese gegen die Berufsgenossenschaft führte, angefordert und erhalten.

Rechtsgrundlage für die Übersendung von Akten durch Sozialleistungsträger an Sozialgerichte ist § 119 Abs. 1 SGG i. V. m. § 35 Abs. 3 SGB I. Danach ist die Behörde zur Aktenübersendung nicht verpflichtet, soweit eine Offenbarung der in den Akten gespeicherten personenbezogenen Daten nach den Übermittlungsvorschriften des SGB X (§ 67 ff.) nicht zulässig ist.

Das LSG Nordrhein-Westfalen hatte in seinem Urteil vom 21. Juli 1982 (Az.: 612-0254-3/87) die unzutreffende Auffassung vertreten, dass § 119 SGG das Rechtsverhältnis der Sozialversicherungsträger als Beteiligte an einem sozialgerichtlichen Verfahren abschließend regele. § 35 SGB I i. V. m. den §§ 67 ff. SGB X – so das LSG – regele nur den Schutz der Sozialdaten im Verwaltungsverfahren der Sozialleistungsträger. Bei der Informationsbeschaffung im sozialgerichtlichen Verfahren würden die §§ 67 ff. SGB X durch die Vorschriften des Sozialgerichtsgesetzes verdrängt. Das Ministerium für Soziales und Familie Rheinland-Pfalz hatte auf eine Anfrage der damaligen Datenschutzkommission hin hierzu eindeutig Stellung genommen und mitgeteilt, dass es die Ansicht des LSG Nordrhein-Westfalen nicht teile.

Ausgehend von der Anwendbarkeit der sozialdatenschutzrechtlichen Vorschriften kommt § 69 Abs. 1 Ziffer 1 2. Alternative SGB X als Übermittlungsgrundlage im vorliegenden Fall nicht in Betracht, da die Übermittlung von Sozialdaten für die Erfüllung einer gesetzlichen Aufgabe des Amtes für soziale Angelegenheiten nicht erforderlich ist. Die Unterstützung von Gerichten kann insoweit nicht als Aufgabe eines Sozialleistungsträgers nach dem Sozialgesetzbuch qualifiziert werden, da es ansonsten der spezialgesetzlichen Regelung in § 69 Abs. 1 Ziff. 2 SGB X, durch die die Tatsachenermittlung in gerichtlichen Streitigkeiten nach dem Sozialgesetzbuch erleichtert und die damit gerade auch im Interesse der Sozialgerichte geschaffen wurde, nicht bedurft hätte.

Für die Übersendung von Akten an Sozialgerichte ist vielmehr § 69 Abs. 1 Ziffer 2 SGB X einschlägig. Hiernach ist eine Übermittlung von Sozialdaten zulässig, soweit sie für die Durchführung eines mit der Erfüllung einer Aufgabe nach Nr. 1 zusammenhängenden gerichtlichen Verfahrens erforderlich ist. Bei Vorliegen dieser Übermittlungsvoraussetzungen steht dem übermittelnden Sozialleistungsträger lediglich eine kursorische Schlüssigkeitsprüfung in Bezug auf die Zulässigkeit der Datenübermittlung zu (vgl. 15. Tb., Tz. 11.2.6).

Fraglich ist jedoch, wann ein solches „Zusammenhangsverfahren" vorliegt. Unproblematisch ist dies dann der Fall, wenn der Sozialleistungsträger selbst Beteiligter des Prozesses ist. Ob eine Datenweitergabe an das Sozialgericht auch dann auf § 69 Abs. 1 Ziff. 2 SGB X gestützt werden kann, wenn die Unterlagen für den Prozess eines anderen Sozialleistungsträgers angefordert werden, wird unterschiedlich beurteilt. Nach einer strengeren Auffassung liegt ein Zusammenhangsverfahren nur dann vor, wenn die Sozialdaten zur Durchführung eines gerichtlichen Verfahrens offenbart werden, die mit der Erfüllung von Aufgaben der offenbarenden Stelle zusammenhängen. Es soll danach also nicht zulässig sein, die bei einem Sozialleistungsträger vorhandenen Sozialdaten zur Durchführung eines Gerichtsverfahrens zu offenbaren, welches mit der Aufgabenerfüllung eines anderen Sozialleistungsträgers zusammenhängt (vgl. Borchert/Haase/Walz, Gemeinschaftskommentar zum SGB, § 69 RdNr. 105; Rasmussen, Sozialdatenschutz in der Praxis, 1997, S. 164). Begründet wird diese Auffassung damit, dass ansonsten über den Umweg des gerichtlichen Verfahrens der Zugriff auf die Gesamtmenge der bei allen Sozialleistungsträgern vorhandenen Daten eröffnet würde, der durch Ziff. 1 gerade nicht ermöglicht werden soll. Auch könne der übermittelnde Leistungsträger kaum beurteilen, ob aus Sicht des anderen Leistungsträgers ein Zusammenhangsverfahren vorliegt.

Der LfD hielt diese Argumentation zwar für beachtlich, erkannte jedoch an, dass im vorliegenden Fall die Berufsgenossenschaft ihrerseits nicht gehindert gewesen wäre, die Schwerbehindertenakte bei der Versorgungsverwaltung gem. § 67 a Abs. 2 SGB X selbst anzufordern, die dann von dieser nach Maßgabe der §§ 69 Abs. 1 3. Alt. und 76 SGB X hätte übermittelt werden können. Über diesen „Umweg" könnten Unterlagen des einen Leistungsträgers letztlich doch in den Prozess des anderen Leistungsträgers eingeführt werden.

Als Kompromiss schlug er deshalb vor, nicht formal darauf abzustellen, ob ein Gerichtsverfahren „eines anderen Sozialleistungsträgers" vorliegt, sondern darauf, ob zwischen dem gerichtlichen Streitgegenstand und den angeforderten Akten ein inhaltlicher Zusammenhang besteht. Ein solcher Zusammenhang kann in Fällen der vorliegenden Art, in denen die Erkrankung der Petentin einerseits Gegenstand eines Rechtsstreits mit der Berufsgenossenschaft und andererseits Gegenstand der Schwerbehindertenakte der Versorgungsverwaltung ist, durchaus angenommen werden. Anders wäre dies jedoch beispielsweise dann zu beurteilen, wenn das Sozialgericht im vorliegenden Fall Akten beim Sozialamt angefordert hätte. Das Sozialministerium schloss sich dem an, da auch nach seiner Auffassung bei dieser Verfahrensweise weder die Ermittlungstätigkeit der Gerichte eingeschränkt wird noch die Sozialleistungsträger mit schwierigen Rechtsfragen in Bezug auf die Übermittlung von Sozialdaten konfrontiert werden.

11.2 Medizinischer Dienst der Krankenversicherung

11.2.1 Die Schere im Kopf – Zweckändernde Datennutzung beim MDK

Eine Petentin wandte sich an den LfD, weil sie eine unzulässige Nutzung ihrer Patientenakte durch den MDK bei einer Einstellungsuntersuchung vermutete. Der Zufall hatte es gewollt, dass sie sich für die erforderliche vertrauensärztliche Untersuchung im Bewerbungsverfahren ausgerechnet bei dem (MDK-)Arzt einzufinden hatte, der sie in einem völlig anderen Zusammenhang, nämlich zur Frage, ob eine Arbeitsunfähigkeit vorlag, untersucht und begutachtet hatte. Aufgrund der negativen Stellungnahme des MDK gegenüber dem künftigen Arbeitgeber kam es nicht zu der erhofften Einstellung. Nahe liegend war, dass die Erkenntnisse, die im Zusammenhang mit der gutachterlichen Stellungnahme zur Arbeitsunfähigkeit gewonnen wurden, auch im Rahmen der Einstellungsuntersuchung zum Tragen kamen.

Datenschutzrechtlich geht es in Fällen dieser Art um die Frage einer zweckändernden Datennutzung durch den MDK. Nach § 275 Abs. 2 Satz 3 SGBV dürfen die rechtmäßig erhobenen und gespeicherten Sozialdaten für andere als die in § 275 SGB V genannten Zwecke nur genutzt werden, wenn dies durch Rechtsvorschriften des Sozialgesetzbuchs angeordnet oder erlaubt ist. Da gesetzliche Bestimmungen zur Nutzungsänderung für die hier in Rede stehende Fallkonstellation nicht existieren, wäre die Verwendung der vorhandenen Informationen für andere Zwecke als unzulässig zu bewerten.

Der MDK stritt eine zweckändernde Datennutzung ab und wies darauf hin, dass die Stellungnahme gegenüber dem potentiellen Arbeitgeber ausschließlich auf eigenen Mitteilungen der Petentin beruht habe; eine Einsichtnahme der Patientenakte habe nicht stattgefunden.

Gleichwohl hätte es im vorliegenden Fall wohl der sprichwörtlichen „Schere im Kopf" bedurft, um ein Ineinandergreifen beider Sachverhalte gänzlich auszuschließen. Der MDK sicherte angesichts dessen zu, künftig vertrauensärztliche Untersuchungen – ohne Hinzuziehen einer evtl. vorhandenen MDK-Akte – von einem anderen Arzt als dem, der in anderer Sache mit dem Patienten bereits befasst war, vornehmen zu lassen.

11.2.2 MDK-Gutachten als „unrichtiges Sozialdatum" im Sinne des § 84 Abs. 1 SGB X?

Nach § 84 Abs. 1 SGB X sind Sozialdaten zu berichtigen, wenn sie unrichtig sind. Wird die Richtigkeit von Sozialdaten von dem Betroffenen bestritten und lässt sich weder die Richtigkeit noch die Unrichtigkeit der Daten feststellen, bewirkt dies keine Sperrung, soweit es um die Erfüllung sozialer Aufgaben geht; die ungeklärte Sachlage ist in geeigneter Weise festzuhalten. Die bestrittenen Daten dürfen nur mit einem Hinweis hierauf genutzt und übermittelt werden.

Im Berichtszeitraum häuften sich die Fälle, in denen ein ärztliches Gutachten des MDK, auf das sich die Krankenkasse bei einer für den Versicherten nachteiligen Entscheidung stützte, von diesem als ein „unrichtiges Sozialdatum" qualifiziert wurde. Die Betroffenen erwarteten, dass das Gutachten zu sperren, aus den Akten zu entfernen und mit einem Verwertungsverbot zu belegen sei.

Der LfD ist der Auffassung, dass derartige Ansprüche nicht bestehen, da ein ärztliches Gutachten grundsätzlich nicht als ein „unrichtiges Sozialdatum" i. S. d. § 84 Abs. 1 SGB X qualifiziert werden kann. Eine datenschutzrechtliche Prüfung hat nämlich zu berücksichtigen, dass dem Betroffenen gegen ein seiner Auffassung nach unzutreffendes MDK-Gutachten keine Rechtsmittel zur Verfügung stehen. Grund hierfür ist die mangelnde Außenwirkung des Gutachtens, das der Krankenkasse lediglich als Entscheidungshilfe im Rahmen des von ihr betriebenen Verwaltungsverfahrens dient. Das Gutachten kann daher nur im Rahmen des Widerspruchs- und Klageverfahrens inzidenter überprüft werden. Würde das streitige Gutachten vernichtet, würde das vom Gesetzgeber vorgesehene Verfahren damit nicht nur konterkariert, sondern sogar unmöglich gemacht. Im Ergebnis würde dies eine nicht mehr zu akzeptierende Instrumentalisierung des Datenschutzes bedeuten. Nichts anderes gilt für ein Gutachten, das von einem angeblich befangenen oder inkompetenten MDK-Gutachter erstellt wurde.

Die inhaltliche Richtigkeit von MDK-Gutachten kann daher grundsätzlich nicht mit den Mitteln des Datenschutzes überprüft werden. Etwas anderes kommt lediglich in den Fällen in Betracht, in denen bei der Gutachtenerstellung erkennbar von falschen Tatsachen ausgegangen worden ist oder der Inhalt des Gutachtens auch für den medizinischen Laien – beispielsweise aufgrund in sich widersprüchlicher Aussagen – nicht nachvollziehbar ist. Der LfD sieht seine Rechtsauffassung durch eine Entscheidung des LG Aachen (NJW 1999, 2746) bestätigt, wonach einem Patienten grundsätzlich kein Anspruch auf Korrektur eines Arztbriefes in Bezug auf Diagnosen und Schussfolgerungen zuzubilligen ist.

11.3 Dialogverfahren der Rentenversicherungsträger

Im 16. Tb. (Tz. 11.3) und im 17. Tb. (Tz. 11.6) wurde über das bundesweite Abrufverfahren und die Widerspruchsmöglichkeit der Versicherten gegen die automatisierte Datenübermittlung berichtet. Datenschutzrechtlich unbefriedigend war, dass die Versicherten von der LVA Rheinland-Pfalz über diese Widerspruchsmöglichkeit nicht unterrichtet wurden. Die LVA befand sich damit zwar in guter Gesellschaft, da sich auch andere Rentenversicherungsträger hierzu nicht veranlasst sahen; entbehrlich wurde die Unterrichtung jedoch damit nicht. Der LfD machte gegenüber der LVA Rheinland-Pfalz vielmehr deutlich, dass ein Widerspruchsrecht, über das der Betroffene nicht informiert ist, ins Leere läuft. Die Ausübung des Widerspruchsrechts setzt daher zwingend eine Unterrichtung voraus. Örtliche Feststellungen bei der LVA Rheinland-Pfalz zeigten, dass kein einziges Widerspruchsmerkmal in den 3,8 Millionen Datensätzen der LVA eingetragen ist. Es widerspricht aber jeglicher Lebenserfahrung, dass dieses Recht von keinem Versicherten wahrgenommen wird, wenn eine angemessene Unterrichtung erfolgt. Während der gesamten Befassung mit der Thematik sind dem LfD keine Argumente vorgetragen worden, die gegen eine Unterrichtung der Versicherten, etwa im Rahmen des Internet-Angebots der LVA, sprechen würden. Durch eine nicht nachvollziehbare Weigerung der Rentenversicherungsträger könnte indes leicht der Eindruck entstehen, dass ein bundesweites Abrufverfahren implementiert werden soll, welches sich bewusst auf die Unkenntnis der Versicherten bezüglich ihrer Widerspruchsrechte stützt. Nach langwierigen Erörterungen fand sich die LVA Rheinland-Pfalz schließlich doch bereit, auf ihrer Internet-Seite einen entsprechenden Hinweis aufzunehmen.

11.4 Outsourcing im Bereich des Landesamtes für Soziales, Jugend und Versorgung

Wie einer öffentlichen Auslobung im Deutschen Ärzteblatt zu entnehmen war, beabsichtigte das Landesamt für Soziales, Jugend und Versorgung, den Auftrag für ärztliche Stellungnahmen und Gutachten zur Beurteilung der Schwerbehinderteneigenschaft und anderer Feststellungsmerkmale nach dem Schwerbehindertengesetz zentral an „Personen, Personengesellschaften oder Institutionen" zu vergeben. Das Landesamt verfolgte damit das Ziel, von der Vielzahl der Einzelvereinbarungen mit externen Ärzten Abstand zu nehmen und die Qualität der gutachterlichen Stellungnahmen sowie die Wirtschaftlichkeit des Verfahrens insgesamt zu verbessern. Es war davon auszugehen, dass als Auftragnehmer nur nichtöffentliche Stellen in Betracht kamen, denen gegenüber nur eingeschränkte Einwirkungsmöglichkeiten der Datenschutzkontrollbehörden bestehen. Angesichts eines Auftragsvolumens von ca. 80 000 Gutachten/Stellungnahmen pro Jahr war darüber hinaus zu befürchten, dass es beim Auftragnehmer zu einer datenschutzrechtlich bedenklichen medizinischen Zentraldatei kommt.

Dadurch, dass sich der LfD frühzeitig in das Verfahren einschaltete, konnte bereits die Ausschreibung elementaren datenschutzrechtlichen Anforderungen Rechnung tragen, was sich auch beim Abschluss des Vertrages mit dem Auftragnehmer fortsetzte. So steht dem Antragsteller gegen die Einschaltung der externen Gutachterstelle ein Widerspruchsrecht zu, auf das er zu Beginn des Verfahrens vom Landesamt ausdrücklich hingewiesen wird. Beim Auftragnehmer dürfen nach Gutachtenerstellung personenbezogene Patientendaten nur im Hinblick auf evtl. Rückfragen für eine Dauer von höchstens sechs Monaten vorgehalten werden. Eine Übernahme von Patientendaten in eigene Datenbestände (z. B. für Schulungszwecke) ist nur in anonymisierter Form zulässig.

Ob es sich bei der Erstellung von Gutachten durch eine externe Stelle um eine Auftragsdatenverarbeitung im Sinne des § 80 SGB X handelt, welche auf Seiten des Auftragnehmers in aller Regel lediglich eine technische Erfüllungshilfe – ohne eigenen Gestaltungsspielraum – voraussetzt, oder ob von einer Funktionsübertragung im Sinne des § 97 SGB X auszugehen ist, konnte dahinstehen, da im Ergebnis identische datenschutzrechtliche Anforderungen bestehen. Hierzu zählt in erster Linie der Abschluss eines Vertrages, der neben den o. g. Punkten auch die Zulässigkeit von Unterauftragsverhältnissen, die Zuständigkeit der Datenschutzkontrollbehörde und Maßnahmen des technisch-organisatorischen Datenschutzes zu regeln hat. Diesen gesetzlichen Anforderungen wurde im vorliegendem Fall Rechnung getragen. Das Outsourcing-Projekt des Landesamtes brachte im Ergebnis für die Betroffenen daher keine datenschutzrechtlichen Verschlechterungen.

11.5 Jugendhilfe

11.5.1 Datenschutz im Zusammenhang mit Leistungen nach dem Unterhaltsvorschussgesetz

Nachdem eine Kreisverwaltung Leistungen nach dem Unterhaltsvorschussgesetz erbracht hatte, forderte sie diese nunmehr vom Betroffenen zurück. Dieser wandte sich an den LfD, weil er über seine Einkommensverhältnisse nicht detailliert Auskunft geben wollte. Insbesondere sah er als Gewerbetreibender nicht ein, seine Einkommensteuerbescheide vorzulegen und über die Vermögensverhältnisse seiner Lebenspartnerin Auskunft zu geben.

Der LfD wies ihn zunächst darauf hin, dass § 6 Abs. 1 UVG für den säumigen Unterhaltsschuldner die Verpflichtung begründet, über alle persönlichen und sachlichen Angelegenheiten im erforderlichen Umfang Auskunft zu erteilen. Neben dieser öffentlichrechtlichen Informationspflicht besteht der allgemeine zivilrechtliche Auskunftsanspruch des Kindes gegen seinen unterhaltspflichtigen Elternteil nach § 1605 BGB, welcher gem. § 7 Abs. 1 UVG zusammen mit dem Hauptanspruch auf Unterhalt auf den Staat, hier also die Kreisverwaltung, übergeht.

Der Umfang der Auskunftspflicht nach § 1605 BGB ist durch die Rechtsprechung näher konkretisiert worden. Bei selbständig tätigen Unterhaltsschuldnern genügt hiernach nicht die ziffermäßige Aneinanderreihung von Einnahmen und einzelnen Kostenarten. Der Unterhaltsschuldner muss vielmehr durch Aufschlüsselung von Einnahmen und Ausgaben seine Einkommens- und Vermögensverhältnisse über einen längeren Zeitraum (in der Regel drei Jahre) innerhalb von sechs Monaten nach Ablauf des Geschäftsjahres offen legen. Dass von einem Gewerbetreibenden die Vorlage der Einkommensteuerbescheide verlangt werden kann, ist in diesem Zusammenhang höchstrichterlich anerkannt.

Was das Verlangen der Kreisverwaltung, auch die Vermögensverhältnisse der Lebenspartnerin offen zu legen, angeht, ergab eine Nachfrage bei der Kreisverwaltung, dass der Petent einen Stundungsantrag gestellt hatte und in diesem Zusammenhang auch die Einkommens- und Vermögensverhältnisse des Lebenspartners formularmäßig abgefragt wurden. Der LfD bewertete dies wie folgt:

Da übergegangene Ansprüche nach dem Unterhaltsvorschussgesetz rechtzeitig und vollständig nach den Bestimmungen des Haushaltsrechts durchzusetzen sind (§ 7 Abs. 3 UVG), kommen insoweit die Vorschriften der Gemeindehaushaltsverordnung zur Anwendung. Hiernach dürfen Ansprüche teilweise oder ganz gestundet werden, wenn ihre Einziehung bei Fälligkeit eine erhebliche Härte für den Schuldner bedeuten würde und der Anspruch durch die Stundung nicht gefährdet erscheint (§ 32 Abs. 1 GemHVO).

Eine erhebliche Härte kann insbesondere dann vorliegen, wenn sich der Schuldner in ungünstigen wirtschaftlichen Verhältnissen befindet. Er ist insoweit darlegungspflichtig, d. h. er hat Unterlagen über seine finanzielle Situation vorzulegen, damit die Verwaltung die Voraussetzungen des Anspruchs prüfen kann.

Sofern der Antragsteller – wie dies hier der Fall war – unvollständige bzw. unplausible Angaben macht, ist der Leistungsträger nicht nur berechtigt, sondern auch verpflichtet, die noch fehlenden Unterlagen beim Betroffenen anzufordern, da andernfalls der Stundungsantrag abgelehnt werden muss.

Soweit in dem betroffenen Formular auch Einkommens- und Vermögensverhältnisse des Ehegatten bzw. Lebenspartners erfragt wurden, war darauf hinzuweisen, dass auch bei der Beantragung von Sozialhilfe im Rahmen der Bedürftigkeitsprüfung das Vermögen des Ehe- bzw. Lebenspartners mit heranzuziehen ist. Nichts anderes kann aber bei der Beantragung von Billigkeitsmaßnahmen (Stundung, Erlass) gelten. Da Personen, die in eheähnlicher Gemeinschaft leben, nicht besser gestellt werden dürfen als Ehegatten (vgl. § 122 BSHG), hängt die Auskunftspflicht auch nicht davon ab, ob die Lebenspartner verheiratet sind oder nicht. Aus diesem Grunde war das von der Kreisverwaltung eingesetzte Formular datenschutzrechtlich nicht zu beanstanden.

11.5.2 Informationsaustausch zwischen Jugendamt und Sozialamt

Eine Sozialarbeiterin des Stadtjugendamtes betreute im Rahmen der sozialpädagogischen Familienhilfe eine Frau mit Kind. Im Rahmen ihrer Betreuungsaufgaben wurde der Sozialarbeiterin bekannt, dass die Frau auch Hilfe zum Lebensunterhalt durch das Sozialamt der Stadtverwaltung bezog und in der Zwischenzeit mit ihrem Lebenspartner in einer anderen Wohnung lebte. Trotz mehrfacher Aufforderungen weigerte sich die Frau allerdings, das Sozialamt über die Veränderungen zu unterrichten. Das Jugendamt wandte sich an den LfD mit der Frage, ob die Mitarbeiterin des Jugendamtes das Sozialamt über die neuen Gegebenheiten unterrichten darf.

Datenschutzrechtlich geht es dabei um die Frage, ob die Information über das Zusammenleben aus dem Betreuungsverfahren auch für Sozialhilfezwecke verwendet und das Sozialamt entsprechend unterrichtet werden darf. Datenschutzrechtlich handelte es sich mithin um eine zweckändernde Datennutzung und eine Datenübermittlung an das Sozialamt. Wegen § 67 Abs. 9 Satz 3 SGB X gelten dabei Jugendamt und Sozialamt jeweils als eigene „speichernde Stelle“ innerhalb der Stadtverwaltung.

Gem. 67 c Abs. 2 SGB X dürfen Sozialdaten von derselben Stelle für andere Zwecke u. a. dann genutzt werden, wenn die Daten für die Erfüllung von Aufgaben nach anderen Rechtsvorschriften des Sozialgesetzbuchs als diejenigen, für die sie erhoben wurden, erforderlich sind (Ziff. 1). Auch die Zulässigkeit der Datenübermittlung hängt von der Erforderlichkeit der Aufgabenerfüllung für andere SGB-Zwecke ab: Nach § 64 Abs. 2 SGB VIII i. V. m. § 69 Abs. 1 Ziffer 1 SGB X ist die Übermittlung von Sozialdaten u. a. dann zulässig, soweit sie für die Erfüllung einer gesetzlichen Aufgabe des Empfängers nach dem Sozialgesetzbuch erforderlich ist, wenn diese eine in § 35 SGB I genannte Stelle ist (3. Alt.).

Im Wesentlichen liegen daher für die zweckändernde Datennutzung und Übermittlung identische Voraussetzungen vor. Diese waren hier erfüllt, da sich das Vorliegen einer eheähnlichen Lebensgemeinschaft unmittelbar auf den Anspruch auf Hilfe zum Lebensunterhalt auswirken kann (vgl. §§ 122, 16, 11 BSHG) und die Bekämpfung von Leistungsmissbräuchen zu den Aufgaben eines Sozialleistungsträgers (hier des Sozialamtes) nach dem Sozialgesetzbuch zu zählen ist. Die Übermittlung von Sozialdaten wäre allerdings dann unzulässig, wenn hierdurch der Erfolg einer Jugendhilfeleistung, für welche die Daten erhoben worden sind, in Frage gestellt würde (§ 64 Abs. 2 SGB VIII). Dies war jedoch im vorliegenden Fall nicht ersichtlich.

Datenübermittlungen, bei denen kein Ersuchen des Empfängers vorliegt (sog. Spontanauskünfte), werden allerdings z. T. als nicht unproblematisch angesehen. So sollen Auskünfte aus freien Stücken nur dann zulässig sein, wenn ein enger Zusammenhang mit den zu erfüllenden Aufgaben der jeweiligen Stellen besteht (KassKomm-Scholz, § 69 SGB X RdNr. 7). Unabhängig davon, ob man sich dieser restriktiven Sichtweise, die aus dem Wortlaut der Übermittlungsbestimmungen des SGB X nicht abzuleiten ist, anschließt oder nicht, kann der geforderte Zusammenhang bei der vorliegenden Fallkonstellation unterstellt werden.

Die Mitarbeiterin des Jugendamtes war damit datenschutzrechtlich nicht gehindert, dem Sozialamt mitzuteilen, dass die von ihr betreute Frau umgezogen ist und in einer nichtehelichen Lebensgemeinschaft wohnt.

11.5.3 Einsicht in Adoptionsunterlagen

Eine Stadtverwaltung bat um Beantwortung der Frage, ob jemandem, der als Kind adoptiert wurde, vom Jugendamt Akteneinsicht in die Adoptionsunterlagen gewährt werden darf. Die Frau wollte so an nähere Informationen über ihre im Ausland lebenden leiblichen Verwandten (Großeltern und Bruder) gelangen und ggf. mit diesen in Kontakt treten.

Unabhängig vom Akteneinsichtsrecht nach § 25 SGB X für Beteiligte eines Verwaltungsverfahrens, dessen Voraussetzungen im konkreten Fall nicht vorlagen, hat der Betroffene gem. § 67 SGB VIII i. V. m. § 83 SGB X einen Anspruch auf Auskunft über die zu seiner Person gespeicherten Daten. Dieses Recht besteht jedoch nicht uneingeschränkt. Insbesondere dann, wenn personenbezogene Daten wegen überwiegender berechtigter Interessen dritter Personen geheim gehalten werden müssen, kommt eine Auskunftserteilung nicht in Betracht (§ 83 Abs. 4 SGB X).

Überwiegende schutzwürdige Interessen der Großeltern bzw. des Bruders der Betroffenen waren hier nicht ersichtlich. Angaben über leibliche Verwandte werden vom Offenbarungs- und Ausforschungsverbot bei Adoptionen (vgl. § 1758 BGB) nicht umfasst.

Wie § 61 Abs. 2 PStG zeigt, hat der Gesetzgeber vielmehr das Recht einer adoptierten Person auf Kenntnis der eigenen Abstammung ab dem 16. Lebensjahr grundsätzlich anerkannt. Eine besondere Schutzbedürftigkeit der von der Auskunftserteilung Betroffenen liegt somit nicht vor.

In der rechtlichen Beurteilung war ferner zu berücksichtigen, dass das Jugendamt über keine Erkenntnisse darüber verfügte, dass die Angehörigen des Betroffenen mit einer Auskunftserteilung nicht einverstanden waren. Selbst wenn man einen entgegenstehenden Willen der Angehörigen unterstellte, ergibt eine Abwägung der beiderseitigen Interessen, dass die Interessen des Betroffenen, Informationen über seine leiblichen Verwandten zu erhalten, gegenüber den (möglichen) Interessen jener, für den Betroffenen anonym zu bleiben, als höherwertig einzustufen sind.

Die Form der Auskunftserteilung bestimmt die speichernde Stelle, also das Jugendamt, nach pflichtgemäßem Ermessen. Dem Auskunftsanspruch kann daher auch durch die Gewährung von Akteneinsicht entsprochen werden.

11.6 Sozialhilfe

11.6.1 Arbeit statt Sozialhilfe

Bei ihren Bemühungen, Sozialhilfeempfänger in den Arbeitsmarkt zu integrieren, machen sich Kreise und Gemeinden verstärkt die Vorteile der automatisierten Datenverarbeitung und moderner Kommunikationsmöglichkeiten zu Nutze. Neben den im 16. Tb. (Tz. 11.5.5) geschilderten Datenschutzfragen waren im Berichtszeitraum Aspekte zu beurteilen, die mit dem Einsatz neuer Datenverarbeitungstechniken verbunden sind.

Eine Kreisverwaltung beabsichtigte in Zusammenarbeit mit verschiedenen Verbandsgemeinden, Arbeitsämtern und kommunalen Beschäftigungsgesellschaften den Einsatz einer spezifischen Software, die eine „passgenaue“ Vermittlung in den Arbeitsmarkt ermöglichen soll. Auf Knopfdruck kann der Lebenslauf mit Lichtbild des Betroffenen samt Bewerbungsschreiben ausgedruckt werden. Die hierfür benötigten Informationen werden teilweise aus dem Sozialhilfeverfahren „Prosoz“ übernommen. Weitere für die Vermittlung erforderliche Daten werden durch Befragung des Hilfeempfängers gewonnen. Der Betroffene soll in Fragebogen dabei z. T. sensible Angaben, etwa zu seiner Gesundheit, zum Bestehen einer Schwangerschaft, zu Vorstrafen, Suchtproblemen und Schulden machen. Neben Selbsteinschätzungen (z. B. „antriebsarm“, „blockiert“, „normal“, „engagiert“) werden auch Bewertungen des Sachbearbeiters über die Arbeitsfähigkeit, soziale Integration, Motivation, äußeres Erscheinungsbild und Konfliktfähigkeit des Hilfeempfängers aufgenommen.

Da es sich bei dem Verfahren um ein vom Bundesministerium für Arbeit und Sozialordnung gefördertes Modellprojekt zur Verbesserung der Zusammenarbeit zwischen Arbeitsämtern und Trägern der Sozialhilfe handelt, welches der Öffentlichkeit unter dem Begriff „MoZArT“ vorgestellt wurde, beurteilt sich die Zulässigkeit der Datenerhebung und -verarbeitung der beteiligten Leistungsträger nach § 18 a Abs. 3 BSHG, § 421 d Abs. 3 SGB III i. V. m. §§ 67 ff. SGB X.

Bei der Datenerhebung stellte sich die für das Verfahren nicht ganz unwesentliche Frage, inwieweit von einer Mitwirkungspflicht des Betroffenen am Modellprojekt auszugehen ist. Wenn Daten beim Betroffenen aufgrund einer Rechtsvorschrift erhoben werden, die zur Auskunft verpflichtet, ist er nämlich gem. § 67 a Abs. 3 SGB X auf diese Vorschrift sowie auf die Folgen der Verweigerung, sonst auf die Freiwilligkeit seiner Angaben hinzuweisen.

Der LfD ging von folgenden Überlegungen aus: Nach §§ 1 Abs. 2, 18 Abs. 1 BSHG hat der Hilfeempfänger auch seine Arbeitskraft zur Beschaffung des Lebensunterhaltes für sich und seine Angehörigen einzusetzen. Weigert er sich, eine zumutbare Arbeit zu leisten, wozu auch das vorwerfbare Unterlassen von Bemühungen um eine Arbeit zu zählen ist, verliert er den Anspruch auf Hilfe zum Lebensunterhalt (§ 25 BSHG). Waren die eigenen Bemühungen des Hilfeempfängers, Arbeit zu finden, erfolglos, ist er zur Teilnahme an Projekten der vorliegenden Art grundsätzlich verpflichtet.

Bei der Befragung des Betroffenen war allerdings nach Auffassung des LfD angesichts der Sensibilität der Daten nicht von einer uneingeschränkten Mitwirkungs- bzw. Offenbarungsverpflichtung auszugehen. Als freiwillig waren insbesondere die Fragen zum Vorliegen sog. Vermittlungshemmnisse zu kennzeichnen, welche auch im Rahmen eines „normalen“ Bewerbungsverfahrens vom künftigen Arbeitgeber nicht erfragt werden dürfen (z. B. Bestehen einer Schwangerschaft). Gleiches galt für die Verarbeitung eines digitalen Lichtbildes sowie für die Selbsteinschätzungen des Betroffenen.

Da die Software es ermöglichte, den Datenbestand beispielsweise nach sämtlichen vorbestraften Alkoholikern auch auf Sachbearbeiterebene auszuwerten, bestand eine weitere datenschutzrechtliche Forderung in der systemtechnisch unterstützten Begrenzung der Auswertungsmöglichkeiten sowie deren Protokollierung und Durchsicht durch den behördlichen Datenschutzbeauftragten.

Die Beteiligung verschiedener Stellen am Modellprojekt erforderte die Erarbeitung eines genauen Zugriffskonzeptes, aus dem ersichtlich wurde, welche Stelle auf welche Daten im Rahmen ihrer jeweiligen Aufgabenerfüllung zwingend zugreifen muss. So erhält beispielsweise die Kreisverwaltung für Zwecke der Arbeitsmarktkoordination lediglich anonymisierte Datensätze. Die im Rahmen des Sozial-Controllings von den Sozialämtern gespeicherten Angaben sowie Freitextangaben im Zusammenhang mit Beratungsterminen werden nur lokal vorgehalten bzw. stehen anderen Nutzern nicht zur Verfügung.

Eine datenschutzrechtliche Begleitung des Projektes erfolgte darüber hinaus in Fragen der Verschlüsselung bei der Nutzung öffentlicher Kommunikationswege sowie der Löschung und Archivierung der verarbeiteten Sozialdaten. Die frühzeitige Beteiligung des LfD gewährleistete damit eine insgesamt datenschutzverträgliche Ausgestaltung des Modellprojekts.

11.6.2 *Ermittlungstätigkeiten der Sozialhilfeträger*

Die Mitarbeiter von Sozialhilfeträgern stehen bei der Antragstellung auf Sozialhilfe häufig vor der Frage, ob und inwieweit Angaben des Betroffenen bei dritten Personen oder Stellen überprüft werden dürfen. Da eine Datenerhebung bei Dritten regelmäßig mit der Offenbarung von geschützten Sozialdaten verbunden ist, kommt sie nur dann in Betracht, wenn andere, weniger belastende Maßnahmen zur Sachverhaltsaufklärung nicht möglich sind (vgl. § 67 a Abs. 2 Ziff. 2 SGB X). Diese gesetzlich vorgeschriebene Erforderlichkeitsprüfung findet häufig nicht sorgfältig genug statt, so dass sich Sozialhilfeempfänger gegenüber Personen ihres persönlichen Umfeldes urplötzlich als solche „geoutet" sehen und sich hierüber beim LfD zu Recht beklagen.

In einem Fall nahm ein Mitarbeiter eines Sozialamtes nach der Beantragung einer einmaligen Beihilfe für einen Kassettenrecorder – ohne mit der Betroffenen Rücksprache zu halten – mit dem Hochschulprofessor der Antragstellerin Kontakt auf, der bestätigen sollte, dass das Gerät für das Studium auch tatsächlich erforderlich war. In einem anderen Fall telefonierte der Sozialamtsmitarbeiter ohne die im Grundsatz erforderliche schriftliche Einwilligung der Eltern einzuholen, mit der Klassenlehrerin des Sohnes, um die näheren Modalitäten eines Zuschusses zur Klassenfahrt zu regeln, was sodann prompt zu einem Streit darüber führte, ob das Telefonat abgesprochen war oder nicht.

Die Grundsätze der Erforderlichkeit und Verhältnismäßigkeit sind insbesondere auch beim Einsatz sog. Sozialhilfeermittler (s. 17. Tb., Tz. 11.2.6.3) zu beachten. Dies gilt in besonderem Maße, wenn es um die Überprüfung geht, ob ein Hilfeempfänger in einer eheähnlichen Gemeinschaft lebt. Eine Stadtverwaltung teilte hierzu in völliger Verkennung der Vorschriften über den Sozialdatenschutz mit, dass „der rechtmäßige Einsatz von Sozialhilfezahlungen oberstes Ziel bei einer Güterabwägung sei und die datenschutzrechtlichen Interessen der Sozialhilfeempfängerin demgegenüber in den Hintergrund zu treten hätten". In einem weiteren Fall observierten Außendienstmitarbeiter einer Stadtverwaltung über mehrere Monate die Wohnung einer Hilfeempfängerin, um festzustellen, ob der potenzielle Lebenspartner dort übernachtet. Um die Beobachtungen zu erleichtern, wurde bei der Zulassungsstelle angefragt, welche Kraftfahrzeuge auf diese Person, die ihrerseits Sozialleistungen weder beantragt hatte noch erhielt, zugelassen sind. Eine schriftliche Befragung der Betroffenen fand als mildere Maßnahme ebenso wenig statt, wie eine unangemeldete Wohnungsbesichtigung. Der LfD beanstandete die Ermittlungsmethoden der Stadtverwaltung als Verstoß gegen datenschutzrechtliche Vorschriften.

11.6.3 Vorlage von Kontoauszügen und Befreiung vom Bankgeheimnis

Im Berichtszeitraum waren erneut zahlreiche Stellungnahmen zu der Frage abzugeben, ob und inwieweit ein Sozialamt zum einen die Vorlage von Kontoauszügen und zum anderen die Befreiung vom Bankgeheimnis verlangen kann.

Die Anforderung von Kontoauszügen der letzten drei bis sechs Monate ist beim Erstantrag auf Sozialhilfe von den Mitwirkungspflichten des Antragstellers (§§ 60 ff. SGB I) gedeckt. Der Sozialleistungsträger hat im Rahmen des Amtsermittlungsgrundsatzes (§ 20 SGB X) die Voraussetzungen für die Gewährung des Anspruchs auf Sozialhilfe zu prüfen. Das Nichtvorhandensein ausreichender eigener Mittel ist gem. § 11 Abs. 1 BSHG wesentliches Tatbestandsmerkmal für den Anspruch auf Hilfe zum Lebensunterhalt. Nach § 60 Abs. 1 Nr. 1 SGB I hat, wer Sozialleistungen beantragt oder erhält, alle Tatsachen anzugeben, die für die Leistung erheblich sind, und auf Verlangen des zuständigen Leistungsträgers der Erteilung der erforderlichen Auskünfte durch Dritte zuzustimmen. Nr. 3 der zitierten Vorschrift verpflichtet die Betroffenen, Beweismittel zu bezeichnen und auf Verlangen Beweisurkunden – also beispielsweise Kontoauszüge oder Sparbücher – vorzulegen.
Bei diesem Verfahren ist jedoch zu beachten, dass eine Speicherung der Auszüge in den Akten in aller Regel nicht erforderlich ist. Es dürfte ausreichend sein, wenn die Vorlage der Kontoauszüge in der Sozialhilfeakte vermerkt wird. Nur wenn hierbei sozialhilferechtlich relevante Daten ermittelt werden, sind die betreffenden Kontoauszüge zu kopieren und zur Leistungsakte zu nehmen.

Dem Antragsteller ist bei der Vorlage von Kontoauszügen jedoch die Möglichkeit zu gestatten, den Verwendungszweck einzelner Kleinstbeträge (beispielsweise Mitgliedschaftsbeiträge für politische Parteien) zu schwärzen.

Nach der Rechtsprechung des Hess. VGH (Beschluss vom 7. Februar 1995, DVBl. 1995, S. 702 f.) ist das routinemäßige Verlangen, der Einholung von Bankauskünften zuzustimmen, eine überflüssige und somit nicht erforderliche Ermittlungstätigkeit. Nur wenn die Richtigkeit von Angaben im konkreten Fall bezweifelt wird, bestehen gegen die Befreiung vom Bankgeheimnis keine Bedenken. Dies bedeutet, dass auch beim Einsatz von Formularen die Befreiung vom Bankgeheimnis nicht routinemäßig erfolgen darf (17. Tb., Tz. 11.2.5).

Hinzuweisen ist auch darauf, dass sich Sozialämter durch den Erwerb bestimmter Formulare bei Verlagen nicht von ihren datenschutzrechtlichen Verpflichtungen „freikaufen" können. In einem Vordruck, der im Zusammenhang mit der Befreiung vom Bankgeheimnis zum Einsatz kam, wurde für den Betroffenen in keiner Weise deutlich, ob und ggf. welches Kreditinstitut ermächtigt werden soll, Bankauskünfte an das Sozialamt zu erteilen. Statt einer Unterschrift des Betroffenen sollte die des Sachbearbeiters genügen. Das Sozialamt sah sich nicht veranlasst, an dem Formular etwas zu ändern, da der Verlag dessen Ordnungsgemäßheit auf Rückfrage bestätigt habe.

Der LfD machte deutlich, dass das Sozialamt als „speichernde Stelle“ i. S. d. § 67 Abs. 9 SGB X für die Einhaltung der datenschutzrechtlichen Vorschriften verantwortlich ist und die Auffassung eines Verlages in diesem Zusammenhang keine Rolle spielt. Auch wies er darauf hin, dass nach § 60 Abs. 1 Ziffer 1 SGB I zwar derjenige, der Sozialleistungen beantragt, u. a. auch der Erteilung der erforderlichen Auskünfte durch Dritte zuzustimmen hat. An diese Zustimmungserklärung sind jedoch inhaltlich keine im Wesentlichen anderen Anforderungen zu stellen, als dies bei einer wirksamen Einwilligungserklärung im Sinne des § 67 b Abs. 2 SGB X der Fall ist. Um dem Antragsteller Klarheit zu verschaffen, in welchen Punkten durch Auskünfte an die Leistungsträger in seine Geheimhaltungssphäre eingegriffen wird, darf das Zustimmungsverlangen des Leistungsträgers nicht pauschal ausgedrückt, sondern muss nach der Person des Dritten und nach dem Inhalt der von diesem einzuholenden Auskünfte so konkret wie möglich gefasst sein (Hauck/Haines, Kommentar zum SGB I, § 60 RdNr. 13). Dem Betroffenen ist insoweit zu verdeutlichen, dass und in welchem Umfang durch seine Erklärung überhaupt eine Befreiung vom Bankgeheimnis erfolgt. Genügt eine Erklärung diesen Anforderungen nicht, sind hierauf gestützte Datenübermittlungen der Kreditinstitute rechtswidrig.

Es bedurfte intensiver Überzeugungsarbeit des LfD, bis eine datenschutzgerechte Überarbeitung des Formulars erreicht war.

12. Datenschutz im Ausländerwesen

12.1 Entwurf eines Gesetzes zur Steuerung und Begrenzung der Zuwanderung und zur Regelung des Aufenthalts und der Integration von Unionsbürgern und Ausländern (Zuwanderungsgesetz)

Auf der Ebene des Bundes wird eine umfassende Neuregelung der Zuwanderung von Ausländern und damit des gesamten Ausländerrechts erörtert. In diesem Zusammenhang wurde der LfD zur Stellungnahme zu den datenschutzrechtlichen Aspekten aufgefordert. Er äußerte sich wie folgt:

Von datenschutzrechtlicher Bedeutung ist insbesondere der Abschnitt 4 (Datenübermittlung und Datenschutz) des Aufenthaltsgesetz-Entwurfs (Gesetz über den Aufenthalt, die Erwerbstätigkeit und die Integration von Ausländern im Bundesgebiet, Art. 1 des Zuwanderungsgesetzes).

§ 84 des Aufenthaltsgesetz-Entwurfs, der die Erhebung personenbezogener Daten regeln soll, ist aus der Sicht des Datenschutzes missverständlich formuliert. Satz 1 schreibt den bereits herkömmlich geltenden Erforderlichkeitsgrundsatz fest. Dagegen ist nichts einzuwenden. Satz 2 allerdings regelt für besonders schutzwürdige Daten (dies sind die Daten im Sinne von § 3 Abs. 9 BDSG), dass diese nur dann erhoben werden dürfen, „soweit dies im Einzelfall zur Aufgabenerfüllung erforderlich ist.“ Damit wird ein Gegensatz zwischen Satz 1 und Satz 2 hergestellt. Daraus ließe sich folgern, dass der Erforderlichkeitsgrundsatz in Satz 1 gerade nicht bedeutet, dass die entsprechenden Daten im Einzelfall zur Aufgabenerfüllung erforderlich sein müssen, dass dies vielmehr eine hinzukommende erschwerende Voraussetzung für die Erhebung von besonders schutzwürdigen Daten sei. Damit wird der Erforderlichkeitsgrundsatz des Satzes 1 stark abgeschwächt. Dies ist – der Gesetzesbegründung zufolge – nicht gewollt. Es wäre auch nicht sachgerecht. Hier muss eine andere Formulierung gefunden werden.

In § 88 Abs. 1 des Aufenthaltsgesetz-Entwurfs ist vorgesehen, dass alle dort genannten Verstöße nicht nur den Arbeitsämtern und den Trägern der gesetzlichen Versicherungen zuzuleiten sind, sondern auch dem Träger der Sozialhilfe. Dies ist zu weitgehend: Voraussetzung für eine derartige Übermittlung sollte zumindest sein, dass der Bezug von Sozialhilfe nahe liegt.

Das Ministerium des Innern und für Sport hat diese Kritikpunkte in das Gesetzgebungsverfahren des Bundes eingebracht.

12.2 Anteil der Speicherung von abgelehnten Asylbewerbern in INPOL

Pressemeldungen waren Anlass für die Kommission beim LfD, sich mit der Frage zu befassen, in welchem Umfang abgelehnte Asylbewerber in polizeilichen Informationssystemen, insbesondere im bundesweiten INPOL, erfasst werden.

Die Recherchen des LfD ergaben, dass abgelehnte Asylbewerber im System INPOL in dieser Eigenschaft nicht gespeichert werden.

Im Fahndungsbestand, der als Teil von INPOL geführt wird, können allerdings gem. § 66 AsylverfahrensG Ausländer zur Aufenthaltsermittlung ausgeschrieben werden, wenn ihr Aufenthaltsort unbekannt ist und sie

- innerhalb einer Woche nicht in der Aufnahmeeinrichtung eintreffen, an die sie weitergeleitet worden sind,
- die Aufnahmeeinrichtung verlassen haben und innerhalb einer Woche nicht zurückgekehrt sind,
- einer Zuweisungsverfügung oder einer Verfügung nach § 60 Abs. 2 Satz 1 AsylverfahrensG innerhalb einer Woche nicht Folge geleistet haben oder
- unter der von ihnen angegebenen Anschrift oder der Anschrift der Unterkunft, in der sie Wohnung zu nehmen haben, nicht erreichbar sind. Diese Voraussetzung liegt vor, wenn der Ausländer eine an die Anschrift bewirkte Zustellung nicht innerhalb von zwei Wochen in Empfang genommen hat.

Zuständig, die Ausschreibung zu veranlassen, sind die Aufnahmeeinrichtung, die Ausländerbehörde, in deren Bezirk sich der Ausländer aufzuhalten hat, und das Bundesamt für die Anerkennung ausländischer Flüchtlinge. Die Ausschreibung darf nur von hierzu besonders ermächtigten Personen veranlasst werden. Die Gruppe der nach dieser Vorschrift in INPOL ausgeschriebenen Ausländer umfasst nach den Angaben des BKA (Stand: 14.Februar 2001) 7 799 Personen.

Gemäß § 42 Abs. 7 AuslG können Ausländer zum Zweck der Aufenthaltsbeendigung in den Fahndungshilfsmitteln der Polizei zur Aufenthaltsermittlung und Festnahme ausgeschrieben werden, wenn ihr Aufenthalt unbekannt ist. Im Fall einer Ausweisung können Ausländer zum Zweck der Einreiseverhinderung außerdem zur Zurückweisung und für den Fall des Antreffens im Bundesgebiet zur Festnahme ausgeschrieben werden. Zweck der letztgenannten Ausschreibung ist insbesondere, bei Personenkontrollen erkennen zu können, ob sich überprüfte Personen unberechtigt im Bundesgebiet aufhalten. Die Ausschreibungsdauer beträgt zehn Jahre, wenn die Rechtswirkung einer Ausweisung gem. § 8 Abs. 2 AuslG nicht kürzer befristet ist. Nach einer vom LfD veranlassten Auswertung des BKA mit Stand vom 8. Februar 2001 sind 641 404 Personen nach dieser Vorschrift (§ 42 Abs. 7 AuslG) im Fahndungsbestand von INPOL ausgeschrieben. Insgesamt sind derzeit 924 540 Personen in INPOL zur Fahndung ausgeschrieben.

Die im Verhältnis zu den sonstigen Personen relativ große Zahl von nach ausländerrechtlichen Vorschriften zur Fahndung ausgeschriebenen Personen (70,2 %, also mehr als zwei Drittel des Gesamtbestandes) erklärt sich primär aus der Speicherungsdauer der nach § 42 Abs. 7 AuslG gespeicherten Daten: Die in diesen Fällen auf grundsätzlich zehn Jahre angelegte Speicherung führt zu einem umfangreichen Datenbestand.

Datenschutzrechtliche Bedenken gegen die auf ausdrücklichen gesetzlichen Regelungen beruhende Verfahrensweise wurden weder von anderen Datenschutzbeauftragten noch vom LfD erhoben.

12.3 Ausschreibungen im Schengener Informations-System (SIS) zur Einreiseverweigerung

Ausländer aus Staaten außerhalb der EU können, wenn sie von einer deutschen Behörde ausgewiesen worden sind, außer im nationalen polizeilichen Informationssystem (INPOL) auch im SIS ausgeschrieben werden. Die SIS-Ausschreibung ermöglicht eine Zurückweisung bereits an den Außengrenzen des Schengengebietes. Im Berichtszeitraum wurde der LfD im Zusammenhang mit SIS-Auschreibungen mit folgenden datenschutzrechtlich relevanten Problemen konfrontiert:

12.3.1 Beachtung der Prüffristen

Ausschreibungen im SIS sind erst seit 1995 möglich. Die bereits bestehenden INPOL-Ausschreibungen wurden zunächst pauschal durch das BKA in das SIS übernommen. Ausschreibungen im SIS zur Einreiseverweigerung sind nach einem Fristablauf von drei Jahren auf ihre Erforderlichkeit zu überprüfen. Nach derzeitiger Praxis erfolgt nach Ablauf der Prüffrist durch das BKA eine automatische Verlängerung der Laufzeit. Diese Verlängerung wird den für die Ausschreibung verantwortlichen Ausländerbehörden mitgeteilt. Wünscht nun die Ausländerbehörde im Einzelfall keine Verlängerung der Ausschreibung, so hat sie dies der Polizei mitzuteilen. Unterbleibt die Mitteilung, so bleibt die Ausschreibung weiterhin bestehen.

Gegen diese „verfahrensvereinfachende“ Praxis hat der LfD Bedenken. Sie führt erfahrungsgemäß dazu, dass eine Prüfung des Einzelfalles über die weitere Speicherung in vielen Fällen unterbleibt. Gerade die Einzelfallprüfung ist nach Ablauf einer Prüffrist zwingend erforderlich. Nach Auffassung des LfD ergibt sich aus Art. 112 SDÜ eine Löschungsfrist nach spätestens drei Jahren, wenn nicht durch die Prüfung der Ausländerbehörde die Notwendigkeit einer weiteren Speicherung ausdrücklich festgestellt wurde.

Der LfD hat seine datenschutzrechtlichen Bedenken zu diesem Problembereich dem zuständigen Ministerium des Innern und für Sport vorgetragen. Dieses legte daraufhin in einem Rundschreiben an die Ausländerbehörden fest, dass nach dreijährigen SIS-Ausschreibungen im Einzelfall zu prüfen ist, ob eine Verlängerung der Ausschreibung erforderlich ist und dass im Falle der Verlängerung die Gründe für diese Entscheidung in der Akte zu vermerken sind.

Diese Regelung ist zwar dem Grunde nach zu begrüßen; der LfD hält sie aber aus datenschutzrechtlicher Sicht nicht für ausreichend. Es besteht weiterhin die Gefahr, dass Mitteilungen zu Prüffristen nicht beachtet werden, was automatisch eine Verlängerung der Laufzeiten über drei Jahre auslöst. Der LfD hat deshalb gegenüber dem Ministerium vorgeschlagen, die Verfahrensweise so zu ändern, dass bei einem Schweigen der zuständigen Ausländerbehörden keine Verlängerung der Speicherung, sondern eine Löschung erfolgt.

12.3.2 Beginn der Prüffristen im SIS

Bei Überprüfungen aus Anlass der Eingaben zweier Petenten ergab sich, dass die Ausschreibung im SIS erst im Jahr 1997 erfolgte, obwohl das Ereignis, das zu diesen Ausschreibungen geführt hatte, bereits im Jahr 1993 lag. Als Beginn der Laufzeit für die Prüffrist wurde 1997, also das Eingabejahr, eingetragen. Die Prüffrist hätte aber schon im Jahr 1993 beginnen müssen. Dies hätte zu einer zwischenzeitlichen Löschung bzw. der Unterlassung einer Ausschreibung im SIS geführt. Stattdessen war für beide Personen eine Speicherung im SIS bis zum Jahre 2003 vorgesehen, also noch zehn Jahre nach dem Ereignis, das der Speicherung zu Grunde lag.

Diese Verfahrensweise hält der LfD für unzulässig, da der Beginn einer Prüffrist bei einer erstmaligen Speicherung identisch sein muss mit dem Zeitpunkt des Ereignisses, das der Speicherung zu Grunde liegt. Dies kommt auch in den Allgemeinen Anwendungshinweisen zum Schengener Durchführungsübereinkommen unter Punkt 2.2.2.1, Satz 3, zum Ausdruck.

12.3.3 Ausschreibungen im SIS bei untergetauchten Asylbewerbern

Dem LfD wurden vom BfD zahlreiche Eingaben marokkanischer Staatsangehöriger übersandt, die bei der französischen Datenschutzbehörde ein Auskunfts- bzw. Löschungsersuchen in Bezug auf ihre Ausschreibung im SIS gestellt hatten. Bei dem Personenkreis handelte es sich um in Deutschland abgelehnte Asylbewerber, die nach Artikel 96 SDÜ im SIS zur Einreiseverweigerung ausgeschrieben waren. Ein großer Teil dieser Personen war ausgeschrieben worden, nachdem der Asylantrag abgelehnt worden und der Antragsteller „untergetaucht" war, ohne dass eine Ausweisung erfolgt war. In diesen Fällen konnte zwar eine nationale Ausschreibung im Fahndungssystem der Polizei erfolgen, für eine SIS-Ausschreibung hätte aber eine Ausweisung vorliegen müssen.

Zur Überprüfung der in diesen Fällen üblichen Ausschreibepraxis wurden vom LfD mehrere örtliche Feststellungen bei Ausländerbehörden durchgeführt. Die Überprüfungen ergaben, dass dort in der Vergangenheit grundsätzlich Schengen-Ausschreibungen dieser Art vorgenommen worden waren, ohne dass eine Ausweisung vorgelegen hatte. Diese Ausschreibungen wurden auf Anregung des LfD gelöscht.

Außerdem wurden auf Anregung des LfD alle Ausländerbehörden durch das Ministerium des Innern und für Sport auf die Rechtslage bei SIS-Ausschreibungen hingewiesen.

12.4 Einführung einer Asyl-Card

Erneut wurde im Berichtszeitraum die Einführung einer Chipkarte für Asylbewerber als Instrument der Identifikation und möglicherweise auch der Leistungsabwicklung gegenüber den Inhabern der Karte vom Bundesministerium des Innern den Ländern vorgeschlagen. Eine Anfrage des Ministeriums des Innern und für Sport an den LfD betraf die probeweise Einführung einer solchen Asyl-Card bei den Asylbewerbern im Land. Der LfD wies insbesondere auf die Problematik hin, eine derartige probeweise Anwendung auf der Grundlage der Einwilligung der betroffenen Asylbewerber durchzuführen: Dabei ist es schwierig, Bedingungen herzustellen, die es erlauben, von Freiwilligkeit auf Seiten der Betroffenen zu sprechen. Deshalb haben sich auch alle Datenschutzbeauftragten, die sich hierzu geäußert haben, ablehnend verhalten.

Diese Frage wurde mit der Kommission beim LfD erörtert. Es ergab sich, dass Übereinstimmung dahin gehend bestand, auch für eine solche Erprobung der Asyl-Card eine gesetzliche Grundlage zu fordern.

13. Finanzverwaltung

13.1 Abgabenordnung

13.1.1 § 31 a Abs. 1 AO

Aufgrund einer Eingabe hatte sich der LfD mit der Datenübermittlung eines Finanzamtes an ein städtisches Ausländeramt zu beschäftigen. Dabei ging es auch um die Anwendung von § 31 Abs. 1 S. 2 AO. In Satz 1 dieser Vorschrift heißt es, die Offenbarung der nach § 30 geschützten Verhältnisse des Betroffenen ist zulässig, soweit sie der Bekämpfung der Schwarzarbeit dient und der Betroffene schuldhaft seine steuerlichen Pflichten verletzt hat. Nach Satz 2 gilt Gleiches, wenn ein Arbeitnehmer ohne die erforderliche Genehmigung nach § 284 Abs. 1 Satz 1 des SGB III beschäftigt ist oder tätig wird.

Nach Ansicht des LfD verweist § 31 a Abs. 1 S. 2 AO auf die Voraussetzungen von Satz 1. Dann ist für eine Offenbarung auch erforderlich, dass der Betroffene die ihm obliegenden steuerlichen Pflichten verletzt hat. Der Anwendungserlass für die Finanzverwaltung sieht dagegen vor, dass die Voraussetzung – schuldhafte Verletzung der steuerlichen Pflichten – nur die Fälle des Satzes 1 betrifft. Gleiches ist auch in der AO-Kartei zu § 31 a der OFD Koblenz geregelt. Der BfD hat nach Hinweis auf diese Situation mittlerweile beim Bundesfinanzministerium auf eine Änderung des Anwendungserlasses hinzuwirken versucht. Dies ist bisher noch ohne Erfolg geblieben.

13.1.2 Zugriff der Finanzverwaltung auf DV-gestützte Buchführungssysteme

Ab 1. Januar 2002 wird es für die Finanzverwaltung durch Änderung der Abgabenordnung möglich sein, auf DV-gestützte Buchführungssysteme von Steuerpflichtigen zuzugreifen. Dieses Recht steht der Steuerverwaltung nur im Rahmen der steuerlichen Außenprüfung zu. Deren sachlicher Umfang soll dadurch nicht erweitert werden. Durch Einführung der neuen Prüfungsmethode sollen rationellere und zeitnahe Außenprüfungen erreicht werden. Hierzu stehen der Finanzbehörde drei Möglichkeiten zur Verfügung:

- Beim unmittelbaren Datenzugriff nimmt die Finanzverwaltung mit Hilfe des Systems des Steuerpflichtigen Einsicht in dessen Unterlagen. Es erfolgt ein Nur-Lesezugriff. Eine Fernabfrage ist ausgeschlossen.

- Beim mittelbaren Datenzugriff kann die Steuerverwaltung verlangen, dass der Steuerpflichtige selbst Daten auswertet, um einen Nur-Lesezugriff zu ermöglichen.
- Bei der Datenträgerüberlassung schließlich kann vom Steuerpflichtigen verlangt werden, dass er die gespeicherten Unterlagen auf einem maschinell verwertbaren Datenträger der Finanzverwaltung zur Auswertung übergibt.

Die vorgesehene Ergänzung der Abgabenordnung konnte aus Sicht des LfD nur bei restriktiver Auslegung mitgetragen werden. Voraussetzung hierfür war, dass kein Online-Zugriff im Wege der Fernabfrage durch die Finanzverwaltung stattfindet, dass sich der Lohnkontenzugriff auf steuerrelevante Teile beschränkt und entsprechende technische Sicherungsmaßnahmen getroffen werden. Eine Protokollierungspflicht für Zugriffe der Finanzverwaltung ergibt sich bereits aus den bestehenden datenschutzrechtlichen Vorschriften. Damit die Betroffenen sich auf die Veränderungen und den damit unter Umständen erhöhten Aufwand einstellen können, wurde erreicht, dass die Vorschrift erst zum 1. Januar 2002 in Kraft tritt.

13.2 Datenerhebungen durch das Finanzamt

13.2.1 *Fahrtenbuch zu steuerlichen Zwecken*

Wer ein Fahrzeug erwirbt und dieses für Geschäftszwecke nutzt, kann die Anschaffungskosten teilweise gegenüber dem Finanzamt steuermindernd geltend machen. Will man keine pauschale Anrechnung, kann man den tatsächlichen Nutzen für Geschäftszwecke durch Führen eines Fahrtenbuches nachweisen. Die erforderlichen Eintragungen in ein solches Fahrtenbuch sorgen immer wieder für Eingaben betroffener Bürger an den LfD. In einem Fall ging es um Veranlagungszeiträume vor 1996. Der Steuerpflichtige hatte in seinem Fahrtenbuch lediglich die Geschäftsfahrten genau aufgezeichnet, für die Privatfahrten hatte er die gefahrenen Kilometer angegeben, ohne nähere Auskünfte zu Zweck und Ziel zu machen. Dies wurde von der Finanzverwaltung und im anschließenden Rechtsstreit durch das Finanzgericht nicht anerkannt. Da der private Gebrauch des Fahrzeugs einen ungewöhnlich geringen Umfang hatte, verlangte man von ihm auch die detaillierte Aufzeichnung seiner Privatfahrten. Begründet wurde dies mit einer Vorschrift aus der Einkommenssteuerrichtlinie 1987. Danach oblag es dem Steuerpflichtigen, zur Abgrenzung der betrieblichen Kosten von denen der privaten Lebensführung den Umfang der betrieblichen Nutzung nachzuweisen.

Ein solcher Nachweis konnte nach Auffassung des LfD damals wie heute dadurch geführt werden, dass die Geschäftsreisen aufgeführt wurden und somit von der Finanzverwaltung nachgeprüft werden konnten. Bestanden Zweifel am geschäftlichen Anlass einer Fahrt, hätte die Finanzverwaltung diese Fahrt nicht als betrieblich veranlasst anerkannt. Dabei spielte es keine Rolle, welchen Zweck die Fahrt tatsächlich hatte. Daher konnte es bei den Privatfahrten nicht darauf ankommen, welches Ziel und welchen Zweck sie verfolgten. Lediglich Datum und Kilometerleistung waren hierfür relevant. Folglich konnte der Steuerpflichtige generell auch *nicht verpflichtet werden, ähnlich umfangreiche Informationen zu seinen Privatfahrten wie zu seinen Geschäftsfahrten aufzu*zeichnen.

Da in der vorgetragenen Sache jedoch bereits ein rechtskräftiges Urteil vorlag, konnte die vertretene Auffassung für den zurückliegenden Zeitraum nicht durchgesetzt werden. Es ist jedoch davon auszugehen, dass zumindest für Veranlagungszeiträume ab 1996 sichergestellt ist, dass die Eintragungen in das Fahrtenbuch für private Zwecke lediglich Datum und Kilometerangaben enthalten müssen und die Finanzverwaltung keine darüber hinausgehenden Eintragungen verlangt. So sehen dies die entsprechenden Richtlinien inzwischen vor.

13.2.2 Steuerliche Geltendmachung eines PCs

Beabsichtigt ein Steuerpflichtiger, die Anschaffungskosten seines PCs steuerlich geltend machen, verlangt das zuständige Finanzamt hierzu des Öfteren die Vorlage einer aktuellen Übersicht über die Verzeichnisstruktur der Festplatten sowie einer Liste der darauf gespeicherten Dokumente. Auf Beschwerden der Betroffenen hin hat der LfD hierzu Folgendes vertreten:

Die in einem Steuerverfahren Beteiligten und andere Personen haben nach der Abgabenordnung der Finanzbehörde die zur Feststellung eines für die Besteuerung erheblichen Sachverhalts erforderlichen Auskünfte zu erteilen. In den fraglichen Fällen ging es um die Beurteilung, ob der PC bei der Festsetzung der Besteuerung als Arbeitsmittel berücksichtigt werden konnte. Dazu war der Nachweis zu erbringen, dass dieser überwiegend für berufliche Zwecke genutzt wurde. Die allgemeine Feststellung einer tatsächlichen beruflichen Nutzung reichte nicht aus. Vielmehr war weiterhin erforderlich, dass gegenüber der festgestellten beruflichen die private Nutzung von ganz untergeordneter Bedeutung war. War nicht nachprüfbar oder nicht klar erkennbar, ob der PC weitaus überwiegend dem Beruf diente, so waren die Aufwendungen für die Anschaffung steuerlich nicht anrechenbar. Daher konnte das Finanzamt grundsätzlich Angaben verlangen, die sichere Rückschlüsse auf die Art der Nutzung zulassen, zumal die gegenüber dem Finanzamt gemachten Angaben dem Steuergeheimnis unterliegen. Wenn sich also aus der Verzeichnisstruktur des Rechners und einer Liste der gespeicherten Dokumente ergab, in welcher Form der PC genutzt wurde, waren die Betroffenen zur entsprechenden Auskunft verpflichtet. Ein Auskunfts- oder Vorlageverweigerungsrecht lag nicht vor.

13.2.3 Lohnsteueraußenprüfung

Die Finanzverwaltung verlangte von der AOK im Rahmen einer Lohnsteuer-Außenprüfung Auskunft über die Krankenversicherungsbeiträge der bei ihnen beschäftigten Dienstordnungsangestellten. Solche Angestellte erhalten einen Rabatt auf ihre Versiche-

rungsbeiträge, der gemäß einem BFH-Urteil als geldwerter Vorteil zu versteuern ist. Das Finanzamt hatte hierzu eine entsprechende Liste der Betroffenen bei der AOK vorgelegt. Diese wandte ein, dass die begehrten Informationen lediglich im Rahmen ihrer Krankenversicherungstätigkeit vorlägen und daher eine Auskunftspflicht nach Steuerrecht nicht bestehe.

Dieser Auffassung der Krankenversicherung schloss sich der LfD nicht an. Zwar ist letztlich der einzelne Angestellte Schuldner der Lohnsteuer, jedoch hat der Arbeitgeber die Lohnsteuer für Rechnung des Arbeitnehmers bei jeder Lohnzahlung einzubehalten. Deswegen muss der Arbeitgeber auch wissen, was der Arbeitnehmer an Arbeitslohn erhält, um die korrekte Lohnsteuersumme einzubehalten. Folglich musste die AOK als Arbeitgeberin wissen, welche Krankenversicherungsbeiträge von ihren Dienstordnungsangestellten gezahlt wurden, um den daraus ermittelten geldwerten Vorteil versteuern zu können. Ob dies ordnungsgemäß geschehen ist, konnte von der Finanzbehörde im Rahmen einer Lohnsteuer-Außenprüfung kontrolliert werden. Die Lohnsteuer-Außenprüfung hat sich u. a. hauptsächlich darauf zu erstrecken, ob alle zum Arbeitslohn gehörigen Einnahmen dem Steuerabzug unterworfen wurden und bei der Berechnung der Lohnsteuer von der richtigen Lohnhöhe ausgegangen worden ist. Folglich war die AOK als Arbeitgeberin verpflichtet, die benötigten Angaben zu machen.

13.3 Datenübermittlungen durch das Finanzamt

13.3.1 Auskünfte an Gewerbeamt

Ein Petent beschwerte sich darüber, dass ein Finanzamt Informationen aus seiner Steuerakte an eine Verbandsgemeinde weitergegeben hatte. Dabei handelte es sich um Informationen über die Verletzung steuerlicher Pflichten. Diese Datenübermittlung führte zur Gewerbeuntersagung für den Petenten.

Die Verletzung steuerrechtlicher Pflichten kann grundsätzlich die Unzuverlässigkeit im gewerberechtlichen Sinn begründen und zur Gewerbeuntersagung führen. Es konnte im vorliegenden Fall daher durchaus zulässig sein, wenn das Finanzamt entsprechende Informationen an die Gewerbebehörde weitergab. Diese Weitergabe war jedoch aufgrund des geltenden Steuergeheimnisses an strenge Voraussetzungen geknüpft, die das Ministerium der Finanzen in einem Rundschreiben von 1991 festgelegt hat. Wenn eine Informationsweitergabe in Frage kommen soll, müssen zunächst Anhaltspunkte für erhebliche steuerliche Verstöße vorliegen (Steuerschuld von mehr als 5 000,– DM oder schleppender Zahlungseingang). Wenn solche Verstöße gegeben sind, ist eine Auskunft zulässig, soweit diese entweder der Durchführung eines Verwaltungs- oder Gerichtsverfahrens in Steuersachen dient, sich aus spezialgesetzlicher Regelung ergibt oder der Gewerbetreibende zugestimmt hat. Im vorliegenden Fall waren die Voraussetzungen für die Mitteilung des Finanzamtes erfüllt, so dass die Datenübermittlung nicht zu beanstanden war.

13.3.2 Auskünfte nach dem Sozialgesetzbuch

In einer weiteren Eingabe im Bereich der Steuerverwaltung ging es um die Datenübermittlung eines Finanzamtes an eine Stadtverwaltung, um die Unterhaltsverpflichtungen der Petentin gegenüber deren Mutter im Rahmen der Hilfe zur Pflege festzustellen. Die Stadtverwaltung hatte trotz mehrmaliger Nachfragen die notwendigen Angaben von der Betroffenen nicht erhalten.

Da es um die Feststellung von Unterhaltsverpflichtungen ging, war das Finanzamt gem. § 21 Abs. 4 SGB X verpflichtet, der Stadtverwaltung Auskünfte über das Einkommen der Petentin zu erteilen. Die Informationen waren für die Festsetzungen im vorliegenden Verfahren erforderlich. Da man sie von der Betroffenen nicht erhalten hatte, durfte die Stadt vom Grundsatz, Daten stets beim Betroffenen zu erheben, abweichen und sich an das Finanzamt wenden. Eine Verletzung des Steuergeheimnisses lag nicht vor, da eine Offenbarung durch Gesetz ausdrücklich zugelassen war.

13.4 Hundesteuersatzung

13.4.1 Auskunftspflicht der Hundehalter

In einer rheinland-pfälzischen Hundesteuersatzung fand sich die Verpflichtung eines jeden Grundstückseigentümers, der Stadt oder dem von ihr Beauftragten auf Nachfrage über die auf dem betreffenden Grundstück gehaltenen Hunde und deren Halter wahrheitsgemäß Auskunft zu geben. Dies stieß auf Bedenken ortsansässiger Grundstückseigentümer.

Diese Vorschrift der Satzung enthielt keine Regelung, die über den auch für kommunale Abgaben geltenden § 93 Abs. 1 AO hinausging. Danach haben die Beteiligten und andere Personen der Finanzbehörde die zur Feststellung eines für die Besteuerung erheblichen Sachverhaltes erforderlichen Auskünfte zu erteilen. Andere Personen als die Beteiligten sollen aber erst dann zur Auskunft angehalten werden, wenn die Sachverhaltsaufklärung durch die Beteiligten nicht zum Ziele führt oder keinen Erfolg verspricht. Dieser sog. Erstbefragungsgrundsatz war, da die fragliche Vorschrift keine Regelung hierzu enthielt, beim Vollzug der Hundesteuersatzung zu beachten.

Da die Vorschrift auch die Verpflichtung enthielt, den von der Stadt Beauftragten Auskunft zu geben, hat der LfD darauf aufmerksam gemacht, dass bei einer Steuererhebung private Dritte nur bedingt beauftragt werden können. Bei der Erhebung des Hundebestandes hält der LfD die Zuhilfenahme privater Dritter nur dann für zulässig, wenn sich deren Tätigkeit auf eine reine Verwaltungshilfe beschränkt und mit keinerlei hoheitlichen Befugnissen versehen ist.

13.4.2 Mitteilungspflicht des Tierschutzvereins an das Hundesteueramt

Ein rheinland-pfälzischer Tierschutzverein sollte dem städtischen Steueramt in regelmäßigen Abständen die Namen und Anschriften von Hundeerwerbern mitteilen. Im Tierschutzverein war man zwar bereit, die Namen der Hundeerwerber, die in der betroffenen Stadt wohnten, mitzuteilen. Jedoch hatte man Bedenken gegen die Übermittlung der Daten auswärtiger Erwerber. Die örtliche Hundesteuersatzung sah vor, dass der bisherige Halter eines Hundes den Hund, der abgeschafft wurde, abzumelden hatte. Im Fall der Veräußerung des Hundes waren bei der Abmeldung Name und Anschrift des Erwerbers anzugeben. Eine Beschränkung der Mitteilungspflicht auf Erwerber mit entsprechendem Wohnsitz bestand nicht. Die Hundesteuersatzung sah vielmehr vor, dass die Gemeinde, in der der Erwerber wohnt, über den Erwerbsvorgang unterrichtet wird. Das diente einer einheitlichen Besteuerung und verhinderte, dass Erwerber der Steuerpflicht dadurch zu entgehen versuchen, dass sie einen Hund in einer anderen Stadt erwerben. Die Satzung verstieß insoweit nicht gegen die Abgabenordnung als höherrangiges Recht und war eine wirksame Rechtsgrundlage für die umfassende Mitteilungspflicht des Tierschutzvereins.

13.5 Korruption in der öffentlichen Verwaltung

Im 17. Tb. (Tz. 13.3) wurde über die weitere Entwicklung der Verwaltungsvorschrift zur Bekämpfung der Korruption in der öffentlichen Verwaltung berichtet. Diese wurde im Berichtszeitraum neu gefasst. Nunmehr sind darin die Unterrichtungspflicht der betroffenen Unternehmen enthalten sowie Regelungen bei Meldungen, die einen Einzelunternehmer betreffen. Für diesen Fall ist vorgesehen, dass die Bestimmungen des Datenschutzes über personenbezogene Daten zu beachten sind. Damit wurden die zentralen Forderungen des LfD umgesetzt.

14. Wirtschaft und Verkehr

14.1 Daten aus der Handwerksrolle im Internet?

Die Anfrage, ob datenschutzrechtliche Bedenken dagegen bestehen, dass in der Handwerksrolle erfasste Daten in separaten Datenbanken für Nutzer aus dem Internet zur Verfügung gestellt werden, hat der LfD wie folgt beantwortet:

Die Einbindung von – für jedermann frei zugänglichen – Datenbanken ins Internet ist datenschutzrechtlich unbedenklich. Im vorliegenden Fall ist allerdings zu beachten, dass die Daten der Handwerksrolle nur unter den einschränkenden Voraussetzungen des § 6 HandwerksO übermittelt werden dürfen. So darf gem. § 6 Abs. 3 Satz 1 HandwerksO eine Einzelauskunft aus der Handwerksrolle nur jemandem erteilt werden, der ein berechtigtes Interesse glaubhaft darlegt. Bei einer listenmäßigen Übermittlung muss der Auskunftsbegehrende nach § 6 Abs. 3 Satz 2 HandwerksO ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft darlegen, und es darf außerdem kein Grund zu der Annahme bestehen, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat. Gem. § 6 Abs. 5 HandwerksO darf der Empfänger die übermittelten Daten nur für den Zweck verarbeiten oder nutzen, zu dessen Erfüllung sie ihm übermittelt werden. Da auch öffentliche Stellen Zugang zum Internet haben, ist ebenfalls die Einschränkung des § 6 Abs. 4 HandwerksO zu beachten. Öffentlichen Stellen sind nur auf Ersuchen Daten aus der Handwerksrolle zu übermitteln, sobald die Kenntnis tatsächlicher oder rechtlicher Verhältnisse selbständiger Handwerker zur Erfüllung ihrer Aufgabe erforderlich ist. Die Prüfung dieser rechtlichen Voraussetzungen für die Auskunftserteilungen aus der Handwerksrolle ist bei Abfragen über das Internet bislang nicht möglich.

Für das von der Handwerkskammer vorgesehene Verfahren steht eine gesetzliche Grundlage also nicht zur Verfügung. Mithin bestehen nur dann aus der Sicht des Datenschutzes keine Bedenken gegen eine Veröffentlichung im Internet, wenn die betroffenen Handwerker hierzu vorher eine Einwilligungserklärung unter Berücksichtigung der Regelungen in § 5 Abs. 2 und 3 LDSG abgegeben haben. Die Wirksamkeit der Einwilligung setzt hier nach Auffassung des LfD voraus, dass die Betroffenen durch vorherige Information über die mit dem Internet verbundenen Risiken aufgeklärt werden. Dazu gehören auch die derzeit noch bestehenden Gefahren für die Datensicherheit, so z. B. mögliche Veränderungen und Löschungen der Daten auf den Internet-Servern.

14.2 Löschung von Daten aus der Gewerbeanzeige nach Abmeldung des Gewerbes

Die Gewerbeordnung enthält keine bereichsspezifische Regelung, wie lange Daten aus der Gewerbeanzeige aufzubewahren sind, nachdem das Gewerbe abgemeldet wurde. Auf dieses Problem wurde der LfD seitens einiger Gemeinden angesprochen. In seiner Antwort hat er darauf hingewiesen, dass gem. § 14 Abs. 11 GewO für das Löschen der nach § 14 Abs. 1 bis 4 GewO erhobenen Daten die Datenschutzgesetze der Länder gelten. Nach § 19 Abs. 2 Nr. 2 LDSG sind personenbezogene Daten zu löschen, wenn ihre Kenntnis für die Daten verarbeitende Stelle zur Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben nicht erforderlich ist, wobei die Erforderlichkeit sich nach den für die Daten verarbeitenden Stellen getroffenen allgemeinen Regelungen über die Dauer der Aufbewahrung von personenbezogenen Daten einschließlich der Erfordernisse einer ordnungsgemäßen Dokumentation richtet. Eintragungen in das Gewerbezentralregister sowie Auskünfte daraus richten sich nach den §§ 149 Abs. 2, 150 a GewO und unterliegen eigenen Löschungsregeln (§§ 152, 153 GewO).

Die Vorschrift des § 14 GewO dient in erster Linie der Überwachung der Tätigkeit der Gewerbetreibenden, indem die Gewerbebehörden durch die Gewerbeanzeigen ein genaues Bild über die Zahl und Art der Gewerbetreibenden bekommen. Wenn nun – wie dem LfD geschildert wurde – Jahre nach der Abmeldung der Gewerbebetriebe an das Gewerbeamt noch immer Anfragen ge-

richtet werden, geht es dabei meist im Interesse der Betroffenen um die Behebung einer Beweisnot. In diesen Fällen könnte die behördliche Dokumentationspflicht das Hinausschieben der Löschung bestimmter Kerninformationen begründen. Dies hat sich nach den dem LfD vorliegenden Informationen z. B. bei Auskünften im Rentenverfahren als sinnvoll erwiesen. Was den Zeitrahmen, den Umfang der Kerninformationen sowie das Medium (Online-Datenbank, gesondert aufzubewahrende Archivdatenträger oder Akten) anbelangt, sollte nach Auffassung des LfD eine landeseinheitliche Verfahrensweise angestrebt werden. Diesbezüglich hat er mit Blick auf praxistaugliche Lösungsmöglichkeiten inzwischen mit dem Wirtschaftsministerium Kontakt aufgenommen.

14.3 Auskünfte aus dem Gewerberegister an Parteien zum Zwecke der Wahlwerbung

Hier ging es um die Frage der Zulässigkeit einer Datenübermittlung seitens des Gewerbeamtes einer Stadtverwaltung an eine Partei zum Zwecke der Wahlwerbung. Der LfD hat die Anfrage zur Auskunftserteilung über Gewerbebetriebe an eine nicht öffentliche Stelle – mit der Maßgabe, dass es sich um die Übermittlung von personenbezogenen Daten, also von Einzelangaben über natürliche Personen i. S. v. § 3 Abs. 1 LDSG handelt – wie folgt beantwortet:

Nach der Regelung in § 14 Abs. 8 Satz 1 GewO stehen die Angaben über Name, betriebliche Anschrift und ausgeübte Tätigkeit des Gewerbetreibenden – die drei Grunddaten aus einer Gewerbeanzeige – zur Übermittlung an nicht öffentliche Stellen bei Glaubhaftmachung eines berechtigten Interesses zur Verfügung.

Zu den berechtigten Interessen zählt jedes von der Rechtsordnung als schutzwürdig anerkannte oder ideelle oder vermögenswerte Interesse des Empfängers der Daten. Auszuscheiden ist lediglich die schlichte Neugier. Danach würde grundsätzlich auch ein politisches Interesse ausreichen.

Eine Abwägung mit den Interessen des Gewerbeanzeigenden an der Nichtweitergabe seiner drei Grunddaten ist in § 14 Abs. 8 Satz 1 GewO nicht vorgesehen. Hintergrund ist die Überlegung, dass die betreffenden Daten ohnehin jedermann zugänglich sein dürften (Telefonbuch, Firmenschild etc.). Zur Glaubhaftmachung genügt die in sich schlüssige Darstellung des berechtigten Interesses. Eine bestimmte Form ist nicht erforderlich. Für die Übermittlung weiterer Daten aus der Gewerbeanzeige muss allerdings gem. § 14 Abs. 8 Satz 2 GewO ein rechtliches Interesse glaubhaft gemacht werden, und es darf kein überwiegendes schutzwürdiges Interesse des Gewerbetreibenden berührt sein.

Im Gesamtzusammenhang dieser Anfrage war nach Auffassung des LfD jedoch darüber hinaus zu berücksichtigen, dass es eine Menge anderer Möglichkeiten gibt, um an die Zielgruppe der Gewerbetreibenden zu gelangen, etwa per „Gelbe Seiten", Postwurfsendung oder Zeitungsannonce. Im Übrigen hat er in diesem Zusammenhang auf Folgendes hingewiesen: Auch wenn die Auskunftsvoraussetzungen des § 14 Abs. 8 Satz 1 GewO vorliegen, bedeutet dies nicht zwangsläufig, dass ein Auskunftsanspruch besteht; denn die Gewerberegister sind keine öffentlichen Register. Vielmehr steht die Auskunftserteilung im pflichtgemäßen Ermessen der Behörde (vgl. Bundestagsdrucksache 12/5826, S. 17).

14.4 Eine Gewerbeabmeldung der besonderen Art

Die von einem Petenten in Gang gebrachten Nachforschungen des LfD haben ergeben, dass aufgrund seines Wegzugs aus einer Verbandsgemeinde sein dort betriebenes Gewerbe von Amts wegen abgemeldet wurde. Die für die Abmeldung erforderlichen Daten hatte die Verbandsgemeindeverwaltung aus dem automatisiert geführten Einwohnerinformationssystem (EWOIS) entnommen. Aus dieser Anwendung heraus besteht wiederum die Möglichkeit, direkt in das Verfahren „Bundeszentralregister-Anfragen" zu verzweigen. Aufgrund eines Bedienungsfehlers in der Sachbearbeitung sind die Daten aus der Gewerbeabmeldung sozusagen in die falsche Richtung gelenkt worden, was letztlich zur Beantragung eines Führungszeugnisses für den Petenten geführt hat.

Der Vorfall bestätigte erneut, dass beim Einsatz multifunktionaler Informationstechnik besondere Gefahren für das Recht auf informationelle Selbstbestimmung bestehen. Es ist eine wiederkehrende Erfahrung, dass gerade in diesem sensiblen Bereich gebotene Vorsichtsmaßnahmen außer Acht gelassen werden, so dass es, wie im vorliegenden Fall, zu vermeidbaren „Irrläufern" kommt.

Der Bürgermeister der betroffenen Verbandsgmeinde hat nach eindringlichem Hinweis des LfD sofort reagiert und aus Anlass dieses Falles gegenüber seinen Bediensteten nochmals eindringlich auf das Erfordernis der datenschutzgerechten Handhabung im Umgang mit den eingesetzten automatisierten Verfahren hingewiesen. Hier bleibt festzustellen, dass mangelnde Sorgfalt in der Sachbearbeitung dazu geführt hat, dass ohne Zutun des Petenten ein privates Führungszeugnis beim Bundeszentralregister beantragt wurde. Was die Schwere des Eingriffs anbelangt, war zu berücksichtigen, dass das Führungszeugnis ausschließlich dem Petenten als dem vermeintlichen Antragsteller übersandt wurde, mithin kein Dritter vom Inhalt des Führungszeugnisses Kenntnis erlangt hatte. Vor diesem Hintergrund war eine förmliche Beanstandung gem. § 25 Abs. 1 LDSG entbehrlich. Die Eingabe hat nach Einschätzung des LfD dort zu einer erheblichen Sensibilisierung im Bereich der praktischen Handhabung automatisierter Verwaltungsverfahren beigetragen.

14.5 Neuerteilung der Fahrerlaubnis und Datenschutz

Regelmäßig erreichen den LfD Eingaben und Anfragen zum Datenschutz im Führerscheinverfahren. Hinsichtlich der rechtlichen Bewertung der ihm geschilderten Vorgänge hat sich herausgestellt, dass folgende grundsätzliche Darlegungen von besonderer Bedeutung sind:

- Führungszeugnisse werden ausschließlich vom Bundeszentralregister erteilt. Wenn Eintragungen vorhanden sind, handelt es sich in aller Regel um rechtskräftige Verurteilungen durch Strafgerichte; daneben können bestimmte Verwaltungsentscheidungen (z. B. Passversagungen oder waffen- und gewerberechtliche Entscheidungen) im Bundeszentralregister eingetragen werden. Das Führungszeugnis zur Vorlage bei Behörden hat gegenüber dem Führungszeugnis für Private einen erweiterten Inhalt. Zum Beispiel gibt es auch Auskunft über geringfügige Strafen, die nicht in ein Führungszeugnis für Private aufgenommen werden, wenn es sich um Straftaten handelte, die bei der Ausübung eines Gewerbes begangen wurden. Diese Führungszeugnisse für Behörden werden zwar von den Betroffenen beantragt, aber nicht ihnen, sondern der Behörde übersandt. Dies führt nicht selten zu der – unzutreffenden – Vermutung, das Führungszeugnis habe irgendeinen „ geheimen Inhalt", den sie nicht erfahren könnten. Vielmehr haben die Betroffenen verschiedene Möglichkeiten, auch den Inhalt behördlicher Führungszeugnisse zu erfahren. Zum einen können sie das Führungszeugnis bei der Behörde einsehen, an die es adressiert wird. Wenn sie es einsehen wollen, bevor es an die Behörde gesandt wird, können sie verlangen, dass es zunächst an ein von ihnen benanntes Amtsgericht geschickt wird, wo sie Einblick nehmen und entscheiden können, ob es an die Behörde weitergeleitet wird.

- Die aus dem Führungszeugnis ersichtlichen Eintragungen im Bundeszentralregister sind für die Fahrerlaubnisbehörde im Rahmen der zu treffenden Entscheidung über den Antrag auf Neuerteilung einer Fahrerlaubnis von erheblicher Bedeutung. Es liegt im öffentlichen Interesse, dass ein Führungszeugnis zur Vorlage bei einer Behörde nach § 30 Abs. 5 BZRG die vorgeschriebenen Eintragungen bis zum Ablauf der im Gesetz bestimmten Fristen vollständig aufweist. Sind mehrere Verurteilungen eingetragen, so sind sie gem. § 38 Abs. 1 BZRG alle in das Führungszeugnis aufzunehmen, solange eine von ihnen in das Führungszeugnis aufgenommen werden muss.

- Erhebliche Verstöße gegen Verkehrsvorschriften oder Strafgesetze können nach § 2 Abs. 4 StVG die Eignung zum Führen von Kraftfahrzeugen ausschließen. Daher hat die Fahrerlaubnisbehörde gem. § 2 Abs. 7 StVG sorgfältige Feststellungen hinsichtlich möglicher Eignungsbedenken zu treffen. Hierzu gehört beispielsweise auch die Beiziehung von Strafakten, die im Führungszeugnis angeführt sind. Der Begriff der Eignung ist umfassend zu verstehen und schließt auch „charakterlich-sittliche" Beurteilungen ein (vgl. Jagusch/Hentschel, Straßenverkehrsrecht ; 35. Auflage, Rz. 20 zu § 2 StVG; siehe auch Begutachtungs-Leitlinien zur Kraftfahrereignung, herausgegeben von der Bundesanstalt für Straßenwesen, Bergisch-Gladbach, Februar 2000, S. 46 ff.).

- Die durch verwertbare Urteile bekannt gewordenen Eignungsbedenken können zur Anforderung eines medizinisch-psychologischen Gutachtens führen. Die Fahrerlaubnisbehörde gibt nach § 11 Abs. 6 FeV die Art der Begutachtung vor, die Auswahl der konkreten Untersuchungsstelle bleibt dem Betroffenen überlassen. Adressat der Anordnung, ein Eignungsgutachten beizubringen, ist also der betroffene Fahrerlaubnisbewerber. Er (nicht die Behörde) ist Auftraggeber der Begutachtung und damit auch Vertragspartner und Kostenschuldner des Gutachters bzw. der begutachtenden Stelle. Ihm, dem Betroffenen, steht auch die Auswahl des Gutachters bzw. bei einer Begutachtungsstelle für Fahreignung die Auswahl der Stelle zu – natürlich im Rahmen der Vorgaben, die die behördliche Anordnung hinsichtlich der Art der Begutachtung setzt. Er hat Anspruch auf die Aushändigung des Gutachtens. Nur mit seiner ausdrücklichen Zustimmung darf das Gutachten unmittelbar der Behörde oder Dritten zugeleitet werden.

- Nach § 2 Abs. 14 StVG darf die Fahrerlaubnisbehörde die von den amtlich anerkannten oder beauftragten Stellen zur Eignungsprüfung benötigten Daten an diese übermitteln. Konkretisiert wird diese Regelung in § 11 Abs. 6 Satz 4 FeV, wonach die Fahrerlaubnisbehörde der untersuchenden Stelle die vollständigen Unterlagen übersendet, soweit sie unter Beachtung der gesetzlichen Verwertungsverbote verwendet werden dürfen. In den Führerscheinakten sind Gutachten, Gesundheitszeugnisse, Registerauskünfte und Führungszeugnisse nach spätestens zehn Jahren zu vernichten, es sei denn, die Unterlagen stehen im Zusammenhang mit einer Registereintragung (vgl. § 2 Abs. 9 StVG). In diesem Zusammenhang ist auch die Verwertungsregelung in § 52 Abs. 2 BZRG zu beachten. Danach dürfen die Tat und die Entscheidung den Betroffenen nach der Tilgung in den Registern im Verfahren über die Erteilung der Fahrerlaubnis nicht mehr vorgehalten werden (vgl. dazu auch Tz. 14.6).

14.6 Probleme bei den Verwertungsregelungen im neuen Fahrerlaubnisrecht

Die Verwertungsregelungen im Fahrerlaubnisrecht sind ein Bereich, der den LfD immer wieder beschäftigt, insbesondere im Hinblick auf die Frage, welche früheren Verkehrsstraftaten im Zusammenhang mit der Neuerteilung einer entzogenen Fahrerlaubnis verwertet werden dürfen. Im 17. Tb. ist die Gesetzeslage vor und nach der Änderung des Straßenverkehrsgesetzes ausführlich dargestellt (vgl. Tz. 14.11 und 14.12). Genau in diesem Bereich der Verzahnung zwischen altem und neuem Recht gab es ein Problem, das der Bundesgesetzgeber bei seiner Regelung übersehen hat. Um die Problemlage zu verdeutlichen, wird nachfolgend kurz dargestellt, welche Regelung bis zur Gesetzesänderung gegolten hat:

Bei Verkehrsstraftaten betrug die Tilgungsfrist nach Straßenverkehrsgesetz fünf Jahre. Eine Verwertung dieser Delikte in Verfahren der Erteilung oder Entziehung einer Fahrerlaubnis war jedoch aufgrund einer Regelung im Bundeszentralregistergesetz zeitlich nicht fest begrenzt. So konnten auch länger als fünf Jahre zurückliegende Verkehrsstraftaten verwertet werden. Das Zusammenspiel dieser beiden Regelungsbereiche, also zum einen die fünfjährige Tilgungsbestimmung im Straßenverkehrsrecht, zum anderen die keine zeitliche Grenze vorsehende Regelung im Bundeszentralregistergesetz haben zu einer allseits als unbefriedigend eingestuften Situation geführt.

Die Verfahrensweisen bei den Führerscheinstellen waren sehr unterschiedlich. Bei örtlichen Feststellungen hat sich herausgestellt, dass Verurteilungen mit allen dazugehörigen Vorgängen, beispielsweise medizinisch-psychologischen Gutachten, manchmal bis in die frühen siebziger Jahre hinein als Bestandteil der jeweiligen Akte aufbewahrt und auch entsprechend genutzt wurden. Andere Führerscheinstellen wiederum haben im Rahmen des Fahrerlaubnisverfahrens getilgte Taten nur dann berücksichtigt, wenn sie nicht länger als zehn Jahre oder 15 Jahre zurücklagen. Aus dieser Situation heraus ergaben sich, insbesondere bei der Bearbeitung von Eingaben, vielfältige Problemlagen, zumal die Rechtsprechung ausdrücklich offen ließ, inwieweit der Verwertung zeitliche Grenzen gesetzt sind.

Mit der Neuregelung, die seit dem 1. Januar 1999 gilt, wurde die Tilgungsfrist nach Straßenverkehrsgesetz von fünf auf zehn Jahre heraufgesetzt. Im Gegenzug ist die nach der früheren Regelung im Bundeszentralregistergesetz zulässige zeitlich unbegrenzte Verwertungsmöglichkeit entfallen. Und wie das bei einem Wechsel von altem zu neuem Recht so üblich ist, hatte der Gesetzgeber auch eine Übergangsbestimmung (§ 65 Abs. 9 Satz 1 StVG) geschaffen. Danach wurden Entscheidungen, die vor dem 1. Januar 1999 im Verkehrszentralregister eingetragen worden sind, nach den früheren Bestimmungen des Straßenverkehrsgesetzes getilgt. Dies würde bedeuten, dass bei den „alten" Verkehrsstraftaten die Tilgungsfrist fünf Jahre beträgt. Eine Verwertung der „Altdelikte" über die Fünf-Jahresfrist hinaus wurde durch die frühere Regelung im Bundeszentralregistergesetz ermöglicht, die jedoch entfallen ist. Dies hätte zu einer vom Gesetzgeber nicht gewollten Besserstellung der Täter geführt, die vor dem 1. Januar 1999 in das Verkehrszentralregister eingetragen wurden. Aus diesem Grunde war eine Rechtsänderung im Straßenverkehrsgesetz erforderlich. So wird nunmehr durch eine Ergänzung von § 65 Abs. 9 Satz 1 StVG klarstellend darauf hingewiesen, dass Entscheidungen nach der früheren Regelung des Bundeszentralregistergesetzes (§ 52 Abs. 2 BZRG in der bis zum 31. Dezember 1998 geltenden Fassung) verwertet werden dürfen, jedoch längstens bis zu dem Tag, der einer zehnjährigen Tilgungsfrist entspricht. Damit sind die entstandenen Unzuträglichkeiten beseitigt und auch die Altfälle harmonisiert.

Im rheinland-pfälzischen Verkehrsministerium wurden die Verfahrenshinweise für das Führerscheinverfahren – wie stets in enger Abstimmung mit dem LfD – entsprechend angepasst.

14.7 Zweckwidrige Nutzung von TÜV-Daten

Eine TÜV-Gesellschaft mit Sitz in einem anderen Bundesland hat in einer groß angelegten Werbeaktion zahlreiche Kfz-Halterinnen und -Halter angeschrieben und Bezug genommen auf den Besuch bei der TÜV-Station, gleichzeitig die Freude darüber zum Ausdruck gebracht, dass den Angeschriebenen „ab sofort das Leben erleichtert" wird. Dazu gehöre, so wurde geworben, ein Dokumentendepot, in dem wichtige Unterlagen, z. B. Fahrzeugscheine archiviert seien. Weiterhin enthielt das Schreiben allerlei Werbeangebote von der Urlaubsreise bis zum Mobiltelefon – und zusätzlich die auf der Vorderseite des Schreibens angebrachte (von einem Tochterunternehmen der TÜV-Gesellschaft hergestellte) TÜV-Service Card mit den bereits eingelesenen personenbezogenen Halterdaten, die anlässlich der TÜV-Untersuchung des Fahrzeuges erhoben wurden.

Viele Angeschriebene beschwerten sich darüber beim LfD, denn sie hatten weder den TÜV noch eine Privatfirma ermächtigt, mit ihren personenbezogenen Daten „hausieren" zu gehen, noch hatten sie die Magnetkarte angefordert.

Im Rahmen seiner Zuständigkeit hat der LfD zu der Angelegenheit wie folgt Stellung genommen:

§ 29 Abs. 1 StVZO verpflichtet die Halter der dort genannten Fahrzeuge, diese in regelmäßigen Abständen auf Vorschriftsmäßigkeit untersuchen zu lassen. Es handelt sich also um eine gesetzlich vorgesehene periodische Zwangsprüfung, Hauptuntersuchung genannt. Die Prüfung ist durch amtlich anerkannte Sachverständige für den Kraftfahrzeugverkehr oder von einer amtlich anerkannten Überwachungsorganisation mittels eines ihr angehörenden Sachverständigen nach Anlage VIII b zu § 29 StVZO vorzunehmen. Die gem. § 29 StVZO tätigen Überwachungsorgane (Sachverständigen) handeln hoheitlich, weil ihre Tätigkeit auf das engste mit dem hierdurch vorbereiteten Verwaltungsakt (Plakettenzuteilung nebst Vermerk im Fahrzeugschein) zusammenhängt (vgl. Jagusch/Hentschel, Straßenverkehrsrecht, 35. Auflage, RdNrn. 22 und 27 zu § 29 StVZO, mit Nachweisen zur Rechtsprechung). Wenn nun ein Halter sein Fahrzeug zur Hauptuntersuchung bei einer TÜV-Untersuchungsstelle vorstellt, trifft er auf einen beliehenen Unternehmer in Person des dort zuständigen Sachverständigen, der – als öffentliche Stelle des Landes Rheinland-Pfalz – den Vorschriften des Kraftfahrsachverständigengesetzes unterliegt. In § 6 Abs. 2 KfSachvG ist bestimmt, dass der Sachverständige personenbezogene Daten, die ihm bei seiner Tätigkeit bekannt geworden sind, nur für diese Tätigkeit verwenden darf. Diese bereichsspezifische Datenschutzvorschrift enthält für Kraftfahrsachverständige mithin ein Verwertungsverbot für tätigkeitsfremde Zwecke, das auch – anderenfalls würde es leer laufen – für den Träger der Technischen Prüfstelle (TÜV e. V.) gilt, dessen Aufgaben wiederum durch die o. g. TÜV-Gesellschaft wahrgenommen werden. Diese Konstruktion führt im Übrigen dazu, dass der Sachverständige zugleich der Technischen Prüfstelle angehört und Angestellter des Geschäftsbesorgers, nämlich der TÜV-Gesellschaft

ist , also jener Gesellschaft, die mit der Werbeaktion an die Kfz-Halter herangetreten ist. Die von den Sachverständigen anlässlich der Hauptuntersuchungen rechtmäßig erhobenen personenbezogenen Daten sind im vorliegenden Fall allerdings seitens der TÜV-Gesellschaft zweckwidrig genutzt und auch einem Tochterunternehmen zugeführt worden, das offensichtlich die geschützten personenbezogenen Halterdaten bereits in einer eigenen Datenbank zu allen möglichen Werbezwecken vorgehalten hatte und darüber hinaus für die Herstellung der (aufgedrängten) TÜV-Service Card zuständig war.

Hier wird deutlich, dass die rechtswidrige Nutzung der personenbezogenen Daten zu einem massiven Eingriff in das informationelle Selbstbestimmungsrecht der Betroffenen führte, da die TÜV-Gesellschaft sich deutlich über klar formulierte gesetzliche Regelungen hinweggesetzt hatte.

In Rheinland-Pfalz übt das Verkehrsministerium die staatliche Aufsicht über die Technische Prüfstelle aus. Sehr zeitnah hat dort eine Unterredung zu dem Thema mit sämtlichen Beteiligten stattgefunden. Als Ergebnis der Erörterungen wurde vereinbart, dass in Rheinland-Pfalz der Versand der TÜV-Service Card sowie des Werbeschreibens unverzüglich eingestellt wird. Darüber wurden auch die Datenschutzbeauftragten der anderen Bundesländer in Kenntnis gesetzt.

14.8 Tagesnachweis des Fahrlehrers

Ein Fahrlehrer hat sich mit folgendem Anliegen an den LfD gewandt:

Die für ihn zuständige untere Aufsichtsbehörde, eine Kreisverwaltung, verlange von ihm, dass er dem Fahrschüler den Tagesnachweis zur Bestätigung der Angaben nach § 18 Abs. 2 FahrlG vorlege. Hierbei könne der Fahrschüler jedoch nicht nur den gesamten Tagesverlauf des Fahrlehrers, sondern auch die Daten anderer Fahrschüler zur Kenntnis nehmen. Betroffen seien beispielsweise Nachschulungskurse von im Straßenverkehr auffällig gewordenen Kraftfahrern sowie Fahrstunden nach einem Führerscheinentzug.

Im Hinblick auf die Regelung des § 18 Abs. 2 FahrlG, wonach die Ausführungen des Fahrlehrers vom Fahrschüler auch „sonst bestätigt“ werden können, war es für den Petenten nicht nachvollziehbar, aus welchem Grunde der Fahrlehrer die entsprechende Bestätigung nicht auf dem persönlichen Ausbildungsnachweis vornehmen können soll.

Der LfD hat sowohl die Stellungnahme der Kreisverwaltung als auch des rheinland-pfälzischen Verkehrsministeriums als oberste Aufsichtsbehörde eingeholt.

Danach wurde insbesondere vorgetragen, dass die Formulierung im Gesetzestext, wonach der Fahrschüler die Ausbildung auch sonst bestätigen kann, sich gem. § 18 Abs. 2 Satz 3 FahrlG ausdrücklich auf die Bestätigung „im Tagesnachweis“ beziehe. In den Beratungen zum Gesetzentwurf sei dieser Zusatz ausschließlich mit dem Ziel aufgenommen worden, auch elektronische Möglichkeiten der Unterzeichnung durch den Fahrschüler zuzulassen (wie z. B. bei der Entgegennahme von Sendungen bei privaten Zustelldiensten). Der Nachweis der Gegenzeichnung durch den Fahrschüler im Tagesnachweis sei für die Fahrschulüberwachung nach § 33 FahrlG unentbehrlich. Dieser Argumentation, wonach die Unterschrift im Tagesnachweis nach der geschilderten Rechtslage zwingend ist, vermochte sich der LfD nicht zu verschließen, zumal in diesem Zusammenhang ergänzend darauf hinzuweisen war, dass die Bundesvereinigung der Fahrlehrerverbände von Anfang an sowohl bei der Konzeption zur Änderung des Fahrlehrerrechts beteiligt als auch im Umsetzungsausschuss und im „Münchener Arbeitskreis“ vertreten war. Wünsche der Fahrlehrer hinsichtlich der organisatorischen Umsetzung der fahrlehrerrechtlichen Vorschriften hätten in diesem Zusammenhang ausreichend berücksichtigt werden können.

Im Übrigen hat das Verkehrsministerium mitgeteilt, dass gegenwärtig bei der Bundesvereinigung der Fahrlehrerverbände eine Schablone erstellt wird, mit der die anderen, den Fahrschüler nicht betreffenden Angaben abgedeckt werden können. Damit würden aus der Sicht des LfD auch datenschutzrechtliche Belange berücksichtigt; denn eine Einsichtnahme des Fahrschülers in die einzelnen Tätigkeiten des Fahrlehrers wäre dann ausgeschlossen.

Fernerhin hat der LfD bezüglich der in der Eingabe geschilderten problematischen Verfahrensweise bei der Durchführung von Nachschulungskursen den – an den Petenten weitergeleiteten – Hinweis erhalten, dass dieser Bereich durch den Fahrlehrer grundsätzlich als Kursstunde ohne Nennung der Teilnehmer oder als „normale“ Fahrstunde in seinem Tagesnachweis verzeichnet wird. Eine namentliche Nennung des jeweils Geschulten, aus der Schlüsse auf dessen Verkehrsverstöße gezogen werden könnten, würde seitens der Aufsichtsbehörde als ein datenschutzrechtlicher Verstoß seitens des Fahrlehrers eingeordnet werden.

14.9 Identitätsausweis in Taxen?

In einigen Bundesländern wurden Überlegungen angestellt, für Taxifahrerinnen und Taxifahrer eine bußgeldbewehrte Pflicht einzuführen, bei der Fahrt ständig eine Identitätskarte offen sichtbar mitzuführen, auf der Name und Lichtbild der Fahrerin oder des Fahrers zu sehen sind. Die Verpflichtung, während der Berufsausübung ständig einen Ausweis mit Namen und Lichtbild bei sich zu tragen und für Dritte gut sichtbar im Innenraum der Taxen anzubringen, würde nach Auffassung des LfD einen erheblichen

Eingriff in das informationelle Selbstbestimmungsrecht der Fahrerinnen und Fahrer darstellen. Die Verordnungsermächtigung des Landesgesetzgebers in § 47 Abs. 3 Satz 3 Nr. 3 Personenbeförderungsgesetz (PbefG) bietet nach seiner Auffassung keine ausreichende Rechtsgrundlage für derartige Einschränkungen des informationellen Selbstbestimmungsrechts.

Das rheinland-pfälzische Ministerium für Wirtschaft, Verkehr, Landwirtschaft und Weinbau hat mitgeteilt, dass dort Pläne hinsichtlich der Einführung eines Identitätsausweises für Taxifahrerinnen und -fahrer nicht bestehen. Ein entsprechendes Vorhaben würde man auch nicht mittragen. In diesem Zusammenhang werde allerdings eine Änderung der BO-Kraft in Erwägung gezogen. Danach soll über die Regelung in § 27 BO-Kraft hinaus im äußeren Bereich des Fahrzeugs, nämlich in das Taxischild, eine gut lesbare Kurzkennzeichnung integriert werden, über die z. B. den Fahrgästen auch nach dem Verlassen des Fahrzeugs die Möglichkeit von Beschwerden ermöglicht wird. Gegen diese Verfahrensweise wäre aus der Sicht des Datenschutzes nichts einzuwenden.

14.10 Das Parken und der Datenschutz

14.10.1 Parkerleichterungen für Schwerbehinderte

Den LfD erreichten Anfragen autofahrender schwer behinderter Personen, die es als diskriminierend empfanden, dass auf dem ihnen als „Sonderparkberechtigte“ ausgestellten Ausweis ihr Name bei einem Parkvorgang für jeden Passanten sichtbar aufgedruckt ist. Hier war darauf hinzuweisen, dass die Frage der praktischen Handhabung bei Parkerleichterungen für Schwerbehinderte bundeseinheitlich mit der Regelung zu den Formblattmustern für den Genehmigungsbescheid und den Ausweis nach § 46 StVO geklärt ist. Danach kann das Namensfeld auf Wunsch des Berechtigten freigelassen werden. In diesen Fällen wird der Name auf der Rückseite des Ausweises eingetragen. Die betroffenen ausweisausstellenden Behörden wurden entsprechend informiert.

14.10.2 Anwohnerparken

Mit den Berechtigungskriterien beim Anwohnerparken hatte sich der LfD aufgrund einer Eingabe zu befassen. Der Petent wandte sich gegen die nach seiner Auffassung unzulässige Datenerhebung im Rahmen des Antrags auf Erteilung einer Parkberechtigung. Insbesondere rügte er die geforderten Angaben zum Typ des Fahrzeugs und zur Fahrerlaubnis.

Bei der Ausstellung eines Anwohner-Parkausweises handelt es sich um einen begünstigenden Verwaltungsakt, der eine Sonderparkberechtigung begründet und als Nachweis dafür dient, dass der Inhaber zu dem begünstigten Personenkreis gehört und auf den dafür gekennzeichneten Flächen parken darf. Nach der Regelung in § 6 Abs. 1 Nr. 14 StVG i. V. m. § 45 Abs. 1 b Nr. 2 StVO kann die Straßenverkehrsbehörde Parkvorrechte schaffen. Ob und inwieweit für Anwohner reservierte Parkflächen zur Verfügung gestellt werden, steht im Ermessen der zuständigen Straßenverkehrsbehörde. Dieses Gestaltungsermessen umfasst auch die Befugnis, den begünstigten Personenkreis näher festzulegen. Üblicherweise werden im Zuge der Einführung der Parkraumbewirtschaftung vom jeweiligen Stadt- bzw. Gemeinderat Berechtigungskriterien festgelegt und beschlossen. Im vorliegenden Fall hat sich jedoch herausgestellt, dass ein diesbezüglicher Ratsbeschluss nicht vorlag. Die Erteilung einer Sonderparkberechtigung für Anwohner richtet sich daher nach der Regelung in Abschnitt IX, Ziffer 2 der Verwaltungsvorschrift zu § 45 Abs. 1 StVO. Danach muss das Kraftfahrzeug, für das eine Sonderparkberechtigung gewährt werden soll, auf den Anwohner als Halter zugelassen sein oder nachweislich vom Antragsteller dauernd genutzt werden. Da der Petent nach seinen Ausführungen Halter des entsprechenden Fahrzeugs war und damit berechtigte Person im Sinne vorgenannter Regelung, sind die Fragen nach dem Typ des Fahrzeugs und der Fahrerlaubnis aus Sicht des LfD keine Kriterien für die Erteilung des Anwohnerparkscheins. Auf dieser Grundlage stand der Erteilung einer Parkberechtigung für den Petenten nichts mehr im Wege.

14.10.3 Ausnahmegenehmigung für Soziale Dienste

Aufgrund der Anfrage einer Sozialstation wurde das Problem der Bekanntgabe des jeweils konkreten (straßen- und hausnummerbezogenen) Einsatzortes der Fahrzeuge dieser Einrichtung an den LfD herangetragen. Hier war es regelmäßig zu „Verwarnungen“ gekommen, wenn der Einsatzort nicht hausnummergenau hinter der Windschutzscheibe des Fahrzeugs angegeben wurde. Der LfD hat aus diesem Anlass das Verkehrsministerium um Mitteilung gebeten, ob Bedenken dagegen bestehen, den Hinweis auf den Einsatzort dergestalt zu umschreiben, dass eine Personenbeziehbarkeit (also die Angabe der vollständigen Adresse des von der Sozialstation Betreuten) vermieden wird. Im Verlauf der Korrespondenz stellte sich heraus, dass der Bund-Länder-Fachausschuss für den Straßenverkehr und die Verkehrspolizei zur Sicherung bundeseinheitlichen Verhaltens der Länder im Zusammenhang mit der Erteilung von entsprechenden Ausnahmegenehmigungen einheitliche Kriterien für Soziale Dienste festgelegt hat. Danach „können Sozialen Diensten (alle Einrichtungen, die im Rahmen der Pflegeversicherung tätig sind) und Personen, die zwingend für die Betreuung hilfsbedürftiger Personen auf ein Kraftfahrzeug angewiesen sind, Ausnahmegenehmigungen zum Parken für ein Fahrzeug eingeräumt werden, das am jeweiligen Einsatzort abgestellt werden muss. Um eventuellen Missbrauch zu verhindern, ist die Angabe des Einsatzortes für die örtlichen Ordnungsbehörden erforderlich.“

Nach Rückfrage des LfD hat sich herausgestellt, dass mit Angabe des Einsatzortes die „Straße“ ohne weitere Individualisierung (Hausnummer) gemeint ist. Damit war das Problem gelöst; denn eine datenschutzrelevante Personenbeziehbarkeit konnte nicht festgestellt werden.

15. Landwirtschaft, Weinbau und Forsten

15.1 Veröffentlichung der Namen von Futtermittelherstellern im Zuge von BSE

Anlässlich der Diskussion um BSE kam es auch zu der Frage, inwieweit der Datenschutz einer Veröffentlichung der Namen von Futtermittelherstellern entgegensteht, deren Produkte mit Tiermehl verunreinigt waren.

Datenschutzrecht schloss eine Datenübermittlung auf Anfrage der Presse nicht aus, wenn die entsprechenden Voraussetzungen – wie bei jeder Datenübermittlung – vorliegen. Dabei kam es hier auf eine Abwägung der betroffenen Interessen an. Bei der hier vorzunehmenden Abwägung des berechtigten Interesses der Öffentlichkeit an der Unterrichtung über die Hersteller überwog dieses jedenfalls dann, wenn eine Lieferung schädlich kontaminierter Futtermittel zweifelsfrei feststand.

15.2 Nutzung der Landwirtschaftlichen Betriebsdatenbank

An den LfD wurde die Frage herangetragen, ob die Daten der Landwirtschaftlichen Betriebsdatenbank zum Zweck der agrarstrukturellen Entwicklungsplanung und zur Vorbereitung und Durchführung von Bodenordnungsmaßnahmen (Flurbereinigung) verwendet werden dürfen. In der fraglichen EG-Verordnung heißt es zur Nutzung, dass die Mitgliedstaaten in allen geeigneten Fällen auf das Integrierte Verwaltungs- und Kontrollsystem (InVeKoS) zurückgreifen. Dieser Rückgriff beschränkt sich jedoch auf die Kontrollen der Erstanträge auf Inanspruchnahme einer Beihilferegelung und die aufeinander folgenden Zahlungsanträge. Diese Kontrollen sollen danach so durchgeführt werden, dass zuverlässig geprüft werden kann, ob die Beihilfevoraussetzungen vorliegen. Der Rückgriff auf InVeKoS dient danach ausschließlich Kontrollzwecken, nachdem Anträge auf Förderung gestellt worden sind. Es war daher nicht davon auszugehen, dass Daten der Landwirtschaftlichen Betriebsdatenbank für Zwecke agrarstruktureller Entwicklungsplanung und zur Vorbereitung und Durchführung von Bodenordnungsmaßnahmen verwendet werden durften.

Auch das Flurbereinigungsgesetz verweist nicht auf die Landwirtschaftliche Betriebsdatenbank, um Informationen für das Flurbereinigungsverfahren zu erhalten, sondern auf andere Quellen zur Datenermittlung. Da die Beteiligten hierbei anzuhören sind, haben sich die Betroffenen ohnehin mit der beabsichtigten Maßnahme auseinander zu setzen und müssen evtl. Angaben machen. Aufgrund der Vorgaben in den einschlägigen Verordnungen zur Begründung und Nutzung von InVeKoS, die die Nutzung auf reine Kontrollzwecke beschränken, hielt der LfD daher eine Nutzung für andere Zwecke ohne Einwilligung der Betroffenen aus datenschutzrechtlicher Sicht für unzulässig.

16. Statistik

16.1 Das Zensusvorbereitungsgesetz für eine registergestützte Volkszählung

Nachdem am 13. Juli 2001 der Bundesrat dem Entwurf eines Gesetzes zur Vorbereitung eines registergestützten Zensus (Zensusvorbereitungsgesetz; BGBl. I S. 1882) mit Stichtag 5. Dezember 2001 abschließend zugestimmt hat, laufen die Vorbereitungen zum Test eines registergestützten Zensus beim Statistischen Landesamt auf Hochtouren.

Diesmal muss sich die Bevölkerung zur Zählung nicht mehr auf den Weg in die jeweiligen Geburtsorte machen; sie muss auch keine Erhebungsbögen mehr ausfüllen, wie dies noch bei der Volkszählung 1987 der Fall war. Es soll auch ohne diese Lästigkeiten funktionieren. Der Königsweg heißt nun „Registergestützte Volkszählung". Bereits in den vergangenen Jahren wurde in Deutschland nach Wegen gesucht, bestehende Datenquellen für Volkszählungen zu nutzen, um die Kosten sowie die Belastung der Bürger zu reduzieren. Die Statistischen Ämter des Bundes und der Länder haben ein datenschutzverträgliches Modell entwickelt, das die Nutzung vorhandener Daten insbesondere aus den Melderegistern vorsieht.

Um nun herauszufinden, ob dieser neue Ansatz in der Praxis überhaupt tauglich ist, soll zunächst die Machbarkeit eines registergestützten Zensus überprüft werden. Ohne diese Erfahrungen im Rahmen eines Tests, so sagen übereinstimmend die Fachleute, ist ein funktionsfähiger registergestützter Zensus nicht realisierbar. Dieser Test erfordert ein eigenes Gesetz, weil z. B. die Gemeinden verpflichtet werden müssen, Einwohnerdaten an die Statistischen Ämter zu liefern (in Rheinland-Pfalz geschieht dies über das DIZ), und auch Auskunftspflichten der betroffenen Einwohnerinnen und Einwohner begründet werden müssen.

Aus den Melderegistern von maximal 570 Gemeinden Deutschlands werden Daten von Einwohnern ausgewählter Gebäude (maximal 38 000) herangezogen. In Rheinland-Pfalz sind 58 Gemeinden mit rund 3 200 Gebäuden beteiligt. In einer Unterstichprobe in bundesweit 230 Gemeinden mit rund 16 000 Gebäuden sollen die statistischen Verfahren, die beim registergestützten Zensus vorgesehen sind, optimiert werden. In Rheinland-Pfalz fallen 20 Gemeinden mit rund 1 200 Gebäuden in diese Unterstichprobe.

Der Test ist in drei Teile untergliedert: Teil 1 besteht aus der sog. Dublettenprüfung. Dafür liefern sämtliche Meldebehörden in der Bundesrepublik Deutschland die Datensätze von Personen aller Geburtsjahrgänge, die am 1. Januar, 15. Mai und 1. September geboren sind. Diese Stichprobenprüfung läuft beim Statistischen Bundesamt zusammen und soll jene Fehler im Meldeverfahren aufdecken, die zu mehrfachen Hauptwohnungsmeldungen geführt haben. Im zweiten und dritten Teil der Testerhebung werden die Daten der Einwohnermelderegister in ausgewählten Gemeinden und Gebäuden mit schriftlichen Befragungen bei den Bewohnern dieser Gebäude und bei den Eigentümern verglichen, um so Erkenntnisse über Fehlbestände in den Registern zu erhalten.

Datenschutzrechtliche Belange wurden seitens der Datenschutzbeauftragten des Bundes und der Länder bereits in einem frühen Entwurfsstadium des Gesetzes eingebracht und werden bei der Erprobung des Alternativkonzepts entsprechend den Vorgaben des Bundesverfassungsgerichts aus seinem Volkszählungsurteil berücksichtigt. So werden alle für die Testuntersuchungen erforderlichen personenbezogenen Daten von den (auf das Statistikgeheimnis verpflichteten) Statistischen Landesämtern und dem Statistischen Bundesamt erhoben und verarbeitet. Alle Einzeldaten verbleiben ausschließlich in besonders geschützten Bereichen der statistischen Ämter und fallen unter die statistische Geheimhaltung. Dort werden die Hilfsmerkmale, wie beispielsweise Name und Anschrift, sobald wie möglich wieder gelöscht. Die Datenüberprüfungen und -berichtigungen im Rahmen der methodischen Untersuchungen erfolgen ebenfalls ausschließlich in den statistischen Ämtern. Rückmeldungen von den statistischen Ämtern an die registerführenden Verwaltungsbehörden, welche die Daten geliefert haben, erfolgen nicht, weil sie nach den Regelungen des Testgesetzes unzulässig sind.

Als Testergebnis gibt es also die denkbaren Alternativen „Statistiktauglichkeit der Register“ oder „Statistikuntauglichkeit der Register“. Für Rheinland-Pfalz ist nach allen Prognosen davon auszugehen, dass die Register statistiktauglich sind und eine registergestützte Zählung Daten von ähnlicher Qualität liefern wird wie eine primärstatistische Vollerhebung.

16.2 Nutzung personenbezogener Daten zur Erarbeitung einer Statistik für den zweiten Versorgungsbericht der Bundesregierung

Mit dem Gesetz zur Neuordnung der Versorgungsabschläge wurde § 62 a BeamtVG („Mitteilungspflicht für den Versorgungsbericht“) eingefügt. Damit sollte eine bereichsspezifische Ermächtigungsgrundlage im Beamtenversorungsgesetz für die Erhebung von Daten bei Personalstellen des Bundes und der Länder (einschließlich der Gemeinden) geschaffen werden, die zur Erstellung des von der Bundesregierung regelmäßig vorzulegenden Versorgungsberichtes benötigt werden. Das Finanzministerium hat den Landesbeauftragten für den Datenschutz um Äußerung gebeten, ob gegen die Wiederaufnahme der zwischenzeitlich ausgesetzten Versendung der Erhebungsvordrucke Bedenken bestehen. Der LfD nahm wie folgt Stellung:

Der durch Artikel 1 des Gesetzes zur Neuordnung der Versorgungsabschläge vom 19. Dezember 2000 als bereichsspezifische Ermächtigungsgrundlage für die Datenerhebung und -übermittlung eingefügte § 62 a BeamtVG ist hinsichtlich des Eingriffsumfangs in das Grundrecht auf informationelle Selbstbestimmung weder bestimmt noch normenklar (vgl. BVerfGE 65,1,44). Bei Statistikgesetzen ist es aus verfassungsrechtlichen Gründen Standard, dass sämtliche Merkmale, aus denen sich das Erhebungsprogramm zusammensetzt, aufgelistet werden. Das gilt auch dann, wenn es sich – wie hier – um eine Statistik im Verwaltungsvollzug (wie z. B. das Hochschulstatistikgesetz) handelt. Hinzu kommt, dass Satz 2 des § 62 a BeamtVG im Unterschied zu Satz 1 keine Übermittlungs-, sondern (lediglich) eine Erhebungsbefugnis enthält. Damit ist jedoch gerade im Anwendungsbereich des Arztgeheimnisses, in welchen erklärtermaßen die Standardfälle des Tatbestandes des Satzes 2 fallen sollen, noch in keiner Weise entschieden, dass die betreffende „Stelle“, bei der angefragt wird, auch übermitteln dürfte.

Angesichts dieser Problemlage könnte eine Lösungsmöglichkeit darin bestehen, die benötigten Daten bei der datenerhebenden/datenspeichernden Stelle auszuwerten und so zusammenzustellen, dass Rückschlüsse auf einzelne Betroffene nicht möglich sind. Damit würde auch dem Problem begegnet, dass bei der Erhebung in Einzelfällen eine Deanonymisierung mit einem gewissen Zusatzwissen nicht zuverlässig ausgeschlossen werden kann. Dieser Personenbezug ist beispielsweise denkbar in Bereichen mit geringen Betroffenenzahlen (z. B. Richter).

Daher sollte aus der Sicht des Datenschutzes bei diesem Sachstand eine Beteiligung an der Datensammlung unterbleiben.

16.3 Umfrage gem. § 7 Statistikregistergesetz

Im Zusammenhang mit dem Aufbau eines Unternehmensregisters für statistische Verwendungszwecke kam es vermehrt zu Anfragen Betroffener, nachdem das Statistische Landesamt entsprechende Fragebögen versandt hatte. Sie hielten die darin geforderten Informationen für datenschutzrechtlich bedenklich, insbesondere die Fragen nach der IHK-Mitgliedsnummer und der Betriebsnummer bei der Bundesanstalt für Arbeit. Der LfD hat wie folgt geantwortet:

Nach der Verordnung des Rates vom 22. Juli 1993 über die innergemeinschaftliche Koordinierung des Aufbaus von Unternehmensregistern für statistische Verwendungszwecke – VO-Nr. 2186/93 – (ABl. EG-Nr. L 196, S. 1) sind die Mitgliedstaaten der Europäischen Union verpflichtet, Unternehmensregister für statistische Verwendungszwecke (Statistikregister) aufzubauen und zu führen. Da die für das Unternehmensregister benötigten Informationen nicht in ausreichendem Maße aus vorhandenem statistischen Datenmaterial übernommen werden konnten, waren Rechtsvorschriften erforderlich, um die Lieferung von Daten aus administrativen Registern und Dateien zur Aufnahme in das Unternehmensregister zu ermöglichen. Das Statistikregistergesetz regelt daher im Wesentlichen die Übermittlung von Informationen aus den Dateien der Finanzverwaltung, der Bundesanstalt für Arbeit, der Industrie- und Handelskammern sowie der Handwerkskammern an die statistischen Ämter. Im Zusammenhang mit dem europaweiten Aufbau von Unternehmensregistern für statistische Verwendungszwecke hat das Statistische Landesamt Anfang Juli 2000 an zahlreiche rheinland-pfälzische Unternehmen und Betriebe einen Erhebungsbogen versandt, in dem nach den Identifikationsnummern der betreffenden Firmen in den Dateien der Finanzverwaltung, der Bundesanstalt für Arbeit, der Industrie- und Handelskammern sowie der Handwerkskammern gefragt wird. Diese Identifikationsnummern werden für den endgültigen Aufbau und anschließend für die laufende Pflege des Unternehmensregisters benötigt. Der Kreis der von der Registerumfrage

Betroffenen erstreckt sich auf jene wirtschaftlich tätigen Einheiten, für die im Rahmen eines vorausgegangenen umfassenden Abgleichs zwischen dem statistischen Register und den Verwaltungsdateien (Stammdaten der Finanzbehörden, der Bundesanstalt für Arbeit, der Industrie- und Handelskammern und der Handwerkskammern) keine Zuordnung über Name und Anschrift getroffen werden konnte. Dies ergibt sich aus Blatt 3 der zur Verfügung gestellten Unterlagen des Statistischen Landesamtes („Zweck der Registerumfrage").

Zu dem von den Petenten angesprochenen Bereich der BfA-Daten hat der LfD mitgeteilt, dass im Entwurf zum Statistikregistergesetz die Befugnis der statistischen Ämter vorgesehen war, der Bundesanstalt für Arbeit aktualisierte Einzelangaben über Unternehmen rückübermitteln zu dürfen. Auf diese Weise sollte die dort zu Zwecken des Verwaltungsvollzugs geführte Betriebsdatei ebenfalls auf den jeweils neuesten Stand gebracht werden. Dies hätte allerdings einen Verstoß gegen den Grundsatz der Trennung von Statistik und Verwaltung bedeutet. Die Datenschutzbeauftragten von Bund und Ländern hatten deshalb auf diese Problematik aufmerksam gemacht. Daraufhin konnte eine Verbesserung erreicht werden. Nunmehr ist in § 3 Abs. 2 StatRegG geregelt, dass die hier in Rede stehenden Rückübermittlungen „ausschließlich für statistische Zwecke in den abgeschotteten Bereich der Bundesanstalt für Arbeit" zu erfolgen haben.

Was die IHK-Daten anbelangt, so war darauf hinzuweisen, dass insbesondere im Hinblick auf die Steuernummer problematisiert wurde, ob die Industrie- und Handelskammern dieses Datum ihrer Kammerzugehörigen den statistischen Ämtern übermitteln dürfen, so wie es nach § 4 StatRegG vorgeschrieben ist. Zwar darf die Steuernummer von den Kammern grundsätzlich nur für Zwecke der Beitragsfestsetzung gespeichert und genutzt werden; allerdings ist die Zweckänderung durch das Statistikregistergesetz ausdrücklich bestimmt und damit zulässig. Eine zusätzliche Regelung im IHK-Gesetz, wie sie etwa § 113 Abs. 2 Satz 8 der HandwerksO vorsieht, nach der die Handwerkskammern die Steuernummer an die statistischen Ämter zum Aufbau und zur Führung des Statistikregisters übermitteln dürfen, ist aus Sicht des LfD nicht erforderlich. Die Industrie- und Handelskammern sind nach § 9 Abs. 3 Satz 2 IHK-Gesetz berechtigt – nach dem Statistikregistergesetz sogar verpflichtet –, die Steuernummer zu übermitteln; soweit damit eine Offenbarung des Steuergeheimnisses verbunden ist, sind sie hierzu nach § 30 Abs. 4 Nr. 2 AO befugt.

Nach allem waren gegen die mit der Registerumfrage einhergehenden Übermittlungen keine durchgreifenden datenschutzrechtlichen Bedenken geltend zu machen.

17. Personaldatenverarbeitung

17.1 Multifunktionskarte für Bedienstete

Unter Tz. 8.2.7 und im 16. Tb. (Tz. 8.2.5) wurde über die Einführung der Multifunktionskarte für Studierende der Universität Trier (TUNIKA) und der Universität Koblenz-Landau berichtet. Auch die Bediensteten der Universität sollten in der Folgezeit mit einer Chipkarte als Dienstausweis mit Zusatzfunktionen ausgestattet werden. Im Bereich der Polizei wurden im Berichtszeitraum die klassischen grünen Papier-Dienstausweise durch Chipkarten ersetzt.

Die Chipkartenausweise können neben dem Identitätsnachweis über vielfältige Zusatzfunktionen verfügen, wie etwa Zutrittsberechtigung zu Gebäuden, Arbeitszeiterfassung, Authentifikation gegenüber Servern oder Zahlungsmittel. Auch als Instrument für digitale Signatur und Verschlüsselung kommen Chipkarten in Betracht. Es liegt auf der Hand, dass die Kontrollmöglichkeiten des Arbeitgebers/Dienstherrn durch den Einsatz von Chipkarten erleichtert werden, was insbesondere bei der Verknüpfung unterschiedlicher Funktionen unter dem Gesichtspunkt des Mitarbeiterdatenschutzes problematisch werden kann. So könnte sich der Arbeitgeber/Dienstherr etwa mittels Zeiterfassungs- und Zutrittsdaten ein Bewegungsprofil seiner Mitarbeiter erstellen.

Es ist zu begrüßen, dass im Rahmen der Novellierung des Landesdatenschutzgesetzes auch eine Vorschrift zum Einsatz von Chipkarten aufgenommen werden soll, in der Zulässigkeit, Verpflichtungen der verantwortlichen Stelle und die Rechte der Betroffenen gesetzlich geregelt werden. Bis zum In-Kraft-Treten der Regelung sollten in einer Dienstvereinbarung mit dem Personalrat die einzelnen Zusatzfunktionen der Karte, beteiligte Stellen, Löschungsfristen, Einsichtsrechte und die Zulässigkeit von Auswertungen verbindlich festgelegt werden.

17.2 Outsourcing im Bereich der Beihilfe

In einer an die Behörde des LfD gerichteten Eingabe wurde erneut die Übertragung der Beihilfeberechnung durch Kommunen auf externe Stellen durch den Beitritt zu einer sog. Beihilfespitzenversicherung problematisiert.

Datenschutzrechtlich hängt die Zulässigkeit dieser Form des „Outsourcings" davon ab, ob die Aufgabe insgesamt, einschließlich der Ausschöpfung zu treffender Ermessensspielräume und Entscheidungskompetenzen, auf den Auftragnehmer übergehen soll (dann Funktionsübertragung) oder ob von diesem bloß untergeordnete Hilfstätigkeiten der Datenverarbeitung wahrgenommen werden (dann Datenverarbeitung im Auftrag, § 4 LDSG).

Diese Abgrenzung kann im Einzelfall jedoch Schwierigkeiten bereiten. Örtliche Feststellungen im kommunalen Bereich haben ergeben, dass sich die Tätigkeit der Kommunen oftmals auf das bloße Entgegennehmen und Weiterreichen der Beihilfeanträge beschränkt und die Aufgabe der Beihilfebearbeitung faktisch nicht mehr von den Behörden wahrgenommen werden kann. Gerade dies ist jedoch ein wesentliches Unterscheidungskriterium zur Funktionsübertragung, die nur auf der Basis einer gesetzlichen Grundlage zulässig wäre.

Die Auslagerung der Beihilfebearbeitung durch den Beitritt zu Beihilfeversicherungen stellt für Kommunen zweifellos eine wirtschaftlich sinnvolle Alternative zur Wahrnehmung der Aufgabe in eigener Zuständigkeit dar. Auch für die betroffenen Beihilfeberechtigten können sich datenschutzrechtlich Vorteile ergeben. So kann die mit der Auslagerung einhergehende Anonymität zwischen Antragsteller und Sachbearbeiter durchaus auch im Interesse des Betroffenen sein, da der vom Gesetzgeber geforderten Abschottung der Beihilfedaten von anderen Personaldaten (§ 102 a S. 2 und 3 LBG) bei dieser Verfahrensweise in besonderem Maße Rechnung getragen wird. Erfahrungsgemäß ist diese Abschottung gerade in kleineren Behörden nur schwer zu realisieren.

Einschränkungen ergeben sich jedoch dann, wenn die Beihilfebearbeitung durch nicht öffentliche Stellen erfolgen soll:

Die Beachtung der datenschutzrechtlichen Bestimmungen durch den Auftragnehmer einschließlich der Duldung der Kontrolle durch den LfD kann in diesen Fällen lediglich vertraglich zugesichert werden (§ 4 Abs. 1 LDSG). Auch dürfte das durch arbeitsvertragliche Sanktionen zu erreichende Schutzniveau bei einem privaten Auftragnehmer deutlich geringer sein. Weiterhin ist zu beachten, dass durch entsprechende vertragliche Vereinbarungen, ggf. auch gegen den ausdrücklichen Willen des Betroffenen, Personen außerhalb des öffentlichen Bereichs, die nicht zum gesetzlich zulässigen Empfängerkreis von Personaldaten gehören, Kenntnis von besonders sensiblen Informationen erhalten.

In diesem Zusammenhang ist auch die Regelung des § 4 Abs. 4 LDSG zu sehen, die bei Berufs- oder besonderen Amtsgeheimnissen, die sich auch auf Beihilfedaten erstrecken, ein grundsätzliches Verbot der Auftragsdatenverarbeitung durch nicht öffentliche Stellen beinhaltet.

Aus diesen Gründen sollte die Bearbeitung der Beihilfeangelegenheiten nach Auffassung des LfD grundsätzlich nur durch andere öffentliche Stellen (z. B. kommunale Beihilfe- oder Versorgungskassen, Zweckverbände) oder – wie dies bei der Pfälzischen Pensionsanstalt bislang auch der Fall ist – durch dem öffentlichen Bereich nahe stehende Beihilfeversicherungen erfolgen, die ihrerseits der strafbewehrten Verschwiegenheitspflicht nach § 203 Abs. 1 Nr. 6 StGB unterliegen.

In Rechtsprechung und Literatur werden zur rechtlichen Einordnung und Zulässigkeit des Outsourcings im Bereich der Beihilfe unterschiedliche Auffassungen vertreten. Das hängt auch damit zusammen, dass entsprechende gesetzliche Vorgaben in Rheinland-Pfalz, wie auch in den meisten anderen Bundesländern, bislang nicht vorhanden sind.

Der LfD hat sich daher gegenüber dem Ministerium der Finanzen für die Schaffung von normenklaren Vorschriften für die Beihilfebearbeitung durch externe Stellen eingesetzt, um den bestehenden Rechtsunsicherheiten bei den Beihilfeberechtigten und den Kommunen hinsichtlich der Zulässigkeit des Outsourcings besser begegnen zu können. Das Ministerium hatte zwar zunächst mitgeteilt, dass bei der anstehenden Neufassung der Beihilfen-Zuständigkeitsverordnung eine Beihilfebearbeitung durch öffentlich-rechtliche Versorgungskassen für den kommunalen Bereich ausdrücklich ermöglicht werden solle, angesichts der in dieser Sache anhängigen Gerichtsverfahren und „gegenteiliger Tendenzen“ in verschiedenen Ländern werde dies jedoch nicht weiter verfolgt. Der LfD fand diese Argumente wenig überzeugend und hat sich daher erneut gegenüber dem Finanzministerium in dem o. g. Sinne eingesetzt.

17.3 Heimarbeitsplätze beim Medizinischen Dienst der Krankenversicherung

Als dem LfD bekannt geworden war, dass beim MDK Mitarbeiterinnen in Heimarbeit Pflegegutachten schreiben, wurden an mehreren Heimarbeitsplätzen örtliche Feststellungen zum Datenschutz getroffen. Die Anforderungen, die bei der Einführung von Heimarbeitsplätzen aus datenschutzrechtlicher Sicht zu beachten sind, wurden bereits im 17. Tb. (Tz. 17.3) ausführlich dargelegt.

Auch wenn das Schreiben von ärztlichen Gutachten (hier ausnahmslos Pflegegutachten) im Wege der Heimarbeit sowohl für die betroffenen Mitarbeiterinnen als auch für den MDK zweifelsohne mit Vorteilen verbunden ist, hat eine datenschutzrechtliche Prüfung auch die schutzwürdigen Interessen der betroffenen Patienten zu berücksichtigen, deren sensible medizinische Daten im Wege der Heimarbeit verarbeitet werden. Diese haben nämlich einen Anspruch darauf, dass mit der Auslagerung der Gutachtenerstellung, über die sie nicht einmal unterrichtet sind, keine – im Vergleich zur Datenverarbeitung in der MDK-Dienststelle – unverhältnismäßige Beeinträchtigung ihrer Datenschutzrechte verbunden ist.

Positiv festzustellen war, dass der MDK seinerseits bereits Maßnahmen zur Sicherstellung des Datenschutzes im Bereich der Heimarbeitsplätze ergriffen hatte. So wurden beispielsweise sämtliche Heimarbeitsplätze mit dienstlich bereitgestellten Systemen ausgestattet, die erstellten Gutachten werden wenige Tage nach Erstellung automatisch gelöscht und es besteht keine Möglichkeit, die Gutachten am Heimarbeitsplatz auszudrucken. Weiterhin wurden die Mitarbeiterinnen und Mitarbeiter vertraglich verpflichtet, keine nicht dienstliche Software zu installieren und Arbeitsplatzbegehungen auch durch Mitarbeiter des LfD zu gestatten.

Unabhängig hiervon stellt sich jedoch die Frage, ob und unter welchen Voraussetzungen angesichts der Sensibilität der Daten eine Verarbeitung im Wege der Heimarbeit grundsätzlich als zulässig zu bewerten ist. Nach Auffassung des LfD kommt § 4 Abs. 4 Satz 2 LDSG entsprechend zur Anwendung, so dass wegen entgegenstehender schutzwürdiger Interessen der Betroffenen die Verarbeitung personenbezogener Daten, die der ärztlichen Schweigepflicht unterliegen, im Wege der Heimarbeit grundsätzlich nicht in Betracht kommt. Aus diesem Grunde ist eine pseudonymisierte Datenverarbeitung am Heimarbeitsplatz anzustreben.

Wie die örtlichen Feststellungen ergeben haben, ist dies – wenn auch mit einem gewissen Aufwand – durchaus zu bewerkstelligen. Auf die vollständige Nennung des Patientennamens könnte beim Diktat künftig verzichtet und stattdessen ein Pseudonym gebildet werden. Auch ist es in aller Regel nicht erforderlich, für das Schreiben der Gutachten die MDK-Akten am Heimarbeitsplatz zur Verfügung zu haben, so dass diese in der MDK-Dienststelle verbleiben könnten. Weiterhin ist eine Anpassung der MDK-Software MEDIKOS dergestalt möglich, dass die Heimarbeiterinnen beim Zugriff auf die Patientendatenbank das zu erstellende Gutachten auch ohne Namensangabe der betreffenden Person eindeutig zuordnen können. Eine abschließende Stellungnahme des MDK lag im Berichtszeitraum noch nicht vor. Angesichts der gewonnenen Erkenntnisse wird sich der LfD mit den ihm zur Verfügung stehenden Möglichkeiten nachhaltig für eine pseudonymisierte Datenverarbeitung am Heimarbeitsplatz einsetzen.

17.4 Datenschutzfragen im Zusammenhang mit der Internet- und E-Mail-Nutzung durch Bedienstete

Der zunehmende Einsatz der Informationstechnologie im Bereich der öffentlichen Verwaltung führte zu zahlreichen Anfragen beim LfD. Unter dem Gesichtspunkt des Mitarbeiterdatenschutzes ist im Bereich der Internet- und E-Mail-Nutzung – wie bei der Telefondatenerfassung auch – zwischen dienstlicher und privater Nutzung zu unterscheiden.

Ist nur die dienstliche Nutzung des Internets oder der E-Mail-Kommunikation erlaubt, findet in Bezug auf die Erhebung, Verarbeitung und Nutzung personenbezogener Mitarbeiterdaten allgemeines Datenschutzrecht Anwendung. Benutzeraktivitäten dürfen im Rahmen der Durchführung von technisch-organisatorischen Datenschutzmaßnahmen nach § 9 Abs. 2 LDSG protokolliert werden. Die Löschungsvorschriften des Teledienstedatenschutzgesetzes finden keine Anwendung, weil sie nur im Verhältnis der Anbieter von Telediensten zu den Nutzern gelten. Vorliegend handelt es sich dagegen um die Frage, welche Daten die nutzende Stelle selbst im Verhältnis zu ihren Mitarbeitern speichern darf. Diese Frage wird durch das Medienrecht nicht geregelt.

Im Zusammenhang mit der Nutzung des Internets begegnet daher die Protokollierung des Benutzernamens, der aufgerufenen Seiten, des Datums und der Uhrzeit des Aufrufs sowie des Umfangs der Nutzung keinen datenschutzrechtlichen Bedenken. Ausgehende dienstliche E-Mails sind gem. § 9 Abs. 2 Ziff. 6 LDSG auch in Bezug auf deren Inhalte elektronisch zu protokollieren, sofern diese nicht in ausgedruckter Form zu den Akten genommen werden.

Die erfassten Protokolldaten dürfen nach § 13 Abs. 5 und § 31 Abs. 5 LDSG grundsätzlich nur zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage und somit nicht zu Zwecken der Verhaltens- oder Leistungskontrolle genutzt werden. Eine stichprobenweise Überprüfung des Arbeitgebers/Dienstherrn, ob sich die Internet- bzw. E-Mail-Nutzung im Rahmen des dienstlich Zugelassenen bewegt, ist damit jedoch nicht ausgeschlossen. Im Rahmen der Novellierung des Landesdatenschutzgesetzes ist eine entsprechende Klarstellung in § 31 Abs. 5 LDSG vorgesehen.

Da die Protokollierung von Nutzeraktivitäten darüber hinaus jedoch nach § 80 Abs. 2 LPersVG mitbestimmungspflichtig ist, hängt die Zulässigkeit der Auswertung von Protokolldaten im konkreten Einzelfall entscheidend vom Ergebnis des Mitbestimmungsverfahrens ab. Aus datenschutzrechtlicher Sicht ist der Abschluss einer Dienstvereinbarung, die analog zur Telefondatenerfassung Regelungen zur Speicherung und Nutzung der erfassten Daten beinhaltet, sicherlich wünschenswert.

Die Situation stellt sich jedoch dann anders dar, wenn auch die private Internet-Nutzung oder E-Mail-Kommunikation zugelassen ist. In diesem Fall liegt zwischen Arbeitgeber/Dienstherrn und Bediensteten ein Anbieter-Nutzer-Verhältnis im Sinne der sog. Multimedia-Vorschriften (Teledienstegesetz, Teledienstedatenschutzgesetz und Mediendienste-Staatsvertrag) vor. Der Arbeitgeber/Dienstherr hat als „Anbieter" grundsätzlich die sich aus dem Teledienstdatenschutzgestz ergebenden Pflichten (vgl. § 4 ff. TDDSG) sowie das Fernmeldegeheimnis nach Art. 10 GG und § 85 Abs. 1 TKG zu beachten.

Die insoweit unterschiedlichen rechtlichen Rahmenbedingunen erfordern daher nicht nur eine klare und eindeutige Regelung darüber, ob die private Internet- bzw. E-Mail-Nutzung zugelassen ist, sondern auch – falls dies der Fall ist – eine von der dienstlichen Nutzung getrennte Datenerfassung. Was bei der E-Mail-Nutzung durch die Vergabe einer separaten privaten E-Mail-Anschrift noch relativ einfach zu bewerkstelligen ist, stößt jedoch bei der Internet-Nutzung an seine Grenzen. Ist das private „Surfen" etwa während der Mittagspause unentgeltlich gestattet, müsste die Protokollierung für den entsprechenden Zeitraum zurückgefahren werden, was bei einer Gleitzeitregelung kaum zu realisieren sein dürfte.

Damit stellt sich die Frage, ob die Betroffenen auf der Basis einer Einwilligungserklärung auf die ihnen bei der Privatnutzung zustehenden Datenschutzrechte verzichten können. In der gegenwärtigen Fassung des § 5 Abs. 2 TDDSG wird die Verarbeitung und Nutzung von Bestandsdaten etwa für Werbe- oder Marktforschungszwecke unter Einwilligungsvorbehalt gestellt. Aufgrund dieser Regelung hatte der LfD in der Vergangenheit die Auffassung vertreten, dass eine weiter gehende Erhebung und Verarbeitung von Nutzungsdaten auch bei erfolgter Einwilligung unzulässig ist. Nach einem Gesetzesentwurf der Bundesregierung zum elektronischen Geschäftsverkehr (Bundestagsdrucksache 14/6098 vom 17. Mai 2001) soll § 5 Abs. 2 jedoch gestrichen werden. Es ist daher davon auszugehen, dass nach dem Willen des Gesetzgebers Bestands- und Nutzungsdaten auf der Basis einer nach § 3 Abs. 1 und 2 TDDSG-E erteilten Einwilligungserklärung des Nutzers auch über den Regelungsbereich des Teledienstedatenschutzgesetzes hinaus erhoben, verarbeitet und genutzt werden dürfen.

Dieser Verzicht kann auch konkludent durch Beachtung der vom Arbeitgeber/Dienstherrn vorgegebenen Bedingungen der Privatnutzung (Bsp.: private Internet-Nutzung nur außerhalb der Arbeitszeit; Kennzeichnung einer E-Mail als „privat") erfolgen. Erforderlich ist jedoch, dass die Nutzer vorher darüber unterrichtet worden sind, dass und in welchem Umfang eine Protokollierung der Internet- und E-Mail-Aktivitäten erfolgt und insoweit das Fernmeldegeheimnis eingeschränkt wird sowie sonstige Vorschriften zum Schutz des Nutzers nach dem Teledienstedatenschutzgesetz nicht zur Anwendung kommen. Weiterhin sind die Nutzer darüber zu unterrichten, unter welchen Voraussetzungen Protokolldaten ausgewertet und an Dritte übermittelt werden (vgl. § 3 Abs. 8 TDDSG-E). Aufgrund dieser Informationen kann der Mitarbeiter dann selbst darüber entscheiden, ob er unter diesen Voraussetzungen das Internet und die E-Mail-Kommunikation privat nutzen möchte oder nicht.

17.5 Aufbewahrung der Ergebnisse von Einstellungstests in der Personalakte

Die Fachhochschule für öffentliche Verwaltung – Fachbereich Polizei – beabsichtigte, die Einstellungstests bei der Polizei zu evaluieren. Der LfD wurde gebeten, sich insbesondere zu Fragen der Anonymisierung und der Anmeldung zum Datenschutzregister zu äußern. Die Beschäftigung mit der Thematik förderte dann zutage, dass in der Vergangenheit die Ergebnisse des mehrtätigen Auswahlverfahrens in recht ausführlicher Form zu den Personalakten der erfolgreichen Bewerber genommen wurden. Dies bezog sich beispielsweise auf das Diktat, den Aufsatz und die Protokolle über Gruppendiskussionen und Einzelgespräche.

Unterlagen über Einstellungstests sind jedoch nicht in Personalakten, sondern als Sachakte zu führen. Denn der Zweck des Auswahlverfahrens und der damit in Zusammenhang stehenden Datenerhebungen ist mit der Entscheidung über die Einstellung oder Ablehnung des Bewerbers erreicht. Da Personalentscheidungen auf der Grundlage der gesamten Personalakte getroffen werden, kann nicht ausgeschlossen werden, dass sich die weitere Aufbewahrung der Unterlagen in der Personalakte im Einzelfall für den Beamten nachteilig auswirken kann. Auch besteht die Gefahr, dass durch die Aufnahme von Gesprächsprotokollen Angaben über die religiöse, weltanschauliche oder politische Anschauung in unzulässiger Weise zum Gegenstand von Personalakten werden.

Das Innenministerium schloss sich dieser Rechtsauffassung an und sagte zu, dass künftig nur noch das Ergebnis des Einstellungstests zu den Personalakten genommen wird. Eine sofortige Bereinigung der Alt-Personalakten sei bei über 10 000 Akten allerdings nicht durchführbar. Es wurde Einvernehmen darüber erzielt, dass diese sukzessive anlassbezogen, also bspw. bei Abgabe der Personalakte an eine andere Dienststelle im Rahmen einer Versetzung, erfolgen soll.

Der LfD setzte sich im Rahmen der Novellierung des Landesdatenschutzgesetzes dafür ein, dass in § 31 LDSG eine gesetzliche Regelung aufgenommen wird, wonach die Weiterverarbeitung der bei ärztlichen oder psychologischen Untersuchungen und Tests erhobenen Daten nur mit schriftlicher Einwilligung des Betroffenen zulässig ist. Dem wurde in dem vorliegenden Gesetzentwurf Rechnung getragen.

17.6 Personaldatenschutz bei Mitarbeitergesprächen

In der Anfrage des Personalrats einer Kreissparkasse ging es um die datenschutzrechtlichen Aspekte bei sog. Rückkehrgesprächen. Diese Gespräche sollten nach der Hausmitteilung der Kreissparkasse mit Mitarbeiterinnen und Mitarbeitern geführt werden, die nach krankheitsbedingter Abwesenheit in den Dienst zurückkehren. In dem – wie es hieß – „ausführlichen" Gespräch sollten die Mitarbeiter u. a. den gegenwärtigen Gesundheitszustand und die Hintergründe der Erkrankung mitteilen. Der Inhalt des Gesprächs sollte dokumentiert, von den teilnehmenden Personen unterzeichnet und an die Personalabteilung weitergeleitet werden.

Dem Arbeitgeber ist es im Rahmen seiner Fürsorgepflicht zwar unbenommen, einzelne Mitarbeiter auf ihre Fehlzeiten und die damit einhergehende Mehrbelastung der Kolleginnen und Kollegen hinzuweisen. Datenschutzrechtlich relevant sind diese Gespräche jedoch insoweit, als die Mitarbeiter bei dieser Verfahrensweise gehalten sind, dem Arbeitgeber Auskunft über ihre Erkrankung zu geben und die Dokumentation des Gesprächs in die Personalakte aufgenommen werden soll.

Ein Arbeitnehmer ist aber – abgesehen bei Gesundheitsgefahren für Kollegen, etwa durch eine ansteckende Krankheit – nicht verpflichtet, dem Arbeitgeber Näheres über seine Erkrankung (z. B. Diagnose, Symptome, Ursachen) mitzuteilen. Dies ergibt sich aus den arbeits- und sozialrechtlichen Vorschriften zur Arbeitsunfähigkeitsbescheinigung, die die Weitergabe von Informationen über die Art der Erkrankung des Arbeitnehmers an den Arbeitgeber gerade nicht vorsehen. In einer Entscheidung des Arbeitsgerichts Mannheim (RDV 2000, 281 f.) weist das Gericht darauf hin, dass eine allgemeine Verpflichtung des Arbeitnehmers, den Arbeitgeber über die Art seiner Erkrankung zu unterrichten, nicht besteht. Beantwortet der Arbeitnehmer die Frage des Arbeitgebers nicht auf freiwilliger Basis, so hat der Arbeitgeber im Regelfall keinerlei rechtliche Möglichkeiten, dies durchzusetzen.

Bei Durchführung der Rückkehrgespräche ist der Arbeitnehmer daher u. a. darauf hinzuweisen, dass er zur Offenbarung über Art, Ausmaß und Hintergründe seiner Erkrankung weder verpflichtet ist noch seine Weigerung, Gesundheitsdaten gegenüber dem Arbeitgeber zu offenbaren, zu beruflichen Nachteilen führt.

Der Personalrat wurde in diesem Sinne unterrichtet. Er wurde auch darauf hingewiesen, dass die Dokumentation der Rückkehrgespräche ebenso wie Aufzeichnungen über sog. Mitarbeiter- oder Personalführungsgespräche, deren Ergebnisse in einer Zielvereinbarung festgehalten werden, aufgrund ihrer Zielsetzung (Verbesserung der Führungs- und Kooperationsbeziehungen zwischen Vorgesetztem und Mitarbeiter) kein zulässiger Gegenstand von Personalakten sind.

Nur in den Fällen, in denen das Gesprächsprotokoll gleichzeitig als Abmahnung oder sonstige schriftliche Missbilligung dienen soll, kommt eine Aufnahme in die jeweilige Personalakte des Mitarbeiters in Betracht.

Da die Vorschriften zum Personaldatenschutz keinerlei Aussagen über diese Form der Mitarbeitergespräche enthalten, wurde gegenüber dem Personalrat die Empfehlung ausgesprochen, Anlass der Gespräche sowie Inhalt und Aufbewahrungsdauer der Protokolle in einer Dienstanweisung oder Dienstvereinbarung zu regeln.

17.7 Datenschutz bei Konkurrentenklagen

Ein Petent hatte sich auf eine ausgeschriebene Stelle eines Amtsrats beworben. Die Dienststelle beabsichtigte, ihm die Stelle zu übertragen, und teilte dem Mitbewerber daher mit, dass dessen Bewerbung keine Berücksichtigung finden konnte. Der Mitbewerber versuchte im einstweiligen Rechtsschutzverfahren die Ernennung des Kollegen zu verhindern und begründete seinen Antrag u. a. mit der schlechteren Beurteilung des Petenten. Der LfD sollte nun zu der Frage Stellung nehmen, ob die personalaktenführende Stelle dem Mitbewerber zulässigerweise Informationen über die Beurteilung des Petenten mitteilen durfte.

Informationsweitergaben im Zusammenhang mit Einstellungs- bzw. Beförderungsverfahren sind vor dem Hintergrund der Rechtsprechung zur sog. beamtenrechtlichen Konkurrentenklage zu beurteilen: Da mit der Ernennung des erfolgreichen Bewerbers das Stellenbesetzungsverfahren abgeschlossen ist und eine anderweitige Besetzung der Stelle selbst dann, wenn sie frei werden sollte, erst in einem weiteren Verfahren nach einer erneuten Ausschreibung möglich ist, muss der unterlegene Bewerber im Wege des einstweiligen Rechtsschutzes bereits die Ernennung des Konkurrenten verhindern. Das Bundesverfassungsgericht hält daher den Dienstherrn für verpflichtet, den Beamten, dessen Bewerbung keinen Erfolg haben wird, vorab davon in Kenntnis zu setzen, damit er ggf. das Verwaltungsgericht wegen einer Verletzung des in Art. 33 Abs. 2 GG verbürgten Rechts auf gleichen Zugang zu jedem öffentlichen Amt nach Eignung, Befähigung und fachlicher Leistung anrufen kann (BVerfG NJW 1990, S. 501).

Dem unterlegenen Mitbewerber sind dabei nicht nur das Ergebnis, sondern auch die Gründe, die für die Auswahlentscheidung maßgeblich waren, mitzuteilen. Nur bei Kenntnis dieser Einzelinformationen ist dieser in der Lage, seinen durch Art. 19 Abs. 4 GG garantierten Anspruch auf effektiven Rechtsschutz, welcher auch die vorherige Prüfung der Erfolgsaussichten einer Klage beinhaltet, wahrzunehmen (vgl. VGH Kassel, NVwZ 1994, S. 398).

Die beamtenrechtlichen Vorschriften zum Personalaktenrecht (§§ 102 ff. LBG) stehen einer diesbezüglichen Informationsweitergabe nicht entgegen: Auskünfte aus einer Personalakte sind gem. § 102 d Abs. 2 S. 1 LBG auch ohne Einwilligung des Betroffenen zulässig, wenn der Schutz höherrangiger Interessen des Dritten die Auskunftserteilung erfordert. Vor dem Hintergrund der Rechtsprechung des Bundesverfassungsgerichtes zu Art. 33 Abs. 2 i. V. m. Art. 19 Abs. 4 GG sind höherrangige Drittinteressen im Konkurrentenstreit grundsätzlich anzunehmen.

Dieses Ergebnis ist aus datenschutzrechtlicher Sicht unbefriedigend: Die Persönlichkeitsrechte des betroffenen Beamten werden bei einer Weitergabe von Informationen, die dem Personalaktengeheimnis unterfallen, in erheblichem Maße beeinträchtigt. Zwar sieht § 102 d Abs. 2 S. 2 LBG aus Gründen der Transparenz vor, dass dem Beamten Inhalt und Empfänger der Auskunft schriftlich mitzuteilen sind; fraglich ist jedoch, ob das Verbot der Anfertigung von Kopien, wie dies in der o. g. Entscheidung des VGH Kassel gefordert wird, den Datenschutzinteressen des Betroffenen hinreichend Rechnung tragen kann. Die Kenntnisnahme sensibler Informationen wird dadurch genauso wenig ausgeschlossen, wie deren zweckwidrige Verwendung. Aus Sicht des LfD sollte daher eine Hinweispflicht der Dienststelle bestehen, dass von der erlangten Kenntnis nur in dem zur Einsicht oder Auskunft berechtigenden Umfang Gebrauch gemacht werden darf.

17.8 Gesamtübersicht über Krankheitstage

Ein Straßen- und Verkehrsamt hatte die ihm zugeordneten Straßenmeistereien aufgefordert, eine Gesamtübersicht der Krankheitstage aller Betriebsarbeiter zu übersenden. Vom LfD zum Hintergrund der Anforderung befragt, teilte das Straßen- und Verkehrsamt mit, dass es für den Bereich der Straßenwärter (Betriebsdienstarbeiter) personalverwaltende und personalaktenführende Behörde sei. Die Straßenmeistereien würden die Kranken- bzw. Urlaubskarteien in Form einer Personalnebenakte führen.

Das Führen als Nebenakte im Sinne des § 102 Abs. 2 Satz 3 LBG würde jedoch voraussetzen, dass hierin nur die Unterlagen enthalten sind, die sich auch in der Grund- oder Teilakte befinden, was hier gerade nicht der Fall war. Bei den Kranken- bzw. Urlaubskarteien dürfte es sich vielmehr – wie dies in der Verwaltungsvorschrift des Ministeriums des Innern und für Sport vom 25. August 1997 (Ziff. 1.4.4) vorgesehen ist – um Teilakten handeln (§ 102 Abs. 2 Satz 1 LBG).

An der rechtlichen Beurteilung der Datenweitergabe durch die Straßenmeistereien ändert dies jedoch nichts: Datenflüsse zwischen Neben- bzw. Teilakte und der Grundakte finden innerhalb ein und derselben Personalakte statt und haben daher keinerlei rechtliche Außenwirkung. Sofern das Führen einer Teilakte aus sachlichen Gründen erforderlich ist und die Informationsweitergabe für Zwecke der Personalverwaltung oder Personalwirtschaft erfolgt, ist die Weitergabe von Personalaktendaten als zulässig zu bewerten.

Da diese Voraussetzungen bei der Anforderung der Gesamtübersicht über die Krankheitstage aller Betriebsdienstarbeiter durch das Straßen- und Verkehrsamt vorlagen, war sie datenschutzrechtlich nicht zu beanstanden.

17.9 Mitarbeiterbefragung im Rahmen von Organisationsuntersuchungen

In einer Stadtverwaltung sollten nach dem Zufallsprinzip ausgewählte Mitarbeiter einem externen Unternehmen im Rahmen von Interviews u. a. folgende Fragen beantworten: „Was glauben Sie, wo werden Sie ganz persönlich in fünf Jahren sein? Gibt es Dinge, über die Sie sich für die Zukunft Sorgen machen? An wen müssten Sie sich wenden, um das Neueste zu erfahren? Was tun Sie, wenn sich jemand in Ihre Arbeit einmischt? Woran erkennt man einen Mitarbeiter der Stadtverwaltung?“ Zum Umgang mit Konflikten sollten die Betroffenen u. a. Aussagen darüber machen, welches die üblichen Konflikte seien, was aus Sicht der Betroffenen zu tun sei und „wer den Preis zu bezahlen habe“. Die Mitarbeiter wurden gebeten, ihre „offene und ehrliche Meinung“ zu sagen; alle Informationen würden „anonym“ und vertraulich behandelt.

Aus datenschutzrechtlicher Sicht ist bei Mitarbeiterbefragungen zwischen sog. Organisationsuntersuchungen und sonstigen Befragungen zu unterscheiden.

Organisationsuntersuchungen im eigentlichen Sinn haben die Prüfung zum Gegenstand, ob die Aufgaben der öffentlichen Verwaltung mit geringerem Personal- und Sachaufwand oder auf andere Weise wirksamer erfüllt werden können. Solche Organisations- und Arbeitsplatzuntersuchungen sind schon wegen des haushaltsrechtlichen Grundsatzes der Sparsamkeit und Wirtschaftlichkeit erforderlich und sinnvoll. Rechtsgrundlage solcher Datenerhebungen ist im Bereich der Beamten § 102 Abs. 4 LBG, im Arbeitnehmerbereich § 31 Abs. 1 LDSG. Die Mitwirkungspflicht der Beamten bzw. Arbeitnehmer ergibt sich aus der beamtenrechtlichen Gehorsamspflicht bzw. aus der individualrechtlichen Nebenpflicht aus dem Arbeitsvertrag (s. 16. Tb., Tz. 17.11).

Sonstige Mitarbeiterbefragungen, in deren Mittelpunkt die subjektive Bewertung des Arbeitsumfeldes steht und in denen ein Sachbezug (Analyse der Aufbau- und Ablauforganisation) fehlt, sind dagegen lediglich auf freiwilliger Basis zulässig.

Im vorliegenden Fall handelte es sich um eine reine Mitarbeiterbefragung. Zwar sollte durch die Analyse festgestellt werden, was in der Stadtverwaltung „gut läuft und was eventuell noch verbessert werden kann“. Hierzu wurden jedoch vorwiegend subjektive Einschätzungen der Betroffenen abgefragt. Solche Datenerhebungen betreffen zumindest teilweise den Kernbereich des informationellen Selbstbestimmungsrechtes und dürfen daher nur auf freiwilliger Basis erhoben werden.

Die Betroffenen waren insoweit gemäß den Anforderungen des § 4 Abs. 2 LDSG in schriftlicher Form auf die Freiwilligkeit der Beantwortung, die Folgen bei einer Nichtbeantwortung sowie darüber zu informieren, welche Daten in welcher Form an die Dienststellenleitung weitergegeben werden und wie die Daten insgesamt weiter verwendet werden (Bsp.: Auswertung durch die Beratungsfirma; Dauer der Speicherung).

Diese Unterrichtung setzte auch eine zutreffende Aussage darüber voraus, ob die Befragung tatsächlich anonymisiert erfolgt. Hiervon konnte aber nicht ausgegangen werden, denn die Mitarbeiter sollten die eigenen Arbeitsaufgaben schildern und angeben, wer ihnen einen eigenständigen Entscheidungsspielraum einräumt. Auch über Kontakte mit höheren Vorgesetzten, insbesondere dem Bürgermeister, sowie über die letzte Veränderung am Arbeitsplatz sollte berichtet werden. Hierdurch war ein Personenbezug herstellbar, auch wenn der Name des Bediensteten nicht erfasst wurde.

Es war allerdings von vornherein beabsichtigt, dass die Stadtverwaltung nur „aufbereitete Ergebnisse“ der Befragung – gemeint waren anonymisierte Daten – erhält. Um dies zu gewährleisten, wurden der behördliche Datenschutzbeauftragte und der Personalrat am Verfahren beteiligt. Da darüber hinaus die Betroffenen umfassend in dem o. g. Sinne unterrichtet wurden, konnte die Befragung letztlich datenschutzverträglich ausgestaltet werden.

18. Datenschutz im kommunalen Bereich

18.1 E-Government

Im Zuge der zunehmenden Nutzung des Internets als modernes Kommunikationsmedium zwischen Bürgern, Wirtschaft und Behörden konkretisieren sich auch immer mehr die Bestrebungen, das Erscheinungsbild der Verwaltung dem anzupassen und die internetfähigen Dienstleistungen elektronisch zur Verfügung zu stellen. Diese gemeinhin als „E-Government“ bezeichneten Projekte sind im Bereich der Bundes-, Landes- und Kommunalverwaltung von großer Bedeutung. Vorhaben wie die Multimedia-Initiative der rheinland-pfälzischen Landesregierung oder die Bundesinitiative „bund online 2005“ deuten an, in welche Richtung sich die öffentliche Verwaltung in den nächsten Jahren entwickeln wird.

Im Lande Rheinland-Pfalz sind bereits einige E-Government-Projekte ins Leben gerufen worden. Am spektakulärsten dürfte die im Dezember 2000 erfolgte fast komplette Ausstattung der Bürger der im Landkreis Birkenfeld gelegenen Gemeinde Oberhambach mit Computern gewesen sein. Dieses mit Unterstützung des Landes Rheinland-Pfalz und anderer Sponsoren finanzierte Pilotprojekt „Ein Dorf ist online“ führte gerade auch für die öffentliche Verwaltung zu einer starken Veränderung der bisherigen Gewohnheiten: Denn die Gemeindebewohner können seither auch ihre Rathaus-Geschäfte online via Internet und unter Einsatz digitaler Signaturkarten von zu Hause aus erledigen.

Im Landkreis Kaiserslautern wurde unter dem Arbeitstitel „Bauen online" die Kreisverwaltung als Baugenehmigungsbehörde in einem Workflowsystem mit allen Verbandsgemeinden sowie der Kataster-, Straßen- und Landwirtschaftsverwaltung vernetzt. Dieses Kreisdatennetz bildet die Grundlage für den Einsatz diverser einheitlicher mehrplatzfähiger Fachanwendungen. Der Bauantrag kann so elektronisch gestellt und bei allen Dienststellen gleichzeitig bearbeitet werden. Die Betroffenen, insbesondere der Architekt, können sich jederzeit über den aktuellen Bearbeitungsstand informieren und selbst eigene Anmerkungen einspielen. Noch für das Jahr 2001 ist die Aufnahme des Wirkbetriebs geplant.

In einem anderen Projekt, das im Landkreis Bitburg-Prüm durchgeführt wird, soll zwischen dem Kreisjugendamt und dem Familiengericht des Amtsgerichtes Bitburg ein Workflow-Management-System eingerichtet werden, um die Kommunikation zwischen diesen sensiblen Stellen im Interesse der Betroffenen schneller und effektiver zu gestalten. Das als „Elektronische Jugendakte Bitburg" bezeichnete Pilotprojekt hat insbesondere zum Ziel, den Aktenaustausch zwischen den beteiligten Behörden zu vereinfachen.

Darüber hinaus gewinnt die IT-gestützte Vorgangsbearbeitung und -verwaltung in den Landesbehörden zunehmend an Bedeutung. Zurzeit wird beispielsweise im Bereich der Mittelinstanzen die Einführung eines elektronischen Dokumentenmanagement-Systems projektiert, das im Hinblick auf eine künftige interaktive Verwaltung von nicht zu unterschätzender Bedeutung ist.

Die datenschutzrechtliche Begleitung der einzelnen Projekte, aber auch des Gesamtprozesses E-Government ist für den LfD eine der Herausforderungen der Zukunft. Vertraulichkeit der Kommunikation und Integrität der Daten, eine klar abgegrenzte Zugriffsrechteverwaltung, eine gründliche Durchforstung der bestehenden Formerfordernisse und der Einsatz der digitalen Signatur sind nur einige Stichworte in diesem Zusammenhang. Mit der Einrichtung einer Arbeitsgruppe zum Thema „E-Government" haben die Datenschutzbeauftragten des Bundes und der Länder mittlerweile einen ersten Schritt getan, über Landes- und Zuständigkeitsgrenzen hinweg sich in diesen Prozess einzubringen und bundesweit einheitliche datenschutzrechtliche Standards zu entwickeln. Auch wenn auf diesem Wege noch zahlreiche technische und finanzielle Hürden zu überwinden sein werden, sollten die Gesichtspunkte der Datensicherheit und des Grundrechtsschutzes auch bei einer auf moderner Technik basierenden Verwaltung nicht an Bedeutung verlieren.

18.2 Kommunale Videoüberwachung

Unter Zugrundelegung der Entschließung der 59. Konferenz der Datenschutzbeauftragten des Bundes und der Länder zu Risiken und Grenzen der Videoüberwachung (s. Anlage 13) hat der LfD in einer Presseerklärung vom 31. März 2000 Empfehlungen für eine datenschutzgerechte Ausgestaltung entsprechender Überwachungsmaßnahmen formuliert. Mit der demnächst zu erwartenden Novellierung des Landesdatenschutzgesetzes wird auch im Landesrecht die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen künftig gesetzlich geregelt sein.

Im Berichtszeitraum hatte der LfD wiederholt zum Einsatz von Videokameras zur Überwachung öffentlicher Flächen Stellung zu nehmen.

18.2.1 Videoüberwachung eines Dorfplatzes durch den Ortsbürgermeister

Aufgrund diverser Beschwerden aus dem Kreise der Anwohner, die sich gegen nächtliche Ruhestörungen, Eigentumsbeschädigungen und sonstige Belästigungen im Rathausbereich durch eine Gruppe von Jugendlichen richteten, griff der Bürgermeister einer Ortsgemeinde selbst zur Tat und überwachte von dem örtlichen Rathaus aus den davor liegenden Platz mit einer Videokamera. Vorherige Bemühungen der örtlichen Polizei bzw. des Ordnungsamtes hatten nicht den gewünschten Erfolg gebracht. Mit der sichtbar am Rathausbalkon angebrachten Videokamera konnte er die Verursacher des nächtlichen Treibens aufnehmen, identifizieren und zur Rede stellen. Die so angesprochenen Jugendlichen entschuldigten sich bei den Anwohnern und leisteten, um einer drohenden Strafanzeige zu entgehen, darüber hinaus noch gemeinnützige Arbeit.

Trotz des erfolgreichen Durchgreifens des Ortsbürgermeisters begegnete dessen Vorgehen rechtlichen Bedenken. Denn die Videoüberwachung durch öffentliche Stellen bedarf in jedem einzelnen Falle einer Rechtsgrundlage. Eine solche lag aber hier für den Ortsbürgermeister nicht vor: Bei der in Frage kommenden Regelung des § 25 a POG ist die in § 89 Abs. 1 POG enthaltene ausdrückliche und ausschließliche Kompetenzzuweisung zugunsten der Verbandsgemeindeverwaltung zu beachten, die für ein Tätigwerden der Ortsgemeindeverwaltung und damit des Ortsbürgermeisters nur im Falle einer Beauftragung durch die allgemeine Ordnungsbehörde Raum lässt. Eine solche hat aber nicht stattgefunden. Die dadurch resultierende Unzulässigkeit seines Handelns hätte der Ortsbürgermeister folglich durch eine vorherige Abstimmung mit der Verbandsgemeinde vermeiden können.

18.2.2 Videoüberwachung des Geldausgabeautomaten eines städtischen Sozialamtes

Auch im Bereich der Sozialämter bedient man sich zunehmend moderner Datenverarbeitungstechniken: So wird in einer Stadtverwaltung die Auszahlung der Sozialhilfe über einen Geldausgabeautomaten abgewickelt. Der Sozialhilfeempfänger erhält vom Mitarbeiter des Sozialamtes eine Chipkarte, die mit dem ihm zustehenden Geldbetrag „aufgeladen" worden ist. Der Sozialhilfeempfänger muss dann innerhalb eines bestimmten Zeitraumes den Betrag am Automaten abheben. Die Chipkarte wird dabei vom Automaten einbehalten und beim nächsten Zahlungstermin neu codiert. Trotz dieser Absicherungen wollte eine Stadtverwaltung

den Geldausgabeautomaten mit einer Videokamera überwachen lassen. Die Erforderlichkeit dieser Maßnahme wurde seitens der Stadtverwaltung mit folgendem Vorfall begründet: Offenbar hatte eine Aushilfsreinigungskraft zwei Kassenkarten entwendet und versucht, am Geldausgabeautomaten eine Auszahlung zu erreichen. Mit der Videokamera, so die Stadtverwaltung, hätte der Diebstahl möglicherweise aufgeklärt werden können.

Im Rahmen seiner datenschutzrechtlichen Bewertung wies der LfD darauf hin, dass der Einsatz von Videokameras durch einen Sozialleistungsträger regelmäßig mit der Erhebung von Sozialdaten einhergeht. Diese Erhebung ist nach den Vorschriften des Sozialgesetzbuchs jedoch nur dann zulässig, wenn die Kenntnis der Daten zur Erfüllung einer Aufgabe der erhebenden Stelle nach dem Sozialgesetzbuch erforderlich ist. Das bedeutet, dass bereits im Zeitpunkt der Datenerhebung die Zulässigkeitsvoraussetzung, also insbesondere die Erforderlichkeit der Aufzeichnung, gegeben sein muss. Genau dies war jedoch bei der von der Stadtverwaltung beabsichtigten Verfahrensweise äußerst fraglich: Über einen längeren Zeitraum wären Daten auch von Personen aufgezeichnet, mithin erhoben worden, welche den Geldausgabeautomaten zulässigerweise und ordnungsgemäß benutzen.
Weiterhin muss der Einsatz von Videokameras insgesamt dem Verhältnismäßigkeitsgrundsatz entsprechen. Der Eingriff in das informationelle Selbstbestimmungsrecht einer Vielzahl von völlig unbeteiligten Personen ist hierbei abzuwägen gegenüber dem Nutzen, welcher mit dem Einsatz verbunden sein könnte. Der LfD kam bei dieser Abwägung zu dem Ergebnis, dass ein einmaliger Vorfall, der im Übrigen zu keinem Schaden bei der Stadtverwaltung geführt hatte und durch einfache organisatorische Vorgaben (wie z. B. die Anweisung, die Kassenkarten nur in verschlossenen Behältnissen aufzubewahren) künftig erheblich erschwert werden kann, insgesamt einen Eingriff in grundrechtsrelevante Rechtspositionen einer Vielzahl von unbeteiligten Personen nicht rechtfertigt.

18.2.3 Videoüberwachung einer Feuerwache

In einem anderen Fall beabsichtigte die freiwillige Feuerwehr einer verbandsfreien Gemeinde den zeitweisen Einsatz einer Video- und Tonüberwachungsanlage in der eigenen Feuerwache. Nachdem es immer häufiger während der Durchführung von einzelnen Feuerwehreinsätzen zu Diebstählen aus der Gerätehalle gekommen war, wollte man nun die Täter auf diese Weise dingfest machen.

Im Ergebnis beurteilte der LfD den zeitweisen Einsatz der Videoüberwachungsanlage während des Feuerwehreinsatzes gestützt auf das allgemeine Hausrecht in Verbindung mit dem Verhältnismäßigkeitsprinzip für datenschutzrechtlich unbedenklich, sofern der Eigentumsschutz nicht in einer anderen die Persönlichkeitsrechte der Betroffenen weniger belastenden Weise gewährleistet werden kann, sich die Aufnahmen auf Bereiche beschränken, in denen sich die Feuerwehrangehörigen nicht regelmäßig aufhalten und alle von der Überwachung betroffenen Personen in geeigneter Form darauf hingewiesen werden.

Im Rahmen der Angemessenheitsprüfung war der Eingriff in die Rechte Dritter (Feuerwehrangehörige; Besucher) gegen den Erfolg der Maßnahmen abzuwägen. Dabei musste differenziert werden: Solange die Kameras lediglich Bereiche im Blick haben, in denen sich gewöhnlich keine Personen aufhalten (z. B. Treppenhaus, Lagerraum, Fahrzeughalle), war die Eingriffsintensität der Maßnahme relativ gering, da keine Verhaltensweisen von Betroffenen beobachtet werden konnten und zudem die von den Kameras aufgenommenen Bilder nicht aufgezeichnet werden sollten. Sie ähnelte einer direkten Beobachtung durch Überwachungspersonal. Dies war im Hinblick auf die damit erreichbare Verhinderung von Eigentumsverletzungen angemessen und somit auch hinzunehmen. Anders war jedoch die Aufnahme solcher Bereiche zu beurteilen, in denen sich die Betroffenen regelmäßig und nicht nur im Vorübergehen aufhalten (z. B. Küche, Aufenthalts-/Wartebereiche, Arbeitsräume). Hier wären insbesondere die Angehörigen der Feuerwehr einer dauerhaften Beobachtung ausgesetzt, die gravierend in die Persönlichkeitssphäre der Aufgenommenen eingreifen würde und in keinem Verhältnis zu dem verfolgten Ziel – Verhinderung von Eigentumsverletzungen bei der Feuerwehr – stünde. Die Überwachung derartiger Bereiche ist daher unangemessen und datenschutzrechtlich unzulässig.

Der zeitgleich beabsichtigte Einsatz einer Tonübertragungsanlage stellte nach Einschätzung des LfD einen Verstoß gegen das Verhältnismäßigkeitsprinzip dar. Denn angesichts der bereits geplanten Videoüberwachung fehlte es zu diesem Zeitpunkt an der Erforderlichkeit für einen weiteren Eingriff in die Persönlichkeitsrechte der betroffenen Personen. Dementsprechend verzichtete die Feuerwehr auf die geplante Tonüberwachung.

18.2.4 Videoüberwachung eines Friedhofs

Die Bedeutung des öffentlich-rechtlichen Hausrechtes im Zusammenhang mit der Durchführung kommunaler Videoüberwachungsmaßnahmen zeigte sich auch in folgendem Fall: Eine Ortsgemeinde wollte einen privaten Nachbarn mit der Videoüberwachung eines Grabes des örtlichen Friedhofs beauftragen. Hintergrund waren regelmäßige Verschmutzungen und Entwendungen von Grabschmuck auf einem bestimmten Grab. Bei der geplanten Überwachung ließ es sich nicht vermeiden, neben dem betroffenen Grab auch vier Nachbargräber aufzuzeichnen; die jeweiligen Aufnahmen sollten nur einen Tag gespeichert und anschließend überspielt werden.

Im Ergebnis hielt der LfD die beabsichtigte Aufzeichnung bei Einhaltung bestimmter Maßgaben für hinnehmbar. Maßgeblich für die Befugnis zur Vornahme von Überwachungsmaßnahmen ist – sofern keine konkreten Regelungen in der Friedhofssatzung enthalten sind – das dem allgemeinen Recht der öffentlichen Sachen zuzuordnende Hausrecht. Wie jeder Eigentümer hat auch die öffentliche Hand als Eigentümerin das Recht, alle angemessenen Maßnahmen zu ergreifen, um Störungen des ordnungsgemäßen

Gebrauchs der Sache zu verhindern. Allerdings ist dabei der allgemeine Grundsatz der Verhältnismäßigkeit zu beachten. Dies spielte im konkreten Fall deshalb eine entscheidende Rolle, weil mit den Aufnahmen auch völlig unbeteiligte Friedhofsbesucher erfasst und in ihrem Verhalten registriert worden wären. Die geplante Videoüberwachung hielt jedoch die Grenzen des Verhältnismäßigkeitsgrundsatzes ein. Das Aufzeichnen war insbesondere erforderlich, da im konkreten Fall kein milderes Mittel gleicher Effizienz zur Verfügung stand. Die denkbare Einschaltung von Aufsichtspersonen wäre erheblich aufwändiger und hätte überhaupt nur bei verdeckter Beobachtung einen annähernden Effekt erzielt. Trotz der damit verbundenen Rechtsbeeinträchtigung unbeteiligter Dritter war auch von der Angemessenheit der geplanten Überwachung auszugehen. Die strikte zeitliche und räumliche Begrenzung der beabsichtigten Maßnahme und die daraus resultierende nur eingeschränkte Beeinträchtigung der Rechte der unbeteiligten Friedhofsbesucher sprachen letztendlich angesichts der durch die Überwachung zu schützenden Rechtsgüter (Eigentum, Totenruhe etc.) für deren Angemessenheit. Nach Einschätzung des LfD war zudem auch die Beauftragung eines privaten Dritten mit der Durchführung der datenschutzrechtlich zulässigen Videoüberwachung unter gewissen Einschränkungen hinnehmbar. Der grundsätzlich mit der Einbeziehung von Privatpersonen zu besorgenden Verstärkung von Rechtsbeeinträchtigungen unbeteiligter Dritter kann nämlich durch entsprechende vertragliche Bindungen – z. B. schriftliche Fixierung der Pflichten im Hinblick auf Nutzung, Verwendung und Löschung der Daten – und eine Verpflichtung nach dem Verpflichtungsgesetz entgegengewirkt werden.

18.3 Stimmungsvoller Marktplatz

Anlässlich örtlicher Feststellungen in anderem Zusammenhang wurde in einer Gemeinde festgestellt, dass im Rathaus eine von außen als solche nur schwer erkennbare Webcam installiert war. Diese machte tagsüber halbstündlich ein Foto vom Marktplatz, das ins Internet eingestellt wurde. Außer dem aktuellen Bild konnte man auch die fünf vorherigen Bilder aufrufen. Das älteste Bild wurde jeweils vom aktuellen überschrieben. Mit den Fotografien sollte die Stimmung des Marktplatzes eingefangen werden. Wenn sich jedoch Personen zu diesen Zeiten nah genug bei der Kamera aufhielten, war nicht auszuschließen, dass sie auf dem Foto identifiziert werden konnten. Einen ausdrücklichen Hinweis auf die Kamera gab es nicht.

Sobald eine Person auf dem Foto identifiziert werden konnte, war § 22 KunsturhG verletzt. Danach dürfen Bildnisse nur mit Einwilligung des Abgebildeten verbreitet oder öffentlich zur Schau gestellt werden. Da der Betroffene hier von der Aufnahme nichts wusste, konnte er seine Einwilligung nicht, auch nicht konkludent, erklären. Im vorliegenden Fall bestand daher die Möglichkeit, entweder einen Hinweis auf das Fotografieren für die Vorbeigehenden rechtzeitig erkennbar anzubringen oder die Webcam so zu positionieren, dass zwar noch der Marktplatz fotografiert wurde, Personen aber nicht mehr erkennbar waren. Die Gemeinde hat sich für die letztere Möglichkeit entschieden: Die Kamera ist nunmehr so positioniert, dass einzelne Personen auf den Aufnahmen nicht mehr erkennbar sind.

18.4 Bürgerbüros

Mittlerweile hat sich in den Städten und Gemeinden des Landes die Einrichtung eines dem Bürger als Kontakt- und Anlaufstelle dienenden Bürgerbüros weitgehend etabliert. Eine Umfrage des LfD im Kreise der rheinland-pfälzischen Stadtverwaltungen ergab, dass zu Beginn des Jahres 2001 mehr als drei Viertel der befragten Städte ein solches Bürgerbüro eingerichtet haben oder in naher Zukunft planen.

Grundsätzlich begrüßt der LfD die im Zusammenhang mit der Einrichtung der Bürgerbüros verfolgten Ziele einer „Verwaltung der kurzen Wege". In Zeiten, in denen Dienstleistungen zunehmend in elektronischer Form angeboten werden, obliegt es gerade auch der öffentlichen Verwaltung, den Kontakt mit dem Bürger so transparent, effektiv und flexibel wie möglich zu gestalten. Allerdings müssen die Bürger auch im Bürgerbüro von der Vertraulichkeit der Kommunikation und einer sicheren, zweckgebundenen Verarbeitung ihrer Daten ausgehen dürfen.

Aus diesem Grunde ist schon bei der räumlichen Ausgestaltung der Bürgerbüros auf die Beseitigung von Mithörmöglichkeiten Dritter durch geeignete Schallschutzmaßnahmen und eine eindeutige Abgrenzung des Warte- vom Beratungsbereich zu achten. Es hat sich herausgestellt, dass bei den bereits eingerichteten Bürgerbüros noch einige Defizite bestehen. So waren beispielsweise die Bedienungsterminals räumlich sehr eng angeordnet oder der Wartebereich nicht eindeutig abgeteilt. Auch die aufgrund mangelhafter Organisation entstehenden beträchtlichen Wartezeiten mit der daraus resultierenden hohen Zahl an vor Ort wartenden Bürgern führten zu einer Situation, in der die Vertraulichkeit nicht ausreichend gewährleistet ist. Andererseits wird eine völlige Abgeschiedenheit in einem Großraumbüro mit vielen Bedienungsschaltern und einer Wartezone kaum zu erreichen sein. Deshalb sollte zusätzlich ein separater Raum zur Verfügung stehen, in dem die Bürger auf eigenen Wunsch ein vertrauliches Gespräch führen können. Hierauf ist deutlich hinzuweisen.

Im Hinblick auf die durch die Einrichtung zentraler Kontaktstellen mögliche Durchbrechung des auch innerhalb der Gemeindeverwaltung geltenden Prinzips der informationellen Gewaltenteilung ist je nach Sensibilität der zu verarbeitenden Daten besonderer Wert auf die freiwillige Inanspruchnahme der Bürgerbüros zu legen: So muss in besonders sensiblen Bereichen wie z. B. in Sozial- oder Steuerangelegenheiten dem Bürger schon im Hinblick auf die Kontaktaufnahme die Wahlmöglichkeit zwischen Bürgerbüro und Fachamt bleiben. Zumindest in den Bereichen mit besonderen Amtsgeheimnissen ist es darüber hinaus der Verwaltung aus den gleichen Gründen verwehrt, eine endgültige Sachbearbeitung in dem Bürgerbüro durchzuführen. In diesem Zusammenhang zeigten sich die bei vielen Städten ausgegebenen Sozial- oder Familienausweise als problematisch: In einigen Fällen wurde deren

Beantragung, Bearbeitung und Ausgabe ausschließlich im Bürgerbüro vorgenommen, wobei teilweise sogar noch Zugriffsbefugnisse aus dem Bürgerbüro auf im Sozialamt eingesetzte EDV-Programme eingeräumt waren. Sowohl diese ämterübergreifenden und äußerst sensible Verfahren betreffenden Zugriffsrechte als auch die fehlende Wahlmöglichkeit wurden seitens des LfD problematisiert und konnten einvernehmlich datenschutzgerecht gelöst werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in der Broschüre „Vom Bürgerbüro zum Internet" Empfehlungen zum Datenschutz für eine serviceorientierte Verwaltung zusammengefasst, in der u. a. auch die Gestaltung von Bürgerbüros thematisiert wird. Die Broschüre wurde den Kommunalverwaltungen des Landes zur Verfügung gestellt.

18.5 Veröffentlichungen auf kommunalen Homepages im Internet

Städte und Gemeinden nutzen zunehmend die sich durch das Internet bietenden Möglichkeiten und präsentieren sich über die lokalen Grenzen hinaus mit reichhaltigen Angeboten der weltweiten Internetgemeinde. Dass es dabei immer wieder zu datenschutzrechtlichen Problemen kommen kann, zeigen die zahlreichen im Berichtszeitraum hierzu durchgeführten Beratungen.

18.5.1 Privatadressen und Privattelefonnummern von Ratsmitgliedern

So stellte sich im Zusammenhang mit der Aktualisierung des eigenen Internet-Angebotes für eine Verbandsgemeinde die Frage, unter welchen Voraussetzungen die Veröffentlichung der Privatadressen und Privattelefonnummern von Ratsmitgliedern datenschutzrechtlich zulässig ist. Die Kommune gab zu bedenken, dass diese Daten bereits im Vorfeld der Kommunalwahlen bei der öffentlichen Bekanntmachung der Wahlvorschläge publiziert seien, so dass nach § 2 Abs. 5 LDSG wohl eine Anwendung des Landesdatenschutzgesetzes ausgeschlossen sei.

In seiner Stellungnahme hielt der LfD die internetgestützte Veröffentlichung der Privatadresse eines kommunalen Mandatsträgers durch die Verbandsgemeinde auf der Grundlage des § 5 Abs. 1 LDSG nur dann für datenschutzrechtlich zulässig, wenn die Betroffenen hierzu eingewilligt haben. Entgegen der Einschätzung der Verbandsgemeinde stand der Anwendung des Landesdatenschutzgesetzes § 2 Abs. 5 LDSG nichts entgegen, da die in das kommunale Internet-Angebot aufzunehmenden Daten selbst nicht direkt den öffentlich bekannt gemachten Wahlvorschlägen, sondern einer erst später erstellten gemeindeinternen und damit nicht allgemein zugänglichen Datenbank entnommen wurden. Da die Veröffentlichung personenbezogener Daten im Internet datenschutzrechtlich als Datenübermittlung an nicht öffentliche Stellen zu werten ist, kam § 16 LDSG als mögliche Rechtsgrundlage in Betracht. Dessen Voraussetzungen waren jedoch nicht gegeben. Ausschlaggebend war dabei u. a., dass der Veröffentlichung der Daten im Internet angesichts der weltweiten Zugriffsmöglichkeiten und des damit zusammenhängenden Gefährdungspotenzials überwiegende schutzwürdige Interessen der Betroffenen entgegenstehen und sie im Gegensatz zur Weiterverbreitung der dienstlichen Adressen und Telefonnummern auch nicht im öffentlichen Interesse liegt.

18.5.2 Privatadressen und Privattelefonnummern der Vorsitzenden örtlicher Vereine

Aus den gleichen Gründen ist auch bei der Veröffentlichung der privaten Anschriften und Telefonnummern der Vorsitzenden von örtlichen Vereinen auf der Homepage einer Gemeinde die Einholung einer entsprechenden Einwilligung unumgänglich. Dies gilt selbst dann, wenn die betreffenden Daten einer lediglich in Papierform vorhandenen Bürgerinformationsbroschüre entstammen und die Vereinsvorsitzenden dieser Veröffentlichung ausdrücklich zugestimmt hatten. Denn mit der Aufnahme der Adressdaten in das kommunale Internet-Angebot vergrößert sich der potenzielle Empfängerkreis gegenüber der nur lokal verbreiteten Bürgerinformationsbroschüre erheblich. Nur insoweit hatten die Betroffenen aber der Preisgabe ihrer Daten zugestimmt, so dass für die beabsichtigte internetgestützte Veröffentlichung die ursprünglich erteilte Einwilligung nicht mehr zugrunde gelegt werden konnte.

18.6 Einsicht in das Wählerverzeichnis

Schon seit geraumer Zeit beschäftigt die im Vorfeld von Bundestags-, Landtags- und kommunalen Wahlen jeweils gesetzlich angeordnete öffentliche Auslegung der Wählerverzeichnisse die Datenschutzbeauftragten des Bundes und der Länder. Denn mit der unbeschränkten Auslegung der Wählerverzeichnisse ist naturgemäß auch die Offenbarung personenbezogener Daten der darin registrierten Wahlberechtigten unabhängig von ihrer im Einzelfall bestehenden Sensibilität oder im Melderegister eingetragener Übermittlungssperren verbunden. Aus diesem Grunde enthielt schon eine Entschließung der 49. Konferenz der Datenschutzbeauftragten des Bundes und der Länder aus dem Jahre 1995 die Forderung, dass entweder in den öffentlich ausliegenden Wählerverzeichnissen nur Name, Vorname und Geburtsdatum der Wahlberechtigten aufgenommen oder bei Wiedergabe der Adressen im Wählerverzeichnis nur Auskünfte zu bestimmten Personen an den Auskunftssuchenden erteilt werden sollten, wenn er zuvor die Adresse dieser Person angegeben hat. Im Übrigen sollte nach Meinung der Datenschutzbeauftragten die Veröffentlichung der mit einer melderechtlichen Auskunftssperre versehenen Bürgerdaten im Wählerverzeichnis unterbleiben.

Erst im Jahre 1999 wurde im Zuge einer Gesetzesinitiative der Landesregierung zur Änderung wahlrechtlicher Vorschriften das bisher in Rheinland-Pfalz unbeschränkte und jedem Wahlberechtigten zustehende Einsichtsrecht in das Wählerverzeichnis eingeengt. Nunmehr gewährt § 6 Abs. 2 LWG jedem Stimmberechtigten das Recht, die Richtigkeit und Vollständigkeit seiner Eintragung im Wählerverzeichnis zu überprüfen. Ein darüber hinausgehendes Einsichtsrecht besteht nur dann, wenn die die Einsicht begehrenden Bürger Zweifel an der Richtigkeit oder Vollständigkeit des Wählerverzeichnisses glaubhaft machen. Ausdrücklich begrenzt die Bestimmung den Verwendungszweck der im Rahmen der Einsicht gewonnenen Erkenntnisse auf die Begründung eines Einspruches gegen das Wählerverzeichnis und für Zwecke der Wahlprüfung.

Die in § 6 Abs. 2 LWG aufgenommenen Änderungen tragen den im Vorfeld geäußerten datenschutzrechtlichen Erfordernissen weitgehend Rechnung, obwohl sie auch weiterhin eine Umgehung der melderechtlichen Auskunftssperren nicht völlig verhindern. Rein theoretisch besteht auch weiterhin die Gefahr, dass Personen, für die beispielsweise zum Schutz der körperlichen Unversehrtheit im Melderegister eine Auskunftssperre eingetragen worden ist, mit Hilfe der Einsichtnahme in das Wählerverzeichnis ausfindig gemacht werden können. Einige Bundesländer nehmen aus diesem Grunde Daten von Wahlberechtigten, für die im Melderegister Sperrvermerke eingetragen sind, von dem Einsichtnahmerecht aus. Trotz aller Bemühungen gelang es dem LfD nicht, die Einfügung einer solchen Regelung in das rheinland-pfälzische Landeswahlgesetz im Rahmen der Änderung wahlrechtlicher Vorschriften zu erreichen.

Zur Erzielung eines gleichmäßigen Schutzstandards bei allen Wahlen wäre es zudem wünschenswert, wenn sowohl die Regelungen des Bundeswahlgesetzes als auch des Kommunalwahlgesetzes zumindest an die im Landeswahlgesetz eingefügten Beschränkungen des Einsichtsrechtes angepasst werden würden. Denn es ist weder sinnvoll noch datenschutzrechtlich hinnehmbar, wenn Wahlberechtigte nur sehr eingeschränkt in die vor Landtagswahlen ausliegenden Wählerverzeichnisse Einblick nehmen dürfen, dagegen aber im Vorfeld von Bundestags- oder kommunalen Wahlen ohne weitere Voraussetzungen die Wählerverzeichnisse einsehen können.

18.7 Nutzung eines internetgestützten Wahlergebniserfassungsdienstes

Bei einer Landratswahl beabsichtigte die betreffende Kreisverwaltung den Einsatz eines internetunterstützten Ergebniserfassungssystems. Dabei sollten die Ergebnisdaten der Stimmbezirke am Wahlabend von den jeweiligen Verbandsgemeinden nach vorheriger Legitimation online auf einem Internetserver erfasst und zusammengeführt werden. Dadurch bestand die Möglichkeit, die Einzelergebnisse und das Gesamtergebnis zeitnah und aktuell im Internet zu präsentieren.

Gegen den Einsatz des internetgestützten Wahlergebniserfassungsdienstes bestanden keine datenschutzrechtlichen Bedenken. Die Wahlergebnisse von Personenwahlen stellen als solche zwar personenbezogene Daten dar, auf deren Vertraulichkeit sich jedoch die einzelnen Wahlbewerber aus übergeordneten verfassungsrechtlichen Gründen nicht berufen können. Denn die Wähler haben ein berechtigtes Interesse zu erfahren, wer gewählt wurde und wie die politische Bedeutung der gewählten oder nicht gewählten Bewerber ist. Dieses Informations- und Transparenzgebot gegenüber den Wahlberechtigten umfasst sogar bereits Zwischenergebnisse einzelner Stimmbezirke. Mangels gesetzlicher Restriktionen kann dabei auch das Internet als Verbreitungsmedium gewählt werden.

Im Einzelfall ist aber im Hinblick auf das zum Einsatz kommende Ergebniserfassungssystem unter dem Gesichtspunkt der IT-Sicherheit auf die Gewährleistung der Integrität der Daten bei der internetgestützten Übermittlung, beispielsweise durch eine geeignete Verschlüsselung, zu achten.

18.8 Landesgesetz über die Volksinitiative sowie zur Änderung der Bestimmungen über Volksbegehren und Volksentscheide

Aufgrund des Landesgesetzes über die Volksinitiative sowie zur Änderung der Bestimmungen über Volksbegehren und Volksentscheide ist das Landeswahlgesetz mit Wirkung vom 18. Mai 2001 geändert worden.

Im Rahmen der zwischen dem fachlich federführenden Innenministerium und dem LfD erfolgten Erörterung der datenschutzrechtlich relevanten Aspekte des Gesetzesvorhabens konnte im Hinblick auf die in den Antrag auf Behandlung der Volksinitiative (§ 60 e LWG n. F.) sowie in den Zulassungsantrag (§ 63 LWG n. F.), die Eintragungslisten (§ 67 Abs. 3 LWG n. F.) und die Eintragungen des Volksbegehrens (§ 69 LWG n. F.) aufzunehmenden personenbezogenen Daten der Vertreter bzw. der Ersatzpersonen sowie der Stimmberechtigten eine datenschutzverträgliche Lösung einvernehmlich herbeigeführt werden. Von den Vertretern der Volksinitiative bzw. des Volksbegehrens und deren Ersatzpersonen muss danach jeweils nur der Name und die Anschrift (Hauptwohnung) angegeben werden, während sie weder den Tag ihrer Geburt noch ihren Beruf oder Stand nennen müssen. Auch bezüglich der Stimmberechtigten konnte auf die Angabe des Geburtsdatums verzichtet werden.

Soweit schließlich der ursprüngliche Gesetzentwurf noch den Vertretern des Volksbegehrens in § 67 Abs. 5 LWG n. F. ein Einsichtsrecht in die Eintragungslisten einräumte, führten die datenschutzrechtlichen Bedenken des LfD an Stelle dessen zur Gewährung eines einmaligen Auskunftsanspruches. Das zunächst vorgesehene Einsichtsrecht stellte zwar ein durchaus geeignetes Kontroll- und Informationsinstrument für die Initiatoren des Volksbegehrens dar, stand aber angesichts seiner geringen sachlichen Erforderlichkeit außer Verhältnis zu dem daraus erwachsenden Vertraulichkeitsverlust. Denn durch das Einsichtsrecht waren die Vertreter des Volksbegehrens auch in der Lage, das Abstimmungsverhalten von Stimmberechtigten in Erfahrung zu bringen. Dazu zählt nicht nur die Tatsache der Eintragung als solcher sowie des aus der Eintragungsliste ersichtlichen Eintragungstextes, sondern auch die Information darüber, dass sich Stimmberechtigte nicht in die Eintragungsliste eingetragen haben. Dies wird insbesondere dann relevant, wenn die Vertreter das Abstimmungsverhalten einzelner Stimmberechtigter überprüfen oder beeinflussen wollen. Eine jederzeit und wiederholt mögliche Einsichtnahme in den eigentlichen Abstimmungsakt eines Stimmberechtigten durch Dritte hätte deshalb dessen Persönlichkeitsrechte berührt und auch im Vergleich zu den bei den Volksabstimmungen geltenden Abstimmungsgrundsätzen einen bedeutsamen Verlust an Vertraulichkeit dargestellt, ohne dass dies sachlich erforderlich gewesen wäre. Da auf der anderen Seite den Informationsbedürfnissen der Organisatoren des Volksbegehrens auch durch die Einräumung eines Auskunftsrechts ausreichend Rechnung getragen werden konnte, war auf das anfänglich geplante Einsichtsrecht schon wegen des Grundsatzes der Verhältnismäßigkeit zu verzichten.

18.9 Gemeinderatsfraktionen und Datenschutz

Auf Gesetzesebene unterblieb bislang – im Gegensatz zu den in § 2 Abs. 2 Satz 1 LDSG erwähnten Landtagsfraktionen – jegliche Regelung zur rechtlichen Einordnung der kommunalen Fraktionen. Angesichts des in § 2 Abs. 1 Nr. 4 LDSG pauschal den kommunalen Gebietskörperschaften zugewiesenen Status als „öffentliche Stelle" ist jedoch davon auszugehen, dass auch die kommunalen Ratsfraktionen als Teil dieser kommunalen Gebietskörperschaften bei ihrem selbständigen, nach außen gerichteten Handeln eigenständiger Adressat datenschutzrechtlicher Vorschriften sein können.

Vor diesem Hintergrund hatte der LfD die datenschutzrechtliche Zulässigkeit einer durch eine Gemeinderatsfraktion betriebenen Datenerhebung bei einer externen Versorgungseinrichtung zu beurteilen. Die Fraktion hatte im Rahmen einer Anfrage in Erfahrung bringen wollen, welche versorgungsrechtlichen Auswirkungen zu Lasten der Verbandsgemeinde bei einer nicht erfolgten Wiederwahl des amtierenden Bürgermeisters entstehen würden und wie hoch die jährliche finanzielle Mehrbelastung für die Verbandsgemeinde wäre. Da hieraus Rückschlüsse auf die Höhe der Versorgungsbezüge des ausscheidenden Gemeindechefs möglich waren, handelte es sich bei den erbetenen Informationen um personenbezogene Daten. Diese dürfen gemäß § 12 Abs. 1 LDSG zulässigerweise nur erhoben werden, wenn ihre Kenntnis zur rechtmäßigen Erfüllung der Aufgaben der erhebenden Stelle erforderlich ist. Zu den Aufgaben von Gemeinderatsfraktionen gehören die Steuerung und Erleichterung der Arbeit des Gemeinderates, wobei Fraktionen allerdings nicht berechtigt sind, Interessen wahrzunehmen, die dem Gemeinderat als Organ der Gemeinde in seiner Gesamtheit zustehen. Im konkreten Fall betraf die Nachfrage der Ratsfraktion den Bereich der kommunalen Haushalts- und Finanzplanung, der zu den originären Aufgaben des Gemeinderates gehört. Diesbezügliche Auskunftsersuchen, die personenbezogene Daten zum Gegenstand haben und die an Stellen außerhalb der Gemeinde gerichtet sind, fallen nicht mehr in den Aufgabenbereich der einzelnen Fraktionen und sind daher datenschutzrechtlich auch nicht zulässig.

Der LfD stimmte seine Bewertung im Vorfeld mit dem Ministerium des Innern und für Sport ab und beanstandete die Datenerhebung durch die Gemeinderatsfraktion als Verstoß gegen datenschutzrechtliche Vorschriften.

18.10 Ratsmitglieder im Bilde – Das Fotografieren während einer Stadtratssitzung

Während der Sitzung des Rates einer rheinland-pfälzischen Stadt fotografierte ein Ratsmitglied mehrere seiner Kollegen. An den Aufnahmen, die offen und für jedermann erkennbar gemacht wurden, nahm niemand Anstoß. Erst eine Woche später meldete sich der Bürgermeister bei dem Fotografen und verlangte unter Berufung auf das Persönlichkeitsrecht der fotografierten Ratsmitglieder und das ihm als Ratsvorsitzenden zustehende Hausrecht die Herausgabe von Bildern und Negativen. Dieses Begehren lehnte der Betroffene ab. Er hatte zwischenzeitlich mit den Abgelichteten gesprochen, die sich weder durch die Aufnahmen gestört gefühlt hatten noch diese herausverlangten.

Im Ergebnis fehlte dem Herausgabeverlangen des Bürgermeisters die Rechtsgrundlage. Die Aufforderung, das Bildmaterial herauszugeben, stellt datenschutzrechtlich eine Erhebung personenbezogener Daten im Sinne von § 12 Abs. 1 LDSG dar. Diese ist danach u. a. zulässig, wenn ihre Kenntnis zur rechtmäßigen Erfüllung der Aufgaben der erhebenden Stelle erforderlich ist. Dies war vorliegend nicht zu erkennen: Die auf dem Bildmaterial enthaltenen personenbezogenen Daten wurden für keine in der Gemeindeordnung oder einer anderen Rechtsgrundlage enthaltene Aufgabe des Gemeinderates oder des Bürgermeisters benötigt. Insbesondere ließ sich das Herausgabeverlangen nicht auf das in § 36 Abs. 2 GemO verankerte Hausrecht des Ratsvorsitzenden bzw. dessen in § 38 GemO enthaltene Ordnungsbefugnisse stützen. Abgesehen davon, dass das Fotografieren von Ratsmitgliedern während einer Ratssitzung in der Geschäftsordnung des Stadtrates nicht untersagt war, hinderte auch die erst nachträgliche Geltendmachung der behaupteten hausrechtlichen Befugnisse eine Berufung hierauf. Denn offenbar hatte das Fotografieren der Ratsmitglieder nicht den Ablauf der damaligen Stadtratssitzung gestört.

Auch die Aspekte des allgemeinen Persönlichkeitsrechtes in Verbindung mit dem Recht am eigenen Bilde rechtfertigten nicht das Herausgabeverlangen. Neben der fehlenden Befugnis des Bürgermeisters, diese Persönlichkeitsrechte Dritter im eigenen Namen geltend zu machen, tritt das allgemeine Persönlichkeitsrecht nämlich dann zurück, wenn ein Staatsorgan – wozu auch ein Gemeinderatsmitglied zählt – in Erfüllung öffentlicher Aufgaben fotografiert wird (vgl. Entscheidung des LG Stuttgart vom 14. Januar 1992, Az. 17 O 586/91, veröffentlicht im Archiv für Presserecht [AfP] 1992, S. 314).

18.11 Namentliche Erfassung der Besucher öffentlicher Stadtratssitzungen

Wegen des beschränkten Platzangebotes sah sich eine Stadtverwaltung gezwungen, generell zu den öffentlichen Sitzungen des Stadtrates Eintrittskarten auszugeben. Bei der Behandlung eines schon im Vorfeld in der Öffentlichkeit äußerst kontrovers diskutierten Themas im Stadtrat wurde darüber hinaus noch namentlich festgehalten, an wen wie viele Eintrittskarten ausgehändigt worden waren. Ziel war es, eine gleichmäßige Verteilung der Besucherplätze zu erreichen.

Aus datenschutzrechtlicher Sicht stößt die namentliche Erfassung der Besucher einer öffentlichen Ratssitzung mangels der nach § 12 Abs. 1 LDSG notwendigen Erforderlichkeit der Datenerhebung auf erhebliche Bedenken. Nach dem für öffentliche Ratssitzungen geltenden Öffentlichkeitsgrundsatz hat jedermann das Recht, im Rahmen der tatsächlichen Gegebenheiten ohne Rücksicht auf seine Gesinnung oder die Zugehörigkeit zu einer bestimmten Bevölkerungsgruppe Zutritt zu den Sitzungen zu erhalten. Die Auswahl des Sitzungssaales hat sich dabei an dem zu erwartenden Besucherandrang zu orientieren. Weist der Sitzungsraum dennoch

zu geringe Kapazitäten auf, richtet sich die Einlassgewährung grundsätzlich nach dem Prioritätsprinzip. Danach ist Interessierten in der Reihenfolge ihrer zeitlichen Präsenz der Zutritt zu gestatten. Weder die namentliche Erfassung der Besucher noch ihre Zuordnung zu einer bestimmten Gruppierung ist hierfür erforderlich. Denn für die Einhaltung des Öffentlichkeitsgrundsatzes kommt es nicht darauf an, dass die von dem Beratungsgegenstand betroffenen unterschiedlichen Interessengruppen jeweils in angemessener Zahl vertreten sind. Solange keine konkreten Anhaltspunkte für mögliche Störungen im Vorfeld einer Sitzung vorliegen, vermag angesichts der dem Ratsvorsitzenden nach § 36 Abs. 2 GemO zur Verfügung stehenden Ordnungsbefugnisse zudem auch nicht der Gesichtspunkt der Gefahrenprävention die Erfassung der Besuchernamen zu rechtfertigen. Im Ergebnis war somit die namentliche Erfassung der Sitzungsbesucher für die Aufgabenerfüllung der Stadtverwaltung nicht erforderlich und daher unzulässig. Sie wird nach Auskunft der Stadtverwaltung in Zukunft unterbleiben.

18.12 Schrankenlose Zugriffsmöglichkeiten für die Behördenleitung?

Anlässlich örtlicher Feststellungen bei einer Stadtverwaltung wurde der LfD mit der Frage befasst, inwieweit die Behördenleitung berechtigt ist, jederzeit direkt und unbeschränkt auf die in elektronischer Form vorgehaltenen Dokumente zugreifen zu können. Im konkreten Fall hatte der Oberbürgermeister sogar selbst Systemadministratorbefugnisse wahrgenommen, wodurch er umfassend auf alle in der Stadtverwaltung in elektronischer Form vorgehaltenen Vorgänge zugreifen konnte.

In datenschutzrechtlicher Hinsicht sind von umfangreichen Zugriffsmöglichkeiten der Behördenleitung nicht nur die Mitarbeiterinnen und Mitarbeiter der Verwaltung, sondern auch diejenigen Bürgerinnen und Bürger betroffen, die sich mit verschiedenen Anliegen an die Verwaltung wenden. Insbesondere bei Stadt- und Kreisverwaltungen eröffnet der Direktzugriff auf Bürgerdaten aus verschiedenen Bereichen der Verwaltung (Sozialamt, Steueramt, Ordnungsamt etc.) die Möglichkeit, sich ein weit gehendes Datenprofil einzelner Einwohner zu erstellen. Aber auch datenschutzrechtliche Interessen der Bediensteten sind hierdurch betroffen.

Häufig werden umfassende Zugriffsberechtigungen damit begründet, dass bei sog. Bürgersprechstunden der unmittelbare Zugriff auf den Vorgang möglich sein müsse. In aller Regel ist jedoch schon bei der Terminvergabe das Anliegen konkret zu bezeichnen, so dass schon im Rahmen der Terminvorbereitung der Vorgang hinzugezogen werden könnte. Eine Situation, die einen sofortigen unmittelbaren Zugriff auf die Akte erforderlich macht, liegt in aller Regel wohl nicht vor. Während es für den Bereich einzelner Fachämter noch hinnehmbar sein könnte, wenn der Behördenleitung ein Online-Zugriff auf sämtliche Vorgänge eröffnet wird, ist dies bei Verwaltungen mit verschiedenen Zuständigkeiten, insbesondere bei Kreis- und Stadtverwaltungen, aus den o. g. Gründen nicht akzeptabel.

Im vorliegenden Fall waren auch die Zugriffsbefugnisse des Bürgermeisters auf die im Geschäftsbereich des Beigeordneten vorgehaltenen Informationen zu problematisieren. § 50 Abs. 6 GemO sieht vor, dass die Beigeordneten ihren Geschäftsbereich im Rahmen der Beschlüsse des Gemeinderats und der allgemeinen Richtlinien des Bürgermeisters selbständig verwalten. Daraus folgt, dass die Gesamtverantwortung des Bürgermeisters insoweit eingeschränkt und ihm ein direkter Zugriff auf alle im Geschäftsbereich eines Beigeordneten anfallenden Daten deshalb zu versagen ist.

Aufgrund der allgemeinen Bedeutung der Thematik hat der LfD in diesem Zusammenhang eine Orientierungshilfe veröffentlicht (siehe Anlage 30). Sie richtet sich an alle Hierarchieebenen einer (kommunalen) Verwaltung, bei denen sich unterschiedliche Funktionsbereiche wie z. B. das Sozialamt, Ordnungsamt oder Steueramt in einer Person bündeln. Auf der Grundlage des vom Bundesverfassungsgericht bestätigten Grundsatzes der informationellen Gewaltenteilung soll der Leitungsebene ein genereller automatisierter und unbeschränkter Zugriff auf personenbezogene Daten verwehrt werden, wenn eine zweckwidrige Verwendung der Informationen durch einen unmittelbaren Zugriff möglich wäre. Zudem ist die in der Person des Zugriffsberechtigten möglicherweise entstehende Kollision zwischen dem reinen aufgabenbedingten Sachinteresse und der Möglichkeit einer umfassenden und unbeschränkten Informationsanreicherung und -verarbeitung grundsätzlich zu vermeiden. Demzufolge begegnet die Einräumung von generellen und unbeschränkten Zugriffsberechtigungen dann keinen datenschutzrechtlichen Bedenken, solange der Berechtigte in seiner Person nicht unterschiedliche Funktionsbereiche zuständigkeitshalber vereinigt. Die Mitbestimmungspflicht des Personalrates nach § 80 Abs. 1 Nr. 3 LPersVG bleibt davon allerdings unberührt.

Darüber hinaus sind die in der o. g. Orientierungshilfe formulierten Grundsätze auch außerhalb der Kommunalverwaltungen anwendbar.

18.13 Grundstücks- und Grundeigentümerdaten für einen Windpark

In weiten Teilen des Landes prägen inzwischen Windenergieanlagen die Landschaft. In diesem Zusammenhang beschloss der Rat einer Verbandsgemeinde, in einer raumplanerisch bereits dafür ausgewiesenen Vorrangfläche weitere derartige Anlagen zu errichten und entsprechende Errichtungsverträge nur mit einer bestimmten privaten Firma abzuschließen.

Vor diesem Hintergrund wandte sich diese Firma an die Verwaltung der Verbandsgemeinde mit dem Wunsch, die Daten derjenigen Grundeigentümer zu erhalten, deren Grundstücke in der ausgewiesenen Vorrangfläche gelegen waren. Die Firma beabsichtigte, im Hinblick auf den gemeindlichen Beschluss die Grundeigentümer direkt anzusprechen und mit ihnen bereits Verhandlungen über

den Abschluss von Gestattungsverträgen zu führen. Auf Anordnung des Bürgermeisters der Verbandsgemeinde wurden die gewünschten Daten der anfragenden Firma zur Verfügung gestellt, ohne dass die Betroffenen vorab über die bevorstehende Datenübermittlung unterrichtet wurden.

Ausgehend von der für die Übermittlung personenbezogener Daten an nicht öffentliche Stellen einschlägigen Regelung des § 16 LDSG fehlt es an den entsprechenden Voraussetzungen für eine zulässige Übermittlung. Insbesondere stellen die wirtschaftlichen Interessen der Errichtungsfirma an dem Erhalt der Daten keine rechtlichen Interessen im Sinne von § 16 Abs. 1 Nr. 3 LDSG dar. Auch der Rückgriff auf § 16 Abs. 1 Nr. 4 LDSG schlug im konkreten Fall fehl, da die darin enthaltene Widerspruchslösung die vorherige Unterrichtung der Betroffenen voraussetzt. Eine solche hatte es aber nicht gegeben.

Die Übermittlung der Grundstücks- und Grundeigentümerdaten war somit unzulässig und wurde gegenüber der Verbandsgemeinde als Verstoß gegen datenschutzrechtliche Vorschriften beanstandet. Angesichts der den Katasterbehörden zugewiesenen Verwaltung von Liegenschaftsdaten ist es im Ergebnis auch durchaus sachgerecht, den Gemeindeverwaltungen diesbezügliche Auskunftserteilungen zu verwehren. Daran vermögen weder die vertraglichen Verpflichtungen der Verbandsgemeinde gegenüber der Firma noch der zugrunde liegende Ratsbeschluss etwas zu ändern. Denn der Verbandsgemeinde ist es nicht gestattet, durch den Abschluss eines Vertrages mit einem Dritten in grundrechtsrelevante Rechtspositionen ihrer Bürger (hier: in das Recht auf informationelle Selbstbestimmung) einzugreifen.

18.14 Datenschutz im Zusammenhang mit der Ausführung der „Gefahrenabwehrverordnung Gefährliche Hunde“

Der LfD wurde im Berichtszeitraum mehrfach darauf angesprochen, ob im Rahmen der Ausführung der „Gefahrenabwehrverordnung Gefährliche Hunde“ eine Einsichtnahme durch die Ordnungsverwaltung in die bei der Steuerverwaltung geführte Hundesteuerkartei datenschutzrechtlich zulässig sei. Die Ordnungsämter begründeten ihren diesbezüglichen Wunsch mit dem Umstand, dass nicht alle Kampfhundebesitzer ihrer aus der Gefahrenabwehrverordnung resultierenden Verpflichtung nachkommen würden und es daher erforderlich sei, im Wege des Abgleichs mit den in der Steuerverwaltung gespeicherten Halterdaten die nachlässigen und damit potenziell unzuverlässigen Hundebesitzer ausfindig zu machen.

Nach der Rechtslage, die insoweit keinen Spielraum eröffnet, ist, solange es sich um die Abwehr der von gefährlichen Hunden ausgehenden allgemeinen Gefahr handelt, sowohl die Einsicht als auch die Übermittlung von in der Hundesteuerkartei enthaltenen Daten an die Ordnungsverwaltung datenschutzrechtlich unzulässig. Bei der Hundesteuer handelt es sich um eine kommunale Abgabe im Sinne von § 1 Abs. 1 KAG. Nach § 3 Abs. 1 Nr. 1 KAG gilt für diese das in § 30 AO verankerte Steuergeheimnis. § 3 Abs. 2 Nr. 5 KAG gestattet nur in Schadensfällen ausnahmsweise die Weitergabe von Namen und Anschrift des Hundesteuerpflichtigen an Behörden und Geschädigte. Die Durchbrechung des Steuergeheimnisses zur Vorbeugung möglicher Schäden sieht das Kommunalabgabengesetz dagegen nicht vor. Die in § 30 Abs. 4 Nr. 5 AO enthaltene Offenbarungsmöglichkeit im Falle eines zwingenden öffentlichen Interesses umfasst zwar grundsätzlich auch Zwecke der Gefahrenabwehr; allerdings muss es sich dann um die Abwehr einer konkreten Gefahr für erhebliche Rechtsgüter handeln. Eine solche liegt aber bei der generell beabsichtigten Einsichtnahme in die Hundesteuerkartei nicht vor, so dass diese der Ordnungsverwaltung verwehrt ist.

Der Gesetzgeber ist angesichts der bestehenden Gefährdungslage aufgerufen, eine weitere Nutzungsmöglichkeit von Hundesteuerdaten auch zu Zwecken der Abwehr der allgemeinen Gefahren, die von gefährlichen Hunden ausgehen, zuzulassen. Dem LfD liegen Informationen vor, wonach eine solche gesetzliche Regelung auch angestrebt wird.

18.15 Keine Blankoeinwilligung zu Datenerhebungen der Unterhaltssicherungsstelle

Eine Kreisverwaltung, die bei der Gewährung von Leistungen nach dem Unterhaltssicherungsgesetz als Unterhaltssicherungsstelle fungiert, verwendete in diesem Zusammenhang eine standardmäßig vorformulierte Einverständniserklärung, in der sich der Antragsteller mit einer Abfrage von entscheidungsrelevanten persönlichen Daten durch die Kreisverwaltung bei seiner Bank, öffentlichen Ämtern, seinen Eltern, seinem Vermieter, seinem Versicherungsunternehmen und/oder seinem Arbeitgeber einverstanden erklären sollte.

Die Einverständniserklärung begegnete grundsätzlichen datenschutzrechtlichen Bedenken:

Gemäß § 5 Abs. 1 Nr. 2 und § 12 Abs. 4 Nr. 1 LDSG bedarf es keiner Einwilligung des Betroffenen, sofern für die Datenerhebung bei Dritten bereits eine entsprechende Rechtsvorschrift existiert. Insbesondere in den Fällen, in denen diese Rechtsgrundlage eine Auskunftspflicht des Dritten konstituiert, würde die Einholung einer Einwilligung fälschlicherweise den Eindruck erwecken, der Betroffene würde die Datenerhebung bei dem Dritten durch Verweigerung der Einwilligung verhindern können. Dies ist aber unzutreffend. Denn die in § 20 USG enthaltenen Auskunfts- und Mitteilungspflichten haben zur Folge, dass der Antragsteller die Datenerhebung bei seinen Familienangehörigen, seinem Arbeitgeber, den Sozialversicherungsträgern, den Finanzbehörden sowie den für die Einberufung und Entlassung in den Wehrdienst zuständigen Stellen bei Vorliegen der entsprechenden Voraussetzungen auch ohne Einwilligung grundsätzlich zu dulden hat. Die von der Kreisverwaltung konzipierte Einverständniserklärung spiegelte dem Betroffenen jedoch ein eigenes Entscheidungsrecht vor, das tatsächlich nicht besteht.

Soweit für die Datenerhebung bei Dritten eine entsprechende bereichsspezifische Rechtsvorschrift fehlt, eröffnet zwar § 12 Abs. 4 Nr. 2 i. V. m. § 5 LDSG die Möglichkeit der Einwilligung. Dabei ist aber Folgendes zu beachten: Der Betroffene ist nach § 5 Abs. 3 LDSG in geeigneter Weise über die Bedeutung der Einwilligung, den Verwendungszweck der Daten und den möglichen Empfängerkreis aufzuklären und auf die Folgen einer Verweigerung der Einwilligung hinzuweisen. Dieser sog. „informierten Einwilligung" muss daher grundsätzlich eine konkrete bzw. bestimmbare Datenverarbeitung zugrunde liegen. Pauschale Einverständniserklärungen, aus denen für den Betroffenen die Tragweite seiner Einwilligung nicht im Einzelnen ersichtlich ist, sind aus datenschutzrechtlicher Sicht deshalb unzulässig. Die von der Kreisverwaltung eingesetzte Einverständniserklärung genügte diesen Anforderungen nicht. Es waren weder die in § 5 Abs. 3 LDSG enthaltenen Aufklärungs- und Hinweispflichten umgesetzt noch konnte der Unterzeichner erkennen, auf welche Daten sich die von ihm abgegebene Erklärung konkret bezog.

Die Einverständniserklärung wird angesichts der Bedenken des LfD von der Kreisverwaltung nicht mehr verwendet.

18.16 Datenschutz und Ortschronik

Der Bürgermeister einer rheinland-pfälzischen Gemeinde beabsichtigte im Zusammenhang mit der Überarbeitung der alten Ortschronik die Veröffentlichung von Zeitungsartikeln aus den Jahren 1938 und 1968. Gegenstand dieser Berichte waren zwei in diesen Jahren vorgefallene Kriminalfälle, bei denen die Täter beide aus der betreffenden Gemeinde stammten. In der damaligen Berichterstattung wurden die Namen der Täter genannt sowie die ihnen zugeschriebenen Taten ausführlich beschrieben.

Datenschutzrechtlich handelt es sich bei einer Veröffentlichung von Zeitungsartikeln in einer Ortschronik, die personenbezogene Daten enthalten, um eine Datenübermittlung an nicht öffentliche Stellen im Sinne von § 16 Abs. 1 Ziff. 1 LDSG. Diese ist u. a. zulässig, wenn sie zur rechtmäßigen Erfüllung der in der Zuständigkeit der übermittelnden Stelle liegenden Aufgaben erforderlich ist und die Voraussetzungen vorliegen, die eine Verarbeitung nach § 12 Abs. 4 LDSG zulassen würden.

Es ist zunächst davon auszugehen, dass die Übermittlung von Informationen zum Zwecke der Veröffentlichung einer Ortschronik als öffentliche Aufgabe der örtlichen Gemeinschaft anzusehen ist, weil damit die gemeindliche Identität gestärkt und das Zusammengehörigkeitsgefühl gefördert werden soll. Auch waren die Daten, wie in § 12 Abs. 4 Satz 1 Ziff. 9 LDSG verlangt, unmittelbar aus allgemein zugänglichen Quellen entnommen worden, so dass es in Anbetracht von § 12 Abs. 4 Satz 2 LDSG nur noch um die Frage ging, ob überwiegende schutzwürdige Interessen der Betroffenen einer Veröffentlichung entgegenstehen würden.

Dies war im Ergebnis der Fall. Denn sofern die in den Zeitungsartikeln genannten Straftäter noch lebten und sich möglicherweise in ihrer Heimatgemeinde oder in der näheren Umgebung aufhielten, wäre der Gesichtspunkt der Resozialisierung als überwiegendes schutzwürdiges Interesse der Betroffenen anzuerkennen, zumal die Strafe längst verbüßt und auch getilgt war. Da sich die Betroffenen demnach selbst als unbestraft bezeichnen konnten und die Verurteilung nicht mehr zu ihrem Nachteil verwertet werden durfte (vgl. §§ 51 und 53 BZRG,) hätte eine Veröffentlichung den in diesen Vorschriften zum Ausdruck kommenden Resozialisierungsgedanken konterkariert. Aber selbst wenn die betroffenen Straftäter in der Zwischenzeit verstorben gewesen wären, musste berücksichtigt werden, dass mit einer solchen Veröffentlichung auch Datenschutzrechte der Angehörigen betroffen sein konnten. Allein die Art und Weise, wie die Zeitungsartikel aus dem Jahre 1938 und 1968 verfasst waren, hätte nach einer Veröffentlichung in der Ortschronik einer relativ kleinen Gemeinde unter Einbeziehung der betroffenen Familien für Gesprächsstoff gesorgt. Die Interessen der Angehörigen, nach so langer Zeit nicht mehr mit dem straffälligen Verhalten von Familienmitgliedern konfrontiert zu werden, war daher als überwiegendes schutzwürdiges Interesse anzuerkennen.

18.17 Opfernamen auf einem Denkmal

Im Zuge der Aufarbeitung der lokalen Geschichte plante eine Stadtverwaltung die Veröffentlichung von Namenslisten aller gemeindlichen Opfer aus der Zeit zwischen 1933 und 1945 auf einem städtischen Mahnmal. Maßgeblich für die Beurteilung der Frage, ob dies datenschutzrechtlich zulässig ist, sind dabei zwei Gesichtspunkte: einerseits die Datenquelle, andererseits der Umstand, ob es sich um Daten lebender oder schon verstorbener Personen handelt.

Sofern die auf dem Mahnmal zu veröffentlichenden Namen aus öffentlichen Archiven stammen, finden die jeweiligen Bestimmungen des Archivrechtes Anwendung. Neben den archivspezifischen Nutzungsbeschränkungen darf personenbezogenes Archivgut gemäß § 3 Abs. 3 Satz 2 LArchG grundsätzlich erst 30 Jahre nach dem Tod der Person bzw., falls das Todesjahr nicht bekannt ist, erst 110 Jahre nach der Geburt des Betroffenen benutzt werden. Eine Verkürzung dieser Sperrfristen ist u. a. gemäß § 3 Abs. 4 Satz 1 Nr. 1 LArchG dann möglich, wenn die Betroffenen eingewilligt haben. Eine Nutzung des Archivgutes ist unabhängig von den Sperrfristen einzuschränken bzw. zu versagen, wenn Grund zu der Annahme besteht, dass schutzwürdige Belange Betroffener oder Dritter entgegenstehen (§ 3 Abs. 2 Nr. 2 LArchG). Dies ist, solange nicht konkrete Einwände Betroffener oder Dritter vorliegen, angesichts der angestrebten Verwendung der Daten nicht anzunehmen. Denn mit dem von der Stadt geplanten Mahnmal sollen die örtlichen Opfer aus der Zeit von 1933 bis 1945 aus ihrer Anonymität herausgehoben werden und dem heutigen Betrachter als Menschen und Mitbürger in Erinnerung bleiben. Schutzwürdige Belange der Betroffenen bzw. Dritter werden dadurch wohl nicht beeinträchtigt.

Entstammen die Opfernamen nicht einem öffentlichen Archiv und handelt es sich um solche noch lebender Personen, findet das Landesdatenschutzgesetz direkt Anwendung. Dies gilt auch dann, wenn unbekannt ist, ob die betreffenden Personen mittlerweile verstorben sind. Die direkte Heranziehung des Landesdatenschutzgesetzes ist nur dann verwehrt, sofern die Daten verstorbenen Personen zuzuordnen sind. Die Veröffentlichung der personenbezogenen Daten Lebender auf einem Mahnmal stellt datenschutzrechtlich eine Datenübermittlung an nicht öffentliche Stellen im Sinne von §§ 3 Abs. 2 Nr. 4 und 16 LDSG dar. Sie ist u. a. nach § 16 Abs. 1 Nr. 2 i. V. m. § 12 Abs. 4 Satz 1 Ziff. 2 und 9 LDSG zulässig, wenn die Betroffenen in die Veröffentlichung der Namen eingewilligt haben oder die Daten unmittelbar aus allgemein zugänglichen Quellen entnommen werden können. Da die Aufnahme der Namen auf dem Mahnmal zugleich als Aufarbeitung der örtlichen Geschichte im öffentlichen Interesse liegt, wäre sie gem. § 16 Abs. 1 Nr. 4 LDSG auch dann zulässig, wenn die Betroffenen nach entsprechender Unterrichtung der beabsichtigten Veröffentlichung nicht widersprochen hätten.

18.18 Weitergabe von Listen der Beschäftigungsstellen ehemaliger NS-Zwangsarbeiter aus dem Stadtarchiv

Zwischen 1933 und 1945 wurden bei zahlreichen Betrieben und Unternehmen in Deutschland Zwangsarbeiter beschäftigt. Der Rat einer rheinland-pfälzischen Stadt griff nun diese Thematik auf und bildete einen aus Ratsmitgliedern bestehenden Arbeitskreis, der zur Aufgabe hatte, die diesbezügliche städtische Geschichte systematisch aufzuarbeiten. In diesem Zusammenhang stießen die Mitglieder des Arbeitskreises auf eine im Stadtarchiv nur für den internen Gebrauch zusammengestellte Liste aller im Stadtgebiet befindlichen Beschäftigungsstellen von Zwangsarbeitern und forderten, diese als Arbeitsunterlage zur Verfügung gestellt zu bekommen. Da diese Liste nach Auskunft des Archivs teilweise Daten noch lebender Einzelpersonen sowie noch existierender Firmen enthielt, bestanden seitens der Stadtverwaltung datenschutzrechtliche Bedenken gegen die Weitergabe einer solchen Liste.

Während die Herausgabe von Listen ehemaliger NS-Zwangsarbeiter aus kommunalen Archiven schon mehrfach Gegenstand von Anfragen beim LfD war, tauchte die Problematik der Weitergabe von Listen früherer Beschäftigungsstellen hier erstmals auf. Für die Nutzung des im Stadtarchiv geführten öffentlichen Archivgutes sind, selbst wenn sich der Nutzerkreis ausschließlich aus Mitgliedern des Stadtrates zusammensetzt, nicht die Gemeindeordnung, sondern die spezielleren Bestimmungen des Landesarchivgesetzes maßgeblich. Ob die Weitergabe der o. g. Liste datenschutzrechtlich zulässig ist, beurteilt sich abschließend nach diesen Regelungen. Grundsätzlich hat gemäß § 3 Abs. 1 LArchG jeder, der ein berechtigtes Interesse darlegt, das Recht, öffentliches Archivgut nach Maßgabe der Rechtsvorschriften und der Benutzungsordnungen zu nutzen. Da der Gebrauch der im Stadtarchiv befindlichen Liste der Aufarbeitung der städtischen Geschichte durch den o. g. Arbeitskreis dienen sollte, lag ein berechtigtes Interesse an der Nutzung des Archivgutes im Sinne von § 3 Abs. 1 LArchG vor. Allerdings ist nach § 3 Abs. 2 Nr. 2 LArchG die Benutzung einzuschränken oder ganz zu versagen, wenn Grund zu der Annahme besteht, dass schutzwürdige Belange Betroffener oder Dritter entgegenstehen. Zweifellos wären mit einer Veröffentlichung der Liste die Belange der noch existierenden Firmen bzw. der aus der Liste hervorgehenden noch lebenden Personen, sofern die Tatsache der Beschäftigung von NS-Zwangsarbeitern nicht bereits zuvor allgemein bekannt war, berührt. Das mögliche Interesse der Betroffenen an der Nichtverbreitung dieser Informationen aus wirtschaftlichen oder persönlichen Gründen muss jedoch in Anlehnung an die in § 7 MG enthaltene Wertung angesichts des konkreten Verwendungszwecks des Archivgutes – der historisch bedeutsamen Aufarbeitung der lokalen Geschichte der NS-Jahre – als weniger schutzwürdig beurteilt werden. Schutzwürdige Belange der Betroffenen im Sinne von § 3 Abs. 2 Nr. 2 LArchG stehen der Benutzung somit nicht entgegen.

Im Ergebnis stimmte der LfD bei Beachtung der in § 3 Abs. 3 und 4 LArchG enthaltenen Regelungen über die Sperrfristen einer Weitergabe der Liste an den Arbeitskreis zu.

19. Telekommunikation

19.1 Die Telekommunikations-Datenschutzverordnung (TDSV 2000)

Nach Zustimmung des Bundesrates hat die Bundesregierung am 22. November 2000 die Telekommunikations-Datenschutzverordnung verabschiedet (BGBl. I 2000 S. 1740 ff.). Vorläufer dieser TDSV 2000 war die Telekommunikationsdienstunternehmen-Datenschutzverordnung (TDSV 1996). Obwohl deren Ermächtigungsgrundlage durch das In-Kraft-Treten des Telekommunikationsgesetzes bereits zum 31. Dezember 1997 weggefallen war, blieb die TDSV 1996 weiterhin in Kraft. Im Rahmen der Novellierung waren aber nicht nur die Vorgaben des Telekommunikationsgesetzes, sondern auch jene der Richtlinie 97/66/EG des Europäischen Parlaments und des Rates vom 15. Dezember 1997 über die Verarbeitung personenbezogener Daten und dem Schutz der Privatsphäre im Bereich der Telekommunikation zu berücksichtigen (vgl. dazu 16. Tb., Tz. 19.1). Nach Art. 15 dieser Richtlinie hätte die Umsetzung in innerstaatliches Recht bis zum 24. Oktober 1998 geschehen müssen. Dieser Verpflichtung ist die Bundesrepublik mit Verabschiedung der TDSV 2000 mit mehr als zweijähriger Verspätung nachgekommen.

Die Verordnung regelt den Schutz personenbezogener Daten der an der Telekommunikation Beteiligten, sofern Anbieter von Telekommunikationsdiensten die Daten verarbeiten.

Die aus seiner Sicht verbesserungsbedürftigen Regelungen des Entwurfs der TDSV 2000 hat der LfD in einer Stellungnahme gegenüber dem Wirtschaftsministerium angesprochen. Im Vergleich zum Referentenentwurf ist es gelungen, einige datenschutzrechtliche Verbesserungen zu erreichen. Eine Verschlechterung hat das Datenschutzniveau im Telekommunikationsbereich allerdings durch die Ausweitung des Zeitraums, in dem Anbieter von Telekommunikationsdiensten Verbindungsdaten ihrer Kunden speichern dürfen, erfahren.

Die Befugnis der Diensteanbieter, Verbindungsdaten gem. § 7 Abs. 3 TDSV 2000 unter Kürzung der Zielnummer um die letzten drei Ziffern zu Abrechnungszwecken zu speichern, ist von bisher 80 Tagen (TDSV 1996) auf sechs Monate nach Versendung der Rechnung erweitert worden. Gehör hatten die Datenschutzbeauftragten zwischenzeitlich beim Wirtschaftsausschuss des Bundesrates gefunden. Dieser hatte als Kompromiss eine Speicherfrist von drei statt sechs Monaten vorgeschlagen. Letzlich folgte der Bundesrat der Empfehlung des Innenausschusses, der eine sechsmonatige Frist gefordert hatte.

Was das Recht des Kunden zur Bestimmung des Umfangs der Datenspeicherung anbelangt, so kann er nach § 7 Abs. 4 TDSV 2000 vom rechnungsstellenden Diensteanbieter verlangen, dass die Verbindungsdaten vollständig gespeichert oder mit Versendung der Rechnung vollständig gelöscht werden. Dieses Wahlrecht der Kunden bestand bislang gegenüber allen Diensteanbietern. Die Beschränkung auf den rechnungsstellenden Diensteanbieter hat zur Folge, dass die Verbindungsdaten bei allen übrigen Diensteanbietern, die z. B. Daten von Call-by-Call-Verbindungen speichern, unabhängig von der ausgeübten Wahl des Kunden bis sechs Monate nach Versendung der Rechnung gespeichert werden dürfen. Hier wird das kommunikative Selbstbestimmungsrecht der Kunden, die auf die Speicherung der Daten bei anderen Dienstleistern keinen Einfluss mehr haben, ein Stück weit zurückgeschraubt.

Insgesamt bleibt jedoch auch bei den neuen Regelungen der Telekommunikations-Datenschutzverordnung ein hohes Datenschutzniveau im Bereich der Telekommunikationsdienste gewährleistet.

Im Folgenden sind einige bereichsspezifische Datenschutzregelungen der TDSV 2000 dargestellt:

- Nach § 3 Abs. 1 TDSV dürfen die Diensteanbieter personenbezogene Daten der an der Telekommunikation Beteiligten zu Telekommunikationszwecken nur erheben, verarbeiten und nutzen, soweit die Verordnung es erlaubt oder der Beteiligte nach den Vorschriften des Bundesdatenschutzgesetzes eingewilligt hat.

- § 3 Abs. 2 TDSV bestimmt, dass die Erbringung von Telekommunikationsdienstleistungen nicht von der Angabe personenbezogener Daten abhängig gemacht werden darf, die für die Erbringung der Dienstleistung nicht erforderlich sind.

- § 9 TDSV berechtigt die Diensteanbieter, zur Eingrenzung und Beseitigung von technischen Fehlern sowie zur Missbrauchsbekämpfung Bestands- und Verbindungsdaten zu erheben, zu verarbeiten und zu nutzen. Für die Missbrauchsbekämpfung (z. B. Leistungserschleichung) dürfen gem. § 9 Abs. 2 TDSV die Verbindungsdaten in der Weise verarbeitet und genutzt werden, dass aus dem Gesamtbestand aller Verbindungsdaten, die nicht älter als sechs Monate sind, die Daten derjenigen Verbindungen des Netzes ermittelt werden, für die tatsächliche Anhaltspunkte den Verdacht der rechtswidrigen Inanspruchnahme von Telekommunikationsnetzen und -diensten begründen.

- Mit der Vorschrift des § 10 TDSV werden Diensteanbieter verpflichtet, als zusätzliche Dienstleistung die sog. „Feststellung ankommender Telefonverbindungen bei bedrohenden und belästigenden Anrufen" anzubieten. Bei technischen Verfahren zur Feststellung ankommender Verbindungen (Fangschaltungen) erfahren die Diensteanbieter und die Kunden, die diese Dienste in Anspruch nehmen, von welchem Anschluss aus wann und wie lange mit welchem Anschluss telefoniert worden ist. Dabei ist der Kunde des Anschlusses, von dem die als bedrohend oder belästigend bezeichneten Anrufe ausgegangen sind, zu unterrichten, dass über die diese Anrufe betreffenden Verbindungen Auskunft erteilt wurde. Davon kann nur abgesehen werden, wenn der Antragsteller darlegt, dass ihm aus dieser Mitteilung wesentliche Nachteile entstehen können und diese Nachteile bei Abwägung mit den schutzwürdigen Interessen des Anschlussinhabers als wesentlich schwerwiegender erscheinen.

- Soweit vom Diensteanbieter eine Rufnummernanzeige realisiert wird, hat er dem anrufenden und den angerufenen Kunden gem. § 11 TDSV kostenfrei die Möglichkeit einzuräumen, die Rufnummernanzeige dauernd oder für jeden Anruf einzeln zu unterdrücken. Der Angerufene muss im Rahmen des technisch Machbaren darüber hinaus die Möglichkeit haben, eingehende Anrufe, bei denen die Rufnummernanzeige durch den Anrufenden unterdrückt wurde, auf einfache Weise unentgeltlich abzuweisen.

Vor dem Hintergrund, dass bereits der Entwurf für eine neue EG-Richtlinie zum Datenschutz in den elektronischen Kommunikationsmedien vorliegt (vgl. Tz. 19.3), wird die TDSV 2000 in ihrer Gültigkeitsdauer wohl beschränkt sein.

19.2 Entwurf einer Telekommunikations-Überwachungsverordnung

Angesichts der Bedrohung, die durch die vernetzte Welt auf uns zukommt, muss es ein ernsthaftes Anliegen der staatlichen Organe sein, eine effektive Strafverfolgung sicherzustellen.

Die zurzeit gültige Fernmeldeverkehrs-Überwachungs-Verordnung vom 18. Mai 1995, die noch auf dem Gesetz über Fernmeldeanlagen beruht, soll durch eine Rechtsverordnung nach § 88 TKG ersetzt werden. Diese Rechtsverordnung soll die Bezeichnung Telekommunikations-Überwachungsverordnung (TKÜV) erhalten, sich an die Betreiber von Telekommunikationsanlagen richten und die technische und organisatorische Umsetzung der Maßnahmen zur Überwachung der Telekommunikation sowie die zulässigen Ausnahmen regeln.

Der erste Entwurf vom Frühjahr 1998 stand bereits im letzten Berichtszeitraum zur Debatte. Kurze Zeit später wurde er aufgrund massiver Proteste – insbesondere seitens der Provider – zurückgezogen. Ein im Sommer 1999 vorgelegtes „Eckpunktepapier" (vgl. 17. Tb., Tz. 19.3) verschwand auch wieder in der Schublade.

Nach den Vorschriften der Strafprozessordnung, des Gesetzes zu Art. 10 Grundgesetz sowie des Außenwirtschaftsgesetzes kann bei Ermittlungen wegen bestimmter Straftaten die Überwachung der Telekommunikation einzelner Personen angeordnet werden. Die geplante Verordnung basiert also auf grundlegenden Gesetzen, in denen die Notwendigkeit staatlicher Überwachung festgeschrieben ist.

Nach der Regelung in § 88 TKG ist jeder Betreiber einer Telekommunikationsanlage verpflichtet, technische Einrichtungen für die Umsetzung derartiger Überwachungsmaßnahmen vorzuhalten.

Im Verordnungsentwurf ist vorgesehen, die Verpflichtung, technische Einrichtungen für Überwachungszwecke vorzuhalten, grundsätzlich auf die Betreiber solcher Telekommunikationsanlagen zu begrenzen, die Telekommunikationsdienstleistungen für die Öffentlichkeit anbieten. Alle anderen Betreiber von Telekommunikationsanlagen, insbesondere die Betreiber unternehmensinterner Telekommunikationsanlagen, Corporate Networks und Nebenstellenanlagen, brauchen entsprechend der in dem Entwurf vorgesehenen Regelungen keine technischen oder organisatorischen Vorkehrungen für die Umsetzung gesetzlich vorgesehener Überwachungsmaßnahmen zu treffen.

Der Entwurf mit Stand Mai 2001 war jedoch so formuliert, dass von den Überwachungsmaßnahmen nicht nur die Sprachtelefonie und der Telefaxverkehr, sondern auch alle anderen elektronischen Kommunikationsplattformen und damit insbesondere auch das Internet erfasst gewesen wäre. Auf die damit verbundenen datenschutzrechtlichen Risiken haben die Datenschutzbeauftragten des Bundes und der Länder in ihrer Entschließung vom 10. Mai 2001 aufmerksam gemacht (vgl. Anlage 26).

Inzwischen gibt es einen neuen Verordnungsentwurf vom 6. September 2001. Danach sind wohl die Anbieter von Internet-Diensten nicht mehr von den Verpflichtungen nach der Verordnung betroffen. Verpflichtet sollen nur noch Zugangsanbieter bleiben, die einen sog. direkten Zugang ermöglichen. Bei dem gegenwärtigen Stand des Entwurfs geht der LfD davon aus, dass jene Zugangsanbieter, die keine Telefonanschlussleitung zur Verfügung stellen, nicht mehr von den Verpflichtungen der Telekommunikations-Überwachungsverordnung betroffen sind. Hier lässt sich eine – nach Auffassung des LfD – sinnvolle Entwicklung dahin gehend erkennen, die Telekommunikationsüberwachung auf die eigentliche Teilnehmeranschlussleitung zu beschränken. Es steht zu hoffen, dass diese positiven Ansätze auch in die Endfassung der Verordnung Eingang finden werden.

19.3 EG-Richtlinienentwurf zum Datenschutz in den elektronischen Kommunikationsmedien

Die Europäische Kommission hat dem Europäischen Parlament und dem Rat einen Vorschlag für eine Richtlinie über die Verarbeitung personenbezogener Daten und zum Schutz der Privatsphäre in der elektronischen Kommunikation – KOM(2000)385 – unterbreitet. Die vorgeschlagene Richtlinie soll die bisherige Telekommunikationsrichtlinie (97/66/EG) ersetzen. Der Richtlinienvorschlag bezweckt seiner Begründung nach die Aufrechterhaltung eines hohen Schutzniveaus für personenbezogene Daten und für die Privatsphäre der Bürger.

Mit dem Vorschlag sollen keine wesentlichen inhaltlichen Änderungen der geltenden Richtlinie vorgenommen werden, sondern lediglich die bisherigen Bestimmungen an neue und vorhersehbare Entwicklungen auf dem Gebiet der elektronischen Kommunikationsdienste und -technologien angepasst werden. Insbesondere soll der Anwendungsbereich der Richtlinie nicht mehr nur die Telekommunikationsdienste (z. B. Telefongesellschaften) umfassen, sondern auf alle elektronischen Kommunikationsnetze und -dienste ausgedehnt werden, also auch auf Provider oder sonstige Anbieter von Leistungen im Internet.

So werden z. B. die sog. „Verkehrsdaten“ neu definiert. Die alte Richtlinie bezog sich noch ausdrücklich auf Daten über den „Verbindungsaufbau“. Eine weitere Änderung betrifft die Teilnehmerverzeichnisse. Kommunikationsdienstleister sollen verpflichtet werden, die Nutzenden zu fragen, ob sie in öffentliche Verzeichnisse aufgenommen werden wollen. Diese sollen vollständig informiert werden, welche Daten von ihnen für welchen Zweck erfasst werden. Angestrebt wird der Erlass technikneutraler Regelungen. Weiterhin sollen Nutzer unabhängig von der Technologie, mit deren Hilfe ein bestimmter Dienst angeboten wird, einen einheitlichen Schutz genießen.

Die Richtlinie enthält auch eine Bestimmung, in der die Befugnisse der Diensteanbieter zur Verarbeitung von Standortdaten der Nutzer und Teilnehmer in elektronischen Kommunikationsnetzen geregelt wird. Solche Standortdaten geben den geographischen Standort eines mobilen Endgerätes und damit auch des entsprechenden Nutzers an. Es ist offensichtlich, dass damit neue Gefährdungen des Persönlichkeitsrechts der Mobilfunknutzer einhergehen können. Daher wird hinsichtlich mobiler Nutzer festgelegt, dass Standortdaten nur mit Einwilligung des Teilnehmers verwendet werden dürfen und dass er die Verarbeitung seiner Standortdaten auf genauso einfache Weise zeitweise unterdrücken kann, wie das für die Anzeige der Rufnummer des Anrufers im Festnetz der Fall ist. Ausgenommen werden „Standortdaten von Notdiensten“.

In Art. 1 Abs. 3 sind die Ausnahmen festgelegt, auf welche die Richtlinie nicht anzuwenden ist: Sie gilt „nicht für Tätigkeiten betreffend die öffentliche Sicherheit, die Landesverteidigung, die Sicherheit des Staates und die Tätigkeiten des Staates im strafrechtlichen Bereich“.

Europäisches Parlament und Europäischer Rat müssen dem Richtlinienvorschlag zustimmen. Ziel der Kommission ist es, die Richtlinie bis Mitte 2002 in Kraft zu setzen.

20. Medien

20.1 Entwurf eines Gesetzes über rechtliche Rahmenbedingungen für den elektronischen Geschäftsverkehr (Elektronischer Geschäftsverkehr-Gesetz-EGG)

Mit diesem Artikel-Gesetz soll die Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über den elektronischen Geschäftsverkehr (ABl. EG Nr. L 178/1 vom 17. Juli 2000) umgesetzt werden. Ziel der Richtlinie ist die Harmonisierung der geltenden innerstaatlichen Regeln für Dienste der Informationsgesellschaft und die Sicherstellung des freien Dienstleistungsverkehrs in diesem Bereich. Die Umsetzung der Richtlinie muss bis zum 17. Januar 2002 erfolgen.

Das EGG ist Teil eines Gesamtpaketes neuer Regelungen für die Informations- und Kommunikationsdienste, mit dem ein moderner Rechtsrahmen für den neuen Wirtschaftssektor geschaffen werden soll. Mit dazu gehören das inzwischen vom Bundesrat beschlossene neue Signaturgesetz und das Gesetz zur Anpassung der Formvorschriften des Privatrechts an den modernen Geschäftsverkehr. Diese Regelwerke sollen die Schaffung einer Sicherheitsinfrastruktur für qualifizierte elektronische Signaturen ermöglichen.

In Artikel 3 des Entwurfs sind Änderungsvorschläge für das Teledienstedatenschutzgesetz enthalten.

Gesetzlicher Handlungsbedarf besteht nach Auffassung der Bundesregierung insbesondere hinsichtlich der Optimierung des Teledienstedatenschutzgesetzes aufgrund der bisherigen Erfahrungen und Entwicklungen. Es wird im Wesentlichen zu folgenden Änderungen kommen:

- Konkretisierung des Geltungsbereichs: Das Teledienstedatenschutzgesetz soll nur noch im Verhältnis von Anbietern und Nutzern von Telediensten gelten. Personenbezogene Daten, die zur Steuerung von Geschäftsprozessen innerhalb oder zwischen Unternehmen oder öffentlichen Stellen verarbeitet werden, fallen nicht mehr in den Anwendungsbereich des Gesetzes.

- Verbesserung der Gesetzessystematik: Die im Gesetz enthaltenen Grundsätze, Pflichten und Erlaubnistatbestände sind übersichtlicher zugeordnet.

- Präzisierung der Einwilligung: Die bisherigen engen gesetzlichen Erlaubnisse für Einwilligungslösungen werden in dem Gesetzentwurf mit dem Ziel konkretisiert, die bestehenden Rechtsunsicherheiten zu beseitigen.

- Verhinderung des Missbrauchs von Telediensten: Um den Zugriff auf rechtswidrige Inhalte besser verfolgen zu können, wird ein neuer Erlaubnistatbestand zur Nutzung von personenbezogenen Daten für Zwecke der Strafverfolgung eingeführt. Dieser erlaubt die Protokollierung von Internetaktivitäten einzelner Verdächtiger, jedoch keine Vollprotokollierung der Internetaktivitäten sämtlicher Kunden.

- Einführung von Sanktionen: In Ergänzung zum Bundesdatenschutzgesetz werden nunmehr auch die wichtigsten Pflichten der Anbieter bußgeldbewehrt und damit den Datenschutzvorschriften größerer Nachdruck verliehen.

Mit der Modernisierung des Teledienstedatenschutzrechts soll das notwendige Vertrauen in die Nutzung der elektronischen Informations- und Kommunikationsdienste gestärkt, verbreiteten Befürchtungen vor Missbrauch von personenbezogenen Daten in den Netzen entgegengewirkt und eine größere Anwenderfreundlichkeit der Datenschutzvorschriften für die Diensteanbieter erreicht werden.

20.2 Das neue Signaturgesetz

Das Signaturgesetz aus dem Jahre 1997, das für die Zulassung der Trust-Center strenge Sicherheitsauflagen verlangt hat, musste an die europäische Signatur-Richtlinie 1999/93/EG vom 13. Dezember 1999 angepasst werden. Die EG-Richtlinie schafft gemeinsame rechtliche Rahmenbedingungen für elektronische Signaturen: einen freien Marktzugang für Anbieter, eine gerichtliche Anerkennung der elektronischen Signatur, die Gleichsetzung der elektronischen Signatur mit der handschriftlichen Unterschrift im materiellen Recht sowie eine Haftungsregelung des Anbieters.

Das deutsche Gesetz über Rahmenbedingungen für elektronische Signaturen vom 16. November 2000 (BGBl. I, 876) sieht nunmehr drei Typen von Signaturen vor: einfache, qualifizierte und qualifizierte mit freiwilliger Akkreditierung. Der dritte Typ entspricht weitgehend dem bisherigen deutschen Signaturgesetz (zu den Anforderungen an den Einsatz elektronischer Signaturlösungen in der Verwaltung vgl. Tz. 21.3.2).

Wenn die Verwaltung über das Internet nicht nur informieren und kommunizieren, sondern auch rechtsverbindliche Transaktionen abwickeln möchte, bedarf dies der Absicherung: Sicherung der Datenintegrität, der Authentifizierung ihrer Urheber und zum Schutz ihrer Vertraulichkeit elektronischer Signatur sowie Verschlüsselungsverfahren.

Art. 3 Abs. 7 der EG-Signatur-Richtlinie bestimmt: „Die Mitgliedstaaten können den Einsatz elektronischer Signaturen im öffentlichen Bereich möglichen zusätzlichen Anforderungen unterwerfen. Diese Anforderungen müssen objektiv, transparent, verhältnismäßig und nicht diskriminierend sein und dürfen sich nur auf die spezifischen Merkmale der betreffenden Anwendung beziehen. Diese Anforderungen dürfen für grenzüberschreitende Dienste für den Bürger kein Hindernis darstellen."

Durch diese Vorschrift wird zum einen klargestellt, dass der Einsatz elektronischer Signaturen im öffentlichen Bereich (z. B. im Gesundheitswesen) aus dem Anwendungsbereich der Richtlinie ausgenommen ist. Dieser kann von den Mitgliedstaaten zusätzlichen Anforderungen unterworfen werden. Daher sind etwa besondere sachlich gerechtfertigte Anforderungen an die Identifzierungs-, Warn-, Feststellungs- oder Beweisfunktion, die für elektronische Willenserklärungen in bestimmten Verwaltungsverfahren gestellt werden, zulässig.

20.3 Datenschutz bei der Befreiung von der Rundfunkgebühr (automatisierte Verfahrensbearbeitung)

Was die Verfahrensweise in Rheinland-Pfalz anbelangt, so wurde bislang der Antrag auf Rundfunkgebührenbefreiung von den Sozialämtern angenommen und nach Durchführung der entsprechenden Berechnung dort entschieden, in Papierform an die GEZ weitergegeben und von dieser elektronisch registriert. Dieses Vorgehen stimmt nur teilweise mit den Regelungen der Landesverordnung über die Voraussetzungen für die Befreiung von der Rundfunkgebührenpflicht überein. Dort ist in § 5 Abs. 2 vorgesehen, dass die Landesrundfunkanstalt über den Antrag auf Vorschlag der genannten Behörden (Sozialämter) entscheidet. Die Landesrundfunkanstalt kann die Behörden jedoch zur Aushändigung des Befreiungsbescheides ermächtigen.

Nunmehr ist ein automatisiertes Verfahren zur Bearbeitung von Anträgen zur Gebührenbefreiung in der Planung, das den Sozialämtern zur Verfügung gestellt werden soll. Das neue Programm kann für alle Gruppen von Antragsberechtigten (auch für Studierende) eingesetzt werden.

Es handelt sich um eine von der GEZ im Auftrag der Landesrundfunkanstalten entwickelte Software für PC. Das Programm soll es den Bearbeitern in den Sozialämtern ermöglichen, die Daten der Befreiungsanträge automatisiert zu erfassen und auf Plausibilität zu überprüfen. Die plausibilisierten Daten werden anschließend per E-Mail oder auf Diskette von den Sozialämtern an die GEZ bzw. an die jeweilige Landesrundfunkanstalt übermittelt. Im automatisierten Verfahren sollen die Sozialämter lediglich solche Entscheidungen im Auftrag der Landesrundfunkanstalt treffen, bei denen aufgrund der eindeutigen Datenlage dem Antrag stattgegeben werden muss. Dagegen sollen Fälle, bei denen Zweifel bestehen, und Fälle, bei denen aufgrund der Datenlage die Anträge abgelehnt werden müssen, durch die Landesrundfunkanstalt bzw. durch die GEZ entschieden werden.

Seitens des LfD bestehen keine Bedenken, dass die Sozialämter auch in Zukunft die Anträge auf Gebührenbefreiung entgegennehmen. Dabei muss jedoch sichergestellt sein, dass es zu keiner unzulässigen Nutzung von Daten kommt, die dem Sozialgeheimnis unterliegen.

Auf die in den Sozialämtern vorhandenen Unterlagen und auf die in automatisierten Verfahren der Sozialämter gespeicherten Sozialdaten darf daher nach Auffassung des LfD nur dann bei der Antragsprüfung zurückgegriffen werden, wenn und soweit die Betroffenen eingewilligt haben.

Im Übrigen ist darauf hinzuweisen, dass die Daten, die im Rahmen des Verfahrens zur Prüfung der Anträge auf Rundfunkgebührenbefreiung erhoben und gespeichert werden, der Zweckbindung unterliegen. Diese Daten dürfen sowohl von den Sozialämtern als auch seitens der Landesrundfunkanstalt nur für den Zweck verwendet werden, für den sie erhoben worden sind.

20.4 Datensparsamkeit bei der Rundfunkfinanzierung

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in ihrer Herbstsitzung 2000 im Zusammenhang mit der Diskussion um eine Neuregelung der Rundfunkfinanzierung einen Beschluss gefasst, in dem sie die Bundesländer auffordert, bei einer Neuordnung der Rundfunkfinanzierung ein Modell zugrunde zu legen, das sich stärker als das bisherige an den Prinzipien der Datenvermeidung, Datensparsamkeit und Dezentralisierung orientiert (vgl. Anlage 17). Es ist das gemeinsame datenschutzrechtliche Anliegen, bei der Weiterentwicklung des Systems der Rundfunkfinanzierung darauf hinzuwirken, dass personenbezogene Daten in möglichst geringem Umfang verarbeitet werden. Nach der Rechtsprechung des Bundesverfassungsgerichts verlangt Art. 5 Abs. 1 Satz 2 GG für die Festsetzung der Rundfunkgebühr ein Verfahren, das dem öffentlich-rechtlichen Rundfunk die zur Erfüllung seiner Aufgabe im dualen System erforderlichen Mittel gewährleistet und ihn vor Einflussnahme auf das Programm wirksam sichert (BVerfGE 90, 60; NJW 1994, 1942). Zuständig für die Erhebung der Rundfunkgebühr sind die Landesrundfunkanstalten, die allerdings diese Aufgabe an die GEZ delegiert haben. Die GEZ ist zwar nicht verfassungsrechtlich vorgegeben; das Einzugsverfahren muss aber staatsfern bleiben, damit kein unzulässiger Druck auf die Programmgestaltung ausgeübt wird. Nach Auffassung des LfD sollte jenen Bestrebungen entgegengewirkt werden, die eine Abschaffung der Rundfunkgebührenpflicht zugunsten einer Rundfunksteuer fordern. Er sieht in der Abschaffung der Gebühren eine Gefährdung der Unabhängigkeit des öffentlich-rechtlichen Rundfunks. Seine Position hat er in einem Schreiben an die Datenschutzbeauftragten des Bundes und der Länder dokumentiert. Als bewährte Rechtsgrundlage für den Rundfunkgebühreneinzug bleibt der jeweils durch die 16 Landesparlamente in Landesrecht transformierte Rundfunkgebührenstaatsvertrag bestehen. Er regelt mit enger Zweckbindung, welche Angaben jeder Rundfunkteilnehmer gegenüber der jeweiligen Rundfunkanstalt zur Einziehung der Rundfunkgebühr machen muss. Bei der Diskussion über alternative Formen der Gebührenerhebung sollte nicht in Vergessenheit geraten, dass bei der Schaffung des Staatsvertrages über den Rundfunk im vereinten Deutschland datenschutzrechtliche Anliegen im Rundfunkgebührenstaatsvertrag weitgehend berücksichtigt wurden.

20.5 Anfragen zur GEZ

In Eingaben werden häufig Fragen im Zusammenhang mit der Gebühreneinzugszentrale der öffentlich-rechtlichen Rundfunkanstalten in der Bundesrepublik Deutschland (GEZ) angesprochen. Soweit hier z. B. die Vorgehensweise eines Mitarbeiters der GEZ bzw. des Südwestrundfunks hinterfragt wird, ist der LfD für eine inhaltliche Stellungnahme nicht zuständig. Denn seine Zuständigkeit beschränkt sich auf Behörden und sonstige öffentliche Stellen des Landes Rheinland-Pfalz.

Die GEZ wird als Abteilung der jeweiligen Landesrundfunkanstalt angesehen, für die sie Gebühren einzieht. Sie hat das Datenschutzrecht des Sitzlandes der Rundfunkanstalt anzuwenden. Für Rheinland-Pfalz ist insoweit der Südwestrundfunk zuständig. Nach § 39 des Staatsvertrages über den Südwestrundfunk gelten für den Datenschutz beim SWR die auf Rundfunkanstalten anwendbaren Bestimmungen des Datenschutzgesetzes des Landes in der jeweils gültigen Fassung, in dem der Dienstort des Intendanten liegt. Da der Dienstort des Intendanten gem. § 1 Satz 3 des Staatsvertrages Stuttgart ist, gilt hier das baden-württembergische Landesdatenschutzgesetz (LDSG B-W). Entsprechende Regelungen sind in den §§ 31 und 32 enthalten. Die Aufgabe der datenschutzrechtlichen Kontrolle des Südwestrundfunks obliegt gem. § 32 Abs. 2 LDSG B-W dem Rundfunkbeauftragten für den Datenschutz (Adresse: Südwestrundfunk, Prof. Dr. Armin Herb, Neckarstr. 230, 70180 Stuttgart). Wenn die Petenten eine Überprüfung des von ihnen vorgetragenen Sachverhalts wünschen, haben sie die Möglichkeit, sich zuständigkeitshalber direkt dorthin zu wenden oder die Unterrichtung durch den LfD zu veranlassen.

Was die Fragen nach der Datenerhebung anbelangt, so kommen grundsätzlich die Meldebehörden als die Stellen in Betracht, die der Rundfunkanstalt Einwohnerdaten zur Verfügung stellen (vgl. dazu Tz. 4.5).

20.6 Datenschutz im rundfunkrechtlichen Erlaubnisverfahren

In einer Eingabe wurde die unbefugte Offenbarung personenbezogener Daten seitens der Landeszentrale für private Rundfunkveranstalter (LPR) beklagt. Aufgrund eines Beschlusses der Versammlung der LPR im rundfunkrechtlichen Erlaubnisverfahren für ein Fernsehprogramm ist ein entsprechender Bescheid ergangen. Adressat dieses Bescheides war sowohl die obsiegende als auch die unterlegene Anbietergemeinschaft, die sich aus einem eingetragenen Verein und einer Kommanditgesellschaft zusammensetzte, deren Kommanditisten und Vereinsmitglieder namentlich bzw. unter einer Familienbezeichnung in dem Bescheid der LPR aufgeführt waren.

Dieser beiden Anbietergemeinschaften im rundfunkrechtlichen Erlaubnisverfahren zugestellte Bescheid ist als ein Verwaltungsakt mit Doppelwirkung einzuordnen. Denn uno actu wird mit der antragsgemäß erteilten Erlaubnis an die obsiegende Anbietergemeinschaft diese begünstigt und die unterlegene Anbietergemeinschaft durch die Ablehnung ihres Antrags belastet.

Die Grundsätze des rundfunkrechtlichen Erlaubnisverfahrens sind in den §§ 5 ff. LRG geregelt. So hat der Antragsteller alle Angaben zu machen, alle Auskünfte zu erteilen und alle Unterlagen vorzulegen, die zur Prüfung des Antrags auf Erteilung der Erlaubnis erforderlich sind (vgl. § 7 Abs. 1 LRG). Darunter fallen gem. §§ 6 Abs. 1 Nr. 1 d und Nr. 6 i. V. m. 13 Nr. 5 sowie § 7 Abs. 2 LRG auch Angaben zu den Beteiligungsverhältnissen und zum Mitgliederbestand.

Die unterlegenen Antragsteller rügten in ihrer Eingabe an den LfD insbesondere die namentliche Benennung aller Kommanditisten samt ihren Kapitalanteilen als einen Verstoß gegen § 10 Satz 1 LRG. Danach dürfen Angaben über persönliche und sachliche Verhältnisse einer natürlichen oder juristischen Person oder einer Personengesellschaft sowie Betriebs- oder Geschäftsgeheimnisse, die der LPR, ihren Organen, ihren Bediensteten oder von ihr beauftragten Dritten im Rahmen der Durchführung ihrer Aufgabenerfüllung anvertraut oder sonst bekannt geworden sind, nicht unbefugt offenbart werden. Hintergrund der Regelung ist, dass die durch das Landesrundfunkgesetz geschaffenen Auskunftspflichten auch sensible persönliche und geschäftliche Daten betreffen. Diese werden durch § 10 LRG vor einer unbefugten Weitergabe geschützt. Die dortige Verweisung auf § 46 Abs. 9 des Gesetzes gegen Wettbewerbsbeschränkungen stellt sicher, dass die im Rahmen von Maßnahmen zur Sicherung von Meinungsvielfalt gewonnenen schutzwürdigen Daten nur für diese Zwecke Verwendung finden dürfen. Soweit personenbezogene Daten verarbeitet werden, finden gem. § 10 Satz 3 LRG die Bestimmungen des Landesdatenschutzgesetzes Anwendung, wobei zu beachten ist, dass sein Anwendungsbereich nach der Regelung in § 2 Abs. 5 LDSG beschränkt ist. So gilt das Landesdatenschutzgesetz nicht für Daten, solange sie in allgemein zugänglichen Quellen gespeichert sind oder wenn Betroffene bestimmte Daten zur Veröffentlichung bestimmt haben. Zu den allgemein zugänglichen Quellen rechnen z. B. Fernsprechverzeichnisse, Adressbücher sowie Register, aus denen personenbezogene Daten ohne Zugangsbeschränkung zur Kenntnis genommen werden können.

In diesem Zusammenhang war nun bedeutsam, dass die Kommanditisten einer KG gem. § 162 Abs. 1 HGB in das Handelsregister namentlich mit dem Betrag der Einlage eines jeden von ihnen einzutragen sind. Das Handelsregister ist ein von den Amtsgerichten geführtes öffentliches Register. Es kann von jedem, der sich informieren möchte, kostenlos eingesehen werden (§ 9 Abs. 1 HGB). Der Name des Kommanditisten und die von ihm geleistete Einlage sind mithin Informationen, bei denen das informationelle Selbstbestimmungsrecht der Betroffenen Einschränkungen unterliegt. Sie haben insofern nicht die Befugnis, über die Verbreitung ihrer Daten selbst zu bestimmen. Im Rahmen der datenschutzrechtlichen Beurteilung war also zu berücksichtigen, dass es sich um allgemein zugängliche Handelsregisterdaten handelt, die jedermann zur Kenntnis nehmen kann. Des Weiteren hat derjenige, der sich als Kommanditist an einer Kommanditgesellschaft beteiligt, mit dieser Entscheidung seine für die Eintragung ins Handelsregister erforderlichen personenbezogenen Daten selbst zur Veröffentlichung (im Handelsregister) bestimmt.

Selbst wenn man die Vorschriften des Landesdatenschutzgesetzes für anwendbar hielte, wäre die Nutzung der Daten aus dem Handelsregister nach § 13 Abs. 2 Nr. 1 i. V. m. § 12 Abs. 4 Nr. 9 LDSG zulässig, denn es handelt sich um Daten, die auch unmittelbar aus allgemein zugänglichen Quellen entnommen werden können, wobei mit Blick auf die obigen Ausführungen keine Anhaltspunkte vorliegen, dass hier überwiegende schutzwürdige Belange entgegenstehen. Da die Daten aus allgemein zugänglichen Quellen stammen, können schutzwürdige Belange erst durch das Hinzutreten weiterer Umstände, etwa durch die Verknüpfung mit anderen, nicht aus dem Handelsregister stammenden Informationen beeinträchtigt werden. Dies wäre z. B. dann der Fall, wenn die Aufstellung der Programmbezugsquellen (vgl. § 9 Abs. 2 LRG) durch die Darstellung im Bescheid der LPR Dritten personenbezogen bekannt gegeben würde. Bei dem zu beurteilenden Sachverhalt lag eine solche Situation nicht vor.

Hier wird deutlich, dass kein Verstoß gegen datenschutzrechtliche Bestimmungen vorliegt, wenn allgemein zugängliche Daten mit der Zustellung des Bescheids der obsiegenden Antragstellerin mitgeteilt werden.

Was die im Bescheid enthaltenen Angaben zu der Struktur des mehr als 20 Mitglieder umfassenden eingetragenen Vereins anbelangt, so war zunächst darauf hinzuweisen, dass nach § 79 Abs. 1 BGB die Einsicht in das Vereinsregister sowie der von dem Verein bei dem Amtsgericht eingereichten Schriftstücke jedem gestattet ist. Im Vereinsregister sind die Gründungsmitglieder (mindestens sieben) sowie die Funktionsträger (Vorsitzender, Kassierer) regelmäßig vermerkt (vgl. § 59 Abs. 3 i. V. m. § 64 Satz 1 BGB). Hinsichtlich der Ausführungen im Bescheid der LPR, wonach es sich bei den Vereinsmitgliedern fast ausschließlich um nicht näher benannte Mitglieder eines bestimmten Familienverbandes handelte, war zu untersuchen, ob es sich dabei um personenbezogene Daten im Sinne des Landesdatenschutzgesetzes handelt. Nach der Regelung in § 3 Abs. 1 LDSG sind personenbezogene Daten Einzelangaben über persönliche oder sachliche Verhältnisse natürlicher Personen. Kennzeichnend für den Begriff „Einzelangabe" ist, dass diese Informationen über eine bestimmte natürliche Person enthält. Angaben über Personenmehrheiten fallen nicht in den Schutzbereich des Landesdatenschutzgesetzes, was dazu führt, dass, bezogen auf die entsprechenden Ausführungen der LPR in dem Bescheid, die Voraussetzungen für das Vorliegen eines personenbezogenen Datums, nämlich die Zuordnung der jeweiligen Information zu einer einzelnen natürlichen Person, nicht erfüllt sind.

Nach allem kam der LfD zu dem Ergebnis, dass eine unbefugte Offenbarung personenbezogener Daten an die obsiegende Antragstellerin nicht vorlag. Die Verfahrensweise der LPR war datenschutzrechtlich nicht zu beanstanden.

20.7 Publizitätspflicht nach § 23 Rundfunkstaatsvertrag

Im Rahmen einer Eingabe hatte sich der LfD mit der Frage zu befassen, ob der Inhaber einer sog. Drittsendezeitlizenz – dies ist die Einräumung von Sendezeit für unabhängige Dritte als vielfaltssichernde Maßnahme gem. § 31 RfStV – den im Rundfunkstaatsvertrag niedergelegten Bestimmungen zur Veröffentlichung des Jahresabschlusses nachkommen muss. Der Petent sah in dieser Forderung der LPR einen Eingriff in seine Persönlichkeitsrechte und argumentierte, dass – bezogen auf seinen speziellen Fall – mit der Veröffentlichung des Jahresabschlusses faktisch seine persönliche Steuererklärung für jedermann einsehbar veröffentlicht wäre.

Ausgangspunkt der datenschutzrechtlichen Würdigung der Angelegenheit ist die Regelung in § 23 Abs. 1 RfStV. Dort wird jedem Rundfunkveranstalter die Verpflichtung auferlegt, jährlich seinen Jahresabschluss und einen Lagebericht nach Maßgabe derjenigen Vorschriften des Handelsgesetzbuches, die für sog. große Kapitalgesellschaften gelten, zu veröffentlichen. Die Regelung dient der Herstellung öffentlicher Transparenz in Bezug auf die Rundfunkveranstalter. Die wirtschaftlichen Träger der durch Rundfunk verbreiteten öffentlichen Meinung werden einer beobachtenden Kontrolle durch die Öffentlichkeit unterworfen.

In diesem Zusammenhang ist von entscheidender Bedeutung, ob es sich bei den nach den Vorschriften des Handelsgesetzbuches vorzulegenden Daten um personenbezogene Daten im datenschutzrechtlichen Sinne handelt. Was den Anwendungsbereich des hier einschlägigen Landesdatenschutzgesetzes anbelangt, gilt es nach der Regelung in § 2 Abs. 5 LDSG nicht für Daten, solange sie in allgemein zugänglichen Quellen gespeichert sind oder wenn Betroffene bestimmte Daten zur Veröffentlichung bestimmt haben.

Zu den allgemein zugänglichen Quellen rechnen z. B. Register, aus denen personenbezogene Daten ohne Zugangsbeschränkung zur Kenntnis genommen werden können. Vorliegend ist darauf hinzuweisen, dass die gesetzlichen Vertreter einer Kapitalgesellschaft stets – unabhängig von der Sonderregelung in § 23 RfStV – gem. §§ 325 ff. HGB ihre offen zu legenden Unterlagen (dazu gehören regelmäßig die Bilanzdaten i. S. v. § 266 HGB) zum Handelsregister einzureichen und anschließend unverzüglich im Bundesanzeiger einen Hinweis bekannt zu machen haben, bei welchem Handelsregister und unter welcher Nummer die Unterlagen eingereicht worden sind. Das Handelsregister ist ein von den Amtsgerichten geführtes öffentliches Register. Es kann von jedem, der sich informieren will, kostenlos eingesehen werden (§ 9 Abs. 1 HGB). So sind Bilanzdaten mithin Informationen, die nicht primär der Individualsphäre des geschäftsführenden Gesellschafters zuzuordnen sind und daher nicht dem informationellen Selbstbestimmungsrecht des Betroffenen selbst unterliegen. Im Rahmen der datenschutzrechtlichen Beurteilung ist also zu berücksichtigen, dass es sich um allgemein zugängliche Handelsregisterdaten handelt, die als solche keinen besonderen Schutz genießen.

Im Übrigen hat derjenige, der sich als Rundfunkveranstalter betätigt, mit dieser Entscheidung seine – im Rahmen des § 23 Abs. 1 RfStV erforderlichen – Daten selbst zur Veröffentlichung bestimmt. Da die vorgenannte Bestimmung nicht nach der Größe der Rundfunkveranstalter unterscheidet, ist allgemein davon auszugehen, dass Interessenten, die sich aufgrund einer Ausschreibung für eine Drittsendezeitlizenz und damit als Veranstalter bundesweiten Fernsehens bewerben, die Bedingungen, unter denen ein Zu-

schlag erfolgt (also insbesondere die rechtlichen Rahmenbedingungen, wie sie sich aus den Vorschriften des Rundfunkstaatsvertrags ergeben) voll inhaltlich bekannt sind. Hier wird deutlich, dass angesichts dieser Sachlage auch der Aspekt des Vertrauensschutzes nicht greift.

Nach allem war nach Auffassung des LfD aufgrund des ihm vorgetragenen Sachverhalts ein Verstoß gegen datenschutzrechtliche Vorschriften nicht festzustellen.

20.8 Neue Medienordnung

Zwischen Bund und Ländern haben auf politischer Ebene im Spätsommer 2001 Sondierungsgespräche zur Reform der Medienordnung stattgefunden. Die Zersplitterung des Datenschutzrechts im Medien- und Telekommunikationsbereich soll beseitigt werden mit dem Ziel, den Datenschutz für die Bürgerinnen und Bürger transparenter zu machen.

Es sind Bestrebungen im Gange, den Telekommunikations- und Multimediadatenschutz in das Bundesdatenschutzgesetz zu überführen, verbunden mit einer Neuordnung der Zuständigkeiten im Datenschutz. Das novellierte Teledienstedatenschutzgesetz soll im Dezember 2001 in Kraft treten. Im Anschluss daran soll auch der Mediendienste-Staatsvertrag entsprechend angepasst werden. Die geplante Neuordnung könnte dann möglicherweise Bestandteil der zweiten Stufe der BDSG-Novellierung werden.

In diesem Zusammenhang stellt sich das Problem, ob Kompetenzen im Mediendatenschutz dem Bund überhaupt übertragen werden können und ob eine Differenzierung zwischen der Regelungskompetenz und der Kontrollkompetenz stattfinden soll. Entscheidend aus datenschutzrechtlicher Sicht ist, dass die Neuordnung des Telekommunikations- und Multimediarechts nicht zu einer Senkung des Datenschutzniveaus führen darf.

Der Meinungsbildungsprozess in Bund und Ländern ist insoweit noch nicht abgeschlossen.

21. Technischer und organisatorischer Datenschutz

Bedeutung und Umfang des Einsatzes automatisierter Verfahren haben deutlich zugenommen. In vielen Bereichen der öffentlichen Verwaltung ist der Einsatz von Informations- und Kommunikationstechnik für die Aufgabenerfüllung unverzichtbar geworden. Neben der flächendeckenden Einführung von IT-Lösungen in bislang nur teilweise automatisierten Bereichen (z. B. in der Justiz) führt insbesondere der Ersatz bzw. die Erweiterung vorhandener Verfahren durch aktuelle technische Lösungen zu datenschutzrechtlichen Fragen und, damit verbunden, zu einem erhöhten Kontroll- und Beratungsaufwand.

In bedeutsamen Verwaltungsbereichen erfolgt gegenwärtig eine Neustrukturierung der Informationsverarbeitung. Aktuelle Beispiele sind Polizei (INPOL-Neu, POLADIS-Neu), Meldewesen (EWOIS-Neu) oder Finanzverwaltung (FISCUS). Gleiches gilt für die Weiterentwicklung der Kommunikationsinfrastruktur der Verwaltung im Rahmen des vom DIZ betriebenen Landesdaten- und Kommunikationsnetzes – LDKN (rlp-Netz). Der veränderte Betrieb des Netzes als zentrale Infrastruktur für Informations- und Kommunikationsdienste verschiedener Verwaltungs- und Wirtschaftsbereiche hat dazu geführt, dass seit seiner Umstrukturierung regelmäßig datenschutztechnische Fragen an den LfD herangetragen wurden.

Von zunehmender Bedeutung ist weiterhin die Neukonzeption von Verwaltungsverfahren unter Einbeziehung Dritter. Erste Pilotversuche zur Televerwaltung zeigen, dass die elektronische Einbeziehung der Verfahrensbeteiligten verstärkt zur Behandlung auch technischer Fragen des Datenschutzes führt. Es ist erkennbar, dass dies im Rahmen der Neuorganisation der Mittelinstanzen und der Multimedia-Initiativen der Landesregierung weiter ansteigen wird.

21.1 Kontroll- und Beratungstätigkeit

Im Berichtszeitraum wurden in 48 Fällen örtliche Feststellungen unter technisch-organisatorischen Gesichtspunkten in unterschiedlichen Bereichen der staatlichen und kommunalen Verwaltung getroffen, u. a. bei folgenden Stellen:

- Amtsgerichten
- Daten- und Informationszentrum Rheinland-Pfalz
- Finanzämter
- Gymnasien
- Kreisverwaltungen
- Landesversicherungsanstalt
- Medizinischer Dienst der Krankenversicherung
- Oberfinanzdirektion
- Polizeiinspektionen
- Polizeipräsidien
- Stadtverwaltungen
- Statistisches Landesamt
- Universität Mainz
- Universitätsklinikum Mainz
- Verbandsgemeinden
- Zentralstelle für Polizeitechnik.

Ergänzt wurden diese durch 19 informatorische Feststellungen, überwiegend zur Klärung des technischen Verfahrensstands. Die Kontrollen erfolgten sowohl in Form allgemeiner Prüfungen als auch unter ausgewählten Gesichtspunkten. Angesichts der personellen Situation der Dienststelle im technischen Bereich hatten anlassbezogene Prüfungen Vorrang vor anlassunabhängigen Kontrollen. Weiterhin wurden aufgrund aktueller Entwicklungen und Änderungen der IT-Strukturen schwerpunktmäßig die Bereiche Polizei, Finanzverwaltung, Sozial- und Gesundheitsverwaltung, Einwohnerwesen und Televerwaltung datenschutzrechtlich begleitet und eine Datenschutzkontrolle in anderen Bereichen zurückgestellt.

Die für eine aussagekräftige datenschutzrechtliche Beurteilung erforderlichen technischen Kenntnisse betreffen zunehmend spezialisierte Bereiche (Chipkartentechnik, Kryptografie, Mobilfunk etc.). Die Heterogenität des IT-Einsatzes und die größere Einsatzbreite der Informationstechnik machen in der Kontroll- und Beratungspraxis vielfach eine intensive Auseinandersetzung mit sehr unterschiedlichen und komplexen Verfahren notwendig. Der LfD hat sich daher dafür eingesetzt, die haushaltsmäßigen Voraussetzungen für eine fallweise Vergabe entsprechender Gutachten und Dienstleistungen zu schaffen. Dem wurde für den Doppelhaushalt 2000/2001 entsprochen. Die Einbeziehung eines Beratungsunternehmens ist erstmals im Rahmen des Penetrationstests des Landesdaten- und Kommunikationsnetzes erfolgt (siehe 21.2.2.3).

Beratungen nach § 24 Abs. 4 LDSG sind in 52 Fällen erfolgt. Die Tendenz, den LfD bereits im Vorfeld geplanter Umstrukturierungen des IT-Einsatzes oder im Zusammenhang mit der Erstellung von Sicherheitskonzepten zu beteiligen, hat sich fortgesetzt. Daneben wurden die Behörden und sonstigen öffentlichen Stellen des Landes und der Kommunen in zahlreichen technischen und organisatorischen Einzelfragen des Datenschutzes beraten.

Die Schulungsaktivitäten wurden im bisherigen Umfang fortgeführt.

21.2 Technisch-organisatorische Datenschutzfragen in ausgewählten Verfahren

21.2.1 Einwohnerinformationssystem Rheinland-Pfalz (EWOIS)

21.2.1.1 Neukonzeption des Verfahrens

Rheinland-Pfalz verfügt als einziges Flächenland über ein zentrales landeseinheitliches Verfahren zur Verarbeitung von Meldedaten. Nach über dreißigjährigem Betrieb wurde eine grundlegende Neukonzeption vorgenommen (vgl. 17. Tb., Tz. 4.1). Die Entwicklung des Nachfolgeverfahrens wurde zwischenzeitlich weitgehend abgeschlossen. Im Gegensatz zum bisherigen Verfahren basiert die künftige Lösung sowohl auf zentralen als auch auf dezentralen Komponenten. Grundsätzlich halten die Meldeämter lokale Datenbestände mit den Meldedaten ihres Zuständigkeitsbereichs vor. Für bestimmte Verfahrensfunktionen wird darüber hinaus ein zentraler Meldedatenbestand gebildet, der regelmäßig mit den lokal vorgehaltenen Daten abgeglichen und aktualisiert wird (Integrationssystem). Aus diesem wird wiederum ein reduzierter Datenbestand erzeugt, der insbesondere für Abfragen durch Stellen der Landesverwaltung zur Verfügung stehen soll.

Vor dem Hintergrund der in der Vergangenheit für das bisherige Verfahren problematisierten Gesichtspunkte hat der LfD im Blick auf die Neukonzeption folgende grundsätzlichen technisch-organisatorischen Anforderungen formuliert:

a) Benutzerverwaltung auf der Grundlage der vorhandenen Funktionsgruppensystematik

   Ein Zugriff auf EWOIS-Daten und -Funktionen darf erst nach einer erfolgreichen Identifikation und Authentifizierung der jeweiligen Stelle möglich sein. Voraussetzung für die gezielte Bereitstellung von EWOIS-Daten ist die eindeutige Bezeichnung der abrufenden Stelle. Die Benutzerverwaltung sollte sich daher an der vorhandenen Funktionsgruppensystematik orientieren, d. h. dem aus der funktionalen Aufgabe der zugreifenden Stelle abgeleiteten Aufbau der Benutzerkennung.

b) Regionale Differenzierung von Zugriffen und Auswertungen

   Der Umfang eines Zugriffs auf den zentralen Bestand und entsprechende Auswertungen müssen nach regionalen Gesichtspunkten wie der Zugehörigkeit zu bestimmten Verwaltungseinheiten oder der örtlichen Zuständigkeit der zugreifenden Stelle differenziert werden können. Grundlage hierfür sollte ebenfalls die o. g. Funktionsgruppensystematik sein.

c) Inhaltliche Differenzierung von Zugriffen und Auswertungen

   Eine Differenzierung des Zugriffs auf Daten und Funktionen muss weiterhin nach inhaltlichen Kriterien möglich sein. Für das Informationssystem ist sicherzustellen, dass EWOIS-Auskünfte auf die zulässigen Angaben beschränkt werden können. Das Datenmodell und die Erstellung von Auskunftsformaten muss flexibel genug sein, um erforderliche Änderungen zeitnah und mit angemessenem Aufwand umsetzen zu können. Bestimmte Daten (z. B. Religionszugehörigkeit, Adoptionsangaben, Historiendaten) unterliegen nach den melderechtlichen Vorschriften besonderen Regelungen beim Zugriff und bei der Löschung. Dies muss im Verfahren abgebildet werden.

d) Protokollierung

Die Nutzung des Verfahrens, d. h. der Aufruf von Funktionen und Zugriffe auf den zentralen Datenbestand, muss in ausreichendem Umfang nachvollziehbar sein. Entsprechend den vom LfD formulierten Grundsätzen soll sich aus der Protokollierung beantworten lassen, wer wann welche Verarbeitung i. S. von § 3 Abs. 2 LDSG veranlasst oder durchgeführt hat (vgl. auch 15. Tb., Tz. 21.8). Folgende Bereiche sind dabei von Bedeutung:
- Sperrung bei mehrfachen fehlerhaften Anmeldeversuchen
- Programm- und Funktionsaufrufe
- Neuaufnahme, Änderung und Löschung/Sperrung personenbezogener Daten
- Abfrage, Auswertung, Übermittlung personenbezogener Daten
- Ergebnisse von Auswertungen mit Zahl der Fälle und Kennzeichnung der Ausgabeform (Bildschirmanzeige, Ausdruck, Ausgabedatei)
- Einrichten, Löschen und Sperren von Benutzerdaten
- Änderung und Vergabe von Zugriffsrechten
- Änderungen der Systemkonfiguration.

Die Anzahl und der Umfang der protokollierten Aktivitäten sind an der Sensibilität der verarbeiteten Daten sowie dem Verwendungszweck zu orientieren. Dementsprechend kann – wie bereits für das gegenwärtige EWOIS praktiziert – auch eine stichprobenweise Protokollierung datenschutzrechtlichen Anforderungen genügen. Um die Nachvollziehbarkeit zu gewährleisten, müssen weiterhin angemessene Auswertungsfunktionen zur Verfügung stehen; die Auswertung von Protokolldaten darf nicht mit einem übermäßigen zeitlichen, finanziellen oder personellen Aufwand verbunden sein.

e) Sicherung der Kommunikation

Soweit ein Zugriff auf den zentralen Bestand nicht über das LDKN, sondern über öffentliche Kommunikationswege erfolgt, ist durch eine Verschlüsselung eine ausreichende Vertraulichkeit der EWOIS-Daten bei der Übertragung zu gewährleisten.

Das Innenministerium hat den Empfehlungen des LfD in der Verfahrenskonzeption Rechnung getragen.

21.2.1.2 Betrieb des Verfahrens

Für das gegenwärtige Verfahren liegen Verfahrenspflege und -betrieb in Händen des DIZ. Der Betreiber des künftigen Verfahrens soll im Rahmen einer offenen Ausschreibung ermittelt werden. Der Betrieb des Integrationssystems und des Informationssystems wird getrennt ausgeschrieben. Die vorgesehenen Aufgaben des Betreibers sollen dabei über den rein technischen Betrieb der Systeme und die Datenhaltung hinausgehen und auch die Wahrnehmung zentraler Verfahrensfunktionen sowie die Softwarewartung und -pflege und gegebenenfalls die technische Weiterentwicklung des Verfahrens umfassen. Dies wird für das Integrationssystem im Auftrag einer gemeinsamen Tochtergesellschaft des Gemeinde- und Städtebundes und des Städtetages erfolgen; diese wiederum handelt im Rahmen eines Vertrags mit den Kommunen. Ähnliches ist für den Betrieb des Informationssystems vorgesehen. Es bleibt abzuwarten, ob durch diese Rahmenbedingungen die Datenschutzkontrolle durch den LfD, insbesondere die Durchführung örtlicher Feststellungen bzw. die Umsetzung notwendiger Verfahrensanpassungen, beeinträchtigt wird.

Die technisch-organisatorischen Anforderungen an den Verfahrensbetrieb sind nach Auffassung des LfD für öffentliche und nichtöffentliche Stellen im Wesentlichen gleich. Ein mit der Vergabe an einen nicht öffentlichen Auftragnehmer verbundener Wegfall der im Rahmen der Rechts- und Fachaufsicht möglichen direkten Einwirkungsmöglichkeiten muss durch eine entsprechende Vertragsgestaltung kompensiert werden. Seitens des LfD wurde in diesem Zusammenhang erneut darauf hingewiesen, dass die im Rahmen der Datenschutzkontrolle entstehenden Kosten als Gemeinkosten des Verfahrens zu berücksichtigen sind, d. h. den kontrollierten Stellen nicht gesondert in Rechnung gestellt werden dürfen. Seitens des Innenministeriums wurde dies zugesichert. Weiterhin ist beim Betreiber ein dem IT-Grundschutzhandbuch des BSI entsprechendes Sicherheitsniveau sicherzustellen. Über die Umsetzung ist ein Nachweis zu erbringen (Sicherheitskonzept). Für Integrationssystem und Informationssystem sind gleiche Sicherheitsanforderungen zu stellen.

Soweit eine Anbindung abfragender Stellen an die zentralen Verfahrenskomponenten Integrationssystem und Informationssystem nicht über das rlp-Netz erfolgen soll, wurde seitens des LfD darauf hingewiesen, dass für eine angemessene Vertraulichkeit der Kommunikation und verlässliche Authentifizierung der Teilnehmer der Einsatz kryptografischer Verfahren erforderlich ist. Wenn dies sichergestellt wird, ist die Wahl des Providers von untergeordneter Bedeutung. Weiterhin darf eine Kommunikation zwischen abfragenden Stellen innerhalb und einem Betreiber außerhalb des rlp-Netzes aus Sicht des LfD nicht dazu führen, dass das vorhandene Sicherheitskonzept für das rlp-Netz aufgebrochen wird. Insbesondere kann ein nicht öffentlicher Betreiber außerhalb Rheinland-Pfalz nicht in das Teilnetz Verwaltung (bzw. der Polizei) des Landesnetzes integriert werden. Möglich ist aus Sicht des LfD die Bildung eines separaten Teilnetzes für den Betreiber und die gesicherte und kontrollierte Kommunikation zwischen diesem und dem LDKN-Teilnetz der abfragenden Stelle.

Den Kommunen soll für die dezentralen Datenbestände ein Hosting-Modell angeboten werden. Seitens des LfD wurden dagegen keine Bedenken erhoben, soweit es sich dabei um getrennte und separat verwaltete Bestände handelt. Bestandsübergreifende Auswertungen dürfen nicht möglich sein. Eine Aufgabe dieses Instanzenkonzepts und die Zusammenlegung eigentlich dezentraler Bestände ist aus Sicht des LfD problematisch.

21.2.2 Landesdaten- und Kommunikationsnetz

21.2.2.1 Änderung der Netzstruktur

Die Liberalisierung des Telekommunikationsmarktes und geänderte Anforderungen der Verwaltungen haben bei Struktur und Nutzung des Landesnetzes zu Veränderungen geführt. Bislang konnte das Landesnetz aufgrund seiner technischen Infrastruktur und des überschaubaren, weitgehend homogenen und ausschließlich aus Verwaltungen bestehenden Teilnehmerkreises als internes Netz der Verwaltung in Rheinland-Pfalz angesehen werden. Diese Situation ändert sich. Künftig ist die Auflösung des bisherigen Backbones und ein dreistufiger Aufbau des Landesnetzes auf der Grundlage von ATM-Verbindungen auf allen Netzebenen vorgesehen. Grundsätzlich sollen die vom DIZ angebotenen Kommunikationsleistungen bei Bedarf von wechselnden Providern erbracht werden können.

Auf der oberen Netzebene werden ausschließlich Vermittlungseinrichtungen des Providers genutzt. Deren Verbindungswege liegen grundsätzlich nicht fest und werden, abhängig von der Netzlast und dem Bandbreitenbedarf, dynamisch zugewiesen; die technische Wegeführung obliegt ausschließlich dem Provider und ist durch das DIZ nicht beeinflussbar. In der mittleren Ebene werden die Vermittlungseinrichtungen vom DIZ administriert. Sie sind, von Ausnahmen abgesehen, in regionalen Einrichtungen des Providers untergebracht. Die untere Netzebene in Form der bei den Verwaltungen vorhandenen Zugangskomponenten zum rlp-Netz wird auch weiterhin durch das DIZ verwaltet und technisch betreut.

Im Vergleich zur bisherigen Situation ergeben sich damit folgende, datenschutzrelevante Veränderungen: Die Knoten der mittleren Netzebene stehen nicht mehr in Räumlichkeiten des Landes, sondern grundsätzlich in – nach Auskunft des DIZ – besonders gesicherten Räumen des Providers. Die Wegeführung im Bereich der oberen Netzebene ist durch das DIZ nicht steuerbar. Die Zugriffsmöglichkeiten auf Vermittlungseinrichtungen liegen damit in bestimmten Fällen außerhalb der Kontrolle des DIZ. Mit der vorgesehenen Inanspruchnahme wechselnder Provider werden Telekommunikationsdienstleistungen gegebenenfalls unter unterschiedlichen oder nicht abschätzbaren Sicherheitsbedingungen erbracht.

Die bisherige Unterbringung der Knotenrechner in Stellen der Landesverwaltung hat gezeigt, dass dies nicht zwingend ein besonderes Maß an Zugangskontrolle gewährleistet. Eine Aufstellung in Räumen des Providers, die besonderen Sicherheitsanforderungen genügt, kommt daher aus Sicht des LfD alternativ in Betracht, soweit die Konfigurationshoheit der Komponenten weiterhin beim DIZ verbleibt. Für die Steuerung, ob und unter welchen Voraussetzungen der Provider auf die Komponenten zugreifen kann und ob dies durch das DIZ erkannt wird, sind akzeptable Lösungen denkbar. Hierzu zählen auf der Basis einer Risikoanalyse und eines darauf aufbauenden Sicherheitskonzepts u. a.

- die Formulierung von Sicherheitsleitlinien für das LDKN,
- die verlässliche Abschottung zu schützender Teilbereiche,
- die Kontrolle der Netzzugänge,
- die Sicherung der Übergänge zu anderen Kommunikationsnetzen,
- der sichere Betrieb der Netzinfrastruktur,
- die Bereitstellung vertrauenswürdiger Kommunikationsdienste,
- die verlässliche Authentisierung der an einer Kommunikation beteiligten Netzkomponenten und Stellen sowie dokumentierte und für die Nutzer verbindliche Anschlussvoraussetzungen und Sicherheitsrichtlinien.

21.2.2.2 Einsatz kryptografischer Verfahren im LDKN

Auf der Grundlage der Empfehlungen im 16. und 17. Tb. hat der LfD die Auffassung vertreten, dass insbesondere der Einsatz kryptografischer Verfahren für die Sicherung der Übertragungswege von Bedeutung ist. Soweit damit eine ausreichende Vertraulichkeit der Kommunikation, die Integrität der Daten und die Authentisierung der Netzkomponenten gewährleistet wird, sind Wahl des Providers und Wegeführung nachrangig.

Dem DIZ kommt nach Auffassung des LfD im Rahmen des Betriebs des rlp-Netzes nach § 3 Abs. 4 des Landesgesetzes zur Errichtung des Daten- und Informationszentrums Rheinland-Pfalz die Aufgabe zu, eine sichere und vertrauenswürdige Infrastruktur für die IT-Kommunikation der Verwaltung zur Verfügung zu stellen. Angesichts veränderter Rahmenbedingungen bei Struktur und Nutzung des rlp-Netzes besteht nach seiner Auffassung die Notwendigkeit, die Übertragung sensibler personenbezogener Daten auch innerhalb des Landesnetzes durch wirtschaftlich vertretbare kryptografische Maßnahmen abzusichern. Entsprechende Empfehlungen wurden von mehreren Seiten ausgesprochen und von einer mit der Untersuchung der Sicherheit im rlp-Netz befassten Arbeitsgruppe aufgegriffen.

Das DIZ hat in der Folge geeignete Lösungen erprobt und in sein Leistungsangebot aufgenommen. In Verbindung mit einem rlp-Netz-Zugang wird künftig eine Verbindungsverschlüsselung zwischen den beteiligten Netzknoten angeboten. Es handelt sich

dabei um eine Zusatzkomponente, die als sog. „Krypto-Box" zwischen dem IT-System des Netzteilnehmers und dessen Zugang zum rlp-Netz installiert wird. Die Verschlüsselung erfolgt automatisch und benutzertransparent für die gesamte Kommunikation, die über die jeweilige Verbindung geführt wird; grundsätzliche technische oder Leistungsprobleme sind nicht zutage getreten. In kryptografischer Hinsicht entspricht die Lösung den Empfehlungen des LfD (vgl. 17. Tb., Tz. 21.3.10). Neben der kryptografischen Sicherung auf der Verbindungsebene bietet das DIZ für die gesicherte E-Mail-Kommunikation auf Anwendungsebene eine Verschlüsselungs- und elektronische Signaturlösung auf der Basis einer Chipkarte an. Aus Sicht des LfD wurden damit die technischen Voraussetzungen zur Einrichtung vertrauenswürdiger Kommunikationswege geschaffen. Einer flächendeckenden Ausstattung des rlp-Netzes mit Krypto-Boxen stehen nach Aussage des DIZ allerdings wirtschaftliche Gesichtspunkte entgegen. Angesichts der damit verbundenen Kosten will das DIZ die Verbindungsverschlüsselung lediglich als optionale Leistung anbieten.

Sollte aus wirtschaftlichen Überlegungen auf die standardmäßige Ausstattung der rlp-Netz-Zugänge mit Kryptokomponenten verzichtet werden, wäre die Notwendigkeit der Verschlüsselung im Blick auf § 9 Abs. 2 Satz 1 LDSG jeweils verfahrensabhängig zu prüfen; diese Verantwortung liegt bei den angeschlossenen öffentlichen Stellen. Nach den Feststellungen des LfD verfügen diese allerdings häufig nicht über die Informationen, die für eine realistische Einschätzung des Sicherheitsniveaus der vom DIZ bereitgestellten Übertragungswege erforderlich sind. Inwieweit die rlp-Netz-Verbindungen unter Inanspruchnahme mehrerer Telekommunikationsdienstleister bereitgestellt werden, welche Sicherheitsanforderungen dabei erfüllt sind und welche Zugriffsmöglichkeiten Dritter gegebenenfalls bestehen, entzieht sich in der Regel deren Kenntnis. Bei lediglich optional angebotenen Verschlüsselungslösungen muss daher seitens des DIZ eine entsprechende Unterrichtung der Teilnehmer des rlp-Netzes erfolgen, so dass diese die genannten Gesichtspunkte bei der Prüfung berücksichtigen können. Gegenwärtig erfolgt dies nicht.

Angesichts der unterschiedlichen Sensibilität von Datenübertragungen, verwaltungsseitig häufig noch nicht vorhandener Verschlüsselungsmöglichkeiten und der Zunahme der elektronischen Kommunikation ist aus Sicht des LfD daher in erster Linie eine obligatorische Leitungsverschlüsselung geeignet, um die notwendige Vertraulichkeit innerhalb des rlp-Netzes sicherzustellen. Die absehbare weitere Öffnung des Landesnetzes im Zusammenhang mit der Neugestaltung des Einwohnerinformationssystems sowie die beabsichtigte Einführung elektronischer Vorgangsverwaltungs- und -bearbeitungssysteme in der Mittelinstanz untermauern diese Auffassung.

Die Polizei Rheinland-Pfalz, als ein bedeutsamer Bereich mit besonders schützenswerten Informationen, beabsichtigt, bei Vorliegen der haushaltsmäßigen Voraussetzungen die elektronische Kommunikation zwischen ihren Dienststellen generell zu verschlüsseln. Dies wird vom LfD ausdrücklich begrüßt. Ein vergleichbarer Schutz der im rlp-Netz genutzten Verbindungswege ist aus seiner Sicht insbesondere für die Kommunikation der Bereiche Justiz, Finanzverwaltung, Sozial- bzw. Gesundheitsverwaltung und Telemedizin von Bedeutung.

21.2.2.3 Penetrationstest der Firewall des LDKN

Im 16. Tb. wurde das Konzept des DIZ zur Absicherung der Internet-Anbindung des Landesnetzes dargestellt. Um eine verlässliche Bewertung des damit erreichten Sicherheitsniveaus zu ermöglichen, hat der LfD unter Einbeziehung eines entsprechenden Unternehmens einen Penetrationstest der zentralen Firewall des rlp-Netzes durchgeführt.

Auf der Grundlage bekannter Sicherheitslücken und Angriffsszenarien wurden Ausspähversuche unternommen und die Verwundbarkeit des Landesnetzes gegenüber Angriffen aus dem Internet untersucht. Im Ergebnis war es im Rahmen der Penetrationstests nicht möglich, aus dem Internet direkt auf Systeme im Verwaltungsnetz zuzugreifen. Denial of Service-Angriffe, d. h. Versuche, die Funktionsfähigkeit der Firewall oder nachgelagerter Systeme zu beeinträchtigen, blieben weitgehend ohne Wirkung. Die Tests sowie eine ergänzende Analyse der Firewall-Konfiguration haben jedoch auch Hinweise auf einzelne Schwachstellen ergeben, deren Beseitigung erforderlich ist, um den hohen Sicherheitsanforderungen an das Landesnetz zu genügen.

So haben sich die der Firewall vorgelagerten Internet-Server in Teilbereichen als angreifbar erwiesen. Auch wenn damit kein direkter Zugriff auf Systeme im Landesnetz möglich war, konnten weiter gehende und aussichtsreiche Angriffe auf diesen Schwachstellen aufbauen. Das DIZ hatte entsprechende Sicherheitsmaßnahmen bereits vorgesehen. Der Test hat nachdrücklich die Notwendigkeit bestätigt, die eingeleiteten Maßnahmen konsequent fortzusetzen. Er hat weiterhin deutlich gemacht, dass die Internet-Absicherung des Landesnetzes einer ständigen Beobachtung und Pflege bedarf, um den Sicherheitsanforderungen dauerhaft gerecht zu werden.

Die aus der Sicherheitsuntersuchung abgeleiteten Empfehlungen wurden, soweit kurzfristig möglich, umgesetzt. In einer überarbeiteten Firewall-Struktur sollen die ausstehenden Maßnahmen berücksichtigt werden. Der LfD wird die weitere Umsetzung verfolgen.

21.2.3 Auswertungs- und Analysedatei der Polizei „Analyst Notebook"

Die Polizei Rheinland-Pfalz setzt in einzelnen Bereichen für Strukturermittlungen probeweise eine Programmlösung für die zusammenhängende Aufbereitung und Darstellung polizeilicher Ermittlungsergebnisse ein. Das Verfahren basiert auf der Software „Analyst Notebook", einem Analyse- und Auswertungsprogramm für unterschiedliche Einsatzbereiche, und gliedert sich in Module

für den Import von Daten (I-Connect), für die Datenhaltung (I-Base) sowie die eigentliche Analyse und Auswertung (Kernsoftware „Analyst Notebook"). Letztere ermöglicht die grafische Darstellung von Beziehungen zwischen Objekten (Personen, Ereignisse, Tatorte usw.) und von Ereignissen in zeitlicher Abfolge. Objekte sind grundsätzlich frei definierbar, ihnen können zusätzliche Daten in jeglicher Form (Grafik-, Text-, Bild-, Video- und Audiodaten) zugeordnet werden.

Die Feststellungen des LfD haben ergeben, dass die gegenwärtig eingesetzte Version nicht über ausreichende Mechanismen der Benutzerverwaltung und Zugriffskontrolle verfügt. Der Zugriffsschutz ist damit allein auf die Rechtevergabe im Betriebssystem beschränkt, d. h. die pauschale Freischaltung oder Sperrung der Anwendung bzw. des Datenbestandes. Innerhalb der Anwendung ist keine Differenzierung von Zugriffsrechten möglich. Ähnliches gilt für die Nachvollziehbarkeit der Nutzung. Mangels Protokollfunktionen sind Eingaben, Änderungen, Löschungen, Auswertungen, Abfragen und Übermittlungen nicht nachvollziehbar. Den in § 9 LDSG genannten Punkten kann damit gegenwärtig nur teilweise Rechnung getragen werden. Soweit künftig ein weiter gehender Einsatz von „Analyst Notebook" vorgesehen ist, sind aus datenschutzrechtlicher Sicht entsprechende Funktionen innerhalb der Anwendung unverzichtbar.

Die Entwicklung der Software liegt nicht in Händen der Polizei Rheinland-Pfalz; diesbezügliche Anpassungen können nur vom Hersteller vorgenommen werden. Der LfD hat empfohlen, diesen dahin gehend anzusprechen. Das Ministerium des Innern und für Sport hat sich der festgestellten Defizite in Teilbereichen bereits angenommen. Weiterhin wurde Kontakt mit dem Hersteller der Software aufgenommen.

21.2.4 Internet-Anbindung von Verwaltungen über das Landesdaten- und Kommunikationsnetz

In seinem 17. Tb. (Tz. 21.3.5) hat der LfD darauf hingewiesen, dass ein Anschluss öffentlicher Stellen an das Internet nur vertretbar ist, wenn zuvor eine Analyse und Bewertung der damit verbundenen Risiken erfolgt und den Gefahren durch technische und organisatorische Sicherheitsmaßnahmen hinreichend begegnet wird. Angesichts der technischen Gegebenheiten im Internet erfordert dies Vorkehrungen auf unterschiedlichen Ebenen. Der Betrieb einer geeigneten, d. h. an sich ändernde Risiken regelmäßig angepassten Firewall ist dabei von zentraler Bedeutung.

Das DIZ betreibt zur Absicherung des Internet-Übergangs des rlp-Netzes eine mehrstufige Firewall-Struktur. Diese gewährleistet u. a., dass nur zugelassene Dienste genutzt werden können, ein Verbindungsaufbau nur aus dem Landesnetz zum Internet hin erfolgen kann und die lokalen Netze angeschlossener Verwaltungen nicht direkt aus dem Internet heraus adressiert werden können. Nach den Feststellungen des LfD wird mit den dabei getroffenen Sicherheitsmaßnahmen den gegenwärtig bedeutsamen Risiken bei der Internet-Kommunikation weitgehend Rechnung getragen (siehe Tz. 21.2.2.3).

Soweit Verwaltungen des Landes einen Internet-Zugang über die Firewall des DIZ realisieren, entfällt damit grundsätzlich die Notwendigkeit, eine entsprechende Firewall selbst vorzuhalten und zu administrieren.

Nicht allen protokoll- und dienstespezifischen Risiken kann jedoch durch eine zentrale Firewall begegnet werden. Abhängig von der IT-Struktur der jeweiligen Verwaltung können aufgrund der technischen Gegebenheiten im Internet Gefährdungen für die angeschlossenen Endsysteme verbleiben. 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. Dies gilt z. B. im Blick auf in Internet-Angeboten enthaltene aktive Komponenten wie ActiveX-Programme, Java-Scripts oder Visual Basic Scripts. Deren generelle Filterung bzw. Sperrung erfolgt aufgrund der damit u. U. verbundenen Einschränkung der Nutzbarkeit von Internet-Angeboten am zentralen Internet-Übergang des Landesnetzes derzeit nicht. Wie im Rahmen der Internet-Nutzung mit aktiven Komponenten zu verfahren ist, ob diese nicht, nur nach Bestätigung des Anwenders oder nur bei bestimmten Internet-Seiten ausgeführt werden, liegt daher in der Verantwortung der jeweiligen Verwaltung. Dies kann z. B. über die Sicherheitseinstellungen der eingesetzten Browser festgelegt werden (siehe hierzu z. B. www.datenschutz.rlp.de/links.htm).

Die Wirksamkeit eines, wie bei der DIZ-Firewall, auf einen zentralen, abgesicherten Internet-Übergang ausgelegten Sicherheitskonzepts setzt voraus, dass innerhalb der angeschlossenen lokalen Netze keine anderweitigen, ungesicherten Internet-Zugänge bestehen. Dies betrifft die lokalen Netze der jeweiligen Verwaltung und liegt insoweit in deren Verantwortung.

Die Filterung auf schadensrelevante Inhalte wie Computerviren ist an der Firewall des DIZ gegenwärtig auf per elektronische Post übertragene Daten beschränkt und erfasst nur die Kommunikation, die über den zentralen Internet-Zugang bzw. die E-Mail-Server des DIZ abgewickelt wird. Nachrichten, die nicht über die zentralen Mailserver des DIZ weitergeleitet werden, unterliegen dieser Virenprüfung nicht. Gleiches gilt für per FTP/HTTP-Download-empfangene Daten. Hier sind die angeschlossenen Verwaltungen im Rahmen der gegenwärtig bereits bestehenden Anforderungen gehalten, einen ausreichenden Virenschutz in eigener Verantwortung sicherzustellen.

Die für den Internet-Übergang des rlp-Netzes getroffenen strukturellen Sicherheitsmaßnahmen erstrecken sich in der Regel nicht auf die Sicherheit auf Anwendungsebene. Soweit z. B. bei der E-Mail-Kommunikation zur Wahrung ausreichender Vertraulichkeit eine Verschlüsselung erforderlich ist, obliegt dies ebenfalls den Anwendern.

21.2.5 Einsatz von Stimmenzählgeräten bei Wahlen zum Landtag

Mit einer Änderung der Stimmenzählgeräteverordnung ist bei Landtagswahlen auch der Einsatz rechnergesteuerter Stimmenzählgeräte möglich geworden. Bislang durften lediglich mechanische oder elektrisch betriebene Geräte eingesetzt werden.

Der LfD hatte im Vorfeld zum Entwurf der Stimmenzählgeräteverordnung Stellung genommen. Den Anregungen des LfD wurde entsprochen. Die Stimmenzählgeräteverordnung bezieht nunmehr neben den eigentlichen Geräten die für deren Steuerung erforderlichen Programme in das Genehmigungsverfahren ein; die zugelassenen Lösungen sollen ein Prüfkriterium für die Unverfälschtheit des Steuerungsprogramms enthalten.

Für die bei der Landtagswahl verwendeten Geräte wurde eine Lösung gewählt, bei der während des Startvorgangs ein die Programmversion eindeutig kennzeichnendes Merkmal ausgegeben wird. Der Prüfbarkeit der Übereinstimmung des vorliegenden mit dem nach § 3 Abs. 1 Stimmenzählgeräteverordnung genehmigten Programms wird damit entsprochen.

Die Empfehlung, die Integrität der Stimmbezirksergebnisse über eine Prüfsumme abzusichern, wurde nicht aufgegriffen. Angesichts der Speicherung der Wahlergebnisse in besonderen, nur im Wahlgerät und über die Steuerungssoftware nutzbaren Speicherbausteinen, aus welchen die Ergebnisse direkt heraus erstellt und angezeigt werden, war dies für die vorgestellte Lösung von untergeordneter Bedeutung.

Soweit jedoch Ergebnisdateien über die reine Anzeige hinaus weiterverarbeitet bzw. weitergegeben werden, sind diese aus Sicht des LfD vor zufälliger oder unbefugter Veränderung zu schützen. Vergleichbare Verfahren wurden bei den für die zurückliegenden Kommunalwahlen eingesetzten Lösungen berücksichtigt. Aufgrund der zwischenzeitlichen Entwicklung stehen elektronische Signaturlösungen zur Verfügung, die eine Sicherung der Datenintegrität erlauben.

21.2.6 Datenaustausch über ISDN-Verbindungen im Verfahren „Arbeit und Bildung statt Sozialhilfe"

Im Rahmen des Verfahrens „Arbeit und Bildung statt Sozialhilfe" (siehe auch Tz. 11.6.1) erfolgt ein regelmäßiger Datenaustausch zwischen den beteiligten Stellen. Hierzu werden tagesaktuell die Daten über ISDN-Wählverbindungen zum zentralen Server der Kreisverwaltung repliziert und von dort an die jeweiligen Empfänger verteilt.

Hinsichtlich des hierzu erstellten Sicherheitskonzepts wurde der LfD um Stellungnahme gebeten. Danach tragen die getroffenen Sicherheitsmaßnahmen den datenschutzrechtlichen Anforderungen an eine verlässliche Authentifizierung der beteiligten Stellen bzw. Netzkomponenten und der Vertraulichkeit der Kommunikation (vgl. 17. Tb., Tz. 21.3.3) weitgehend Rechnung. In zwei Punkten hat er allerdings gebeten, die Vorschläge zu überprüfen:

Für die Administration der ISDN-Router in der Kreisverwaltung bzw. bei den angeschlossenen Stellen ist ein Fernzugriff per Telnet-Protokoll vorgesehen. Angesichts des überschaubaren und festgelegten Teilnehmerkreises war aus seiner Sicht fraglich, ob Konfigurationsänderungen mit einer Häufigkeit zu erwarten sind, die einen derartigen Fernzugang erfordert, oder ob nicht der lokale Zugang der Systembetreuung der Kreisverwaltung ausreichend ist. Sollte die Notwendigkeit des Fernzugriffs bejaht werden, ist aus Sicht des LfD lediglich eine Realisierung geeignet, bei welcher die für die Anmeldung benötigten Informationen (Benutzername und Passwort) nicht im Klartext übertragen werden und die Anzahl fehlgeschlagener Anmeldeversuche begrenzt werden kann.

Zur Wahrung der Vertraulichkeit bei der täglichen Datenreplikation zum Server der Kreisverwaltung war die Verschlüsselung der Daten während der Übertragung vorgesehen. Der hierbei genutzte einfache DES-Algorithmus mit einer Schlüssellänge von 56 Bit hat sich als angreifbar erwiesen. Auch wenn die flankierenden Sicherheitsmaßnahmen das Risiko eines hierzu erforderlichen unbefugten Zugriffs auf die Replikationsdaten vermindern, ist aus Sicht des LfD angesichts der fortschreitenden technischen Entwicklung, der Sensibilität der im Verfahren übertragenen Sozialdaten sowie des Missbrauchspotentials kompromittierter Anmeldedaten im Rahmen der Transportkontrolle nach § 9 Abs. 2 Nr. 9 LDSG eine höherwertige Verschlüsselung erforderlich (vgl. die Empfehlungen hierzu im 17. Tb. Tz. 21.3.10); zumindest jedoch sollte bei Bedarf ein Wechsel zu geeigneteren Algorithmen möglich sein.

Im Blick auf die nachgewiesene Sicherheitsschwäche und den sinkenden Aufwand für Kompromittierungen kann dies mit dem einfachen DES-Algorithmus (56 Bit) nicht dauerhaft gewährleistet werden. Das Bundesamt für Sicherheit in der Informationstechnik weist darauf hin, dass symmetrische Schlüssel mit einer Länge von weniger als 60 Bit gebrochen werden können und anzunehmen ist, dass diese Grenze in Zukunft auf 80 Bit steigen wird. Insoweit sind vorhandene Erweiterungen auf den Triple DES-Algorithmus (3DES) mit 168 Bit Schlüssellänge zu nutzen. Eine kürzere Schlüssellänge kann datenschutzrechtlichen Anforderungen lediglich dann genügen, wenn in regelmäßigen kurzfristigen Abständen ein automatischer Wechsel des Schlüssels erfolgt oder auf höherer Protokollebene eine angemessene kryptografische Absicherung vorgenommen wird.

Der LfD hat daher vorgeschlagen, die angebotenen Lösungsvorschläge dahin gehend zu überdenken; den Empfehlungen wurde gefolgt.

21.2.7 Telemedizinprojekt im Bereich der Schlaganfallversorgung

Im Rahmen eines telemedizinischen Pilotprojekts wird der elektronische Austausch von Radiologiedaten erprobt. Der LfD wurde in der Planungsphase bei der Erstellung des Pflichtenhefts beteiligt und um Stellungnahme gebeten.

Im Blick auf die Konzeption des Projekts sind unter Datensicherheitsgesichtspunkten aus seiner Sicht vorrangig drei Bereiche von Bedeutung: die IT-Ausstattung der Schlaganfalleinheiten, deren Absicherung gegenüber unbefugten Zugriffen aus dem für die Datenübermittlung genutzten Übertragungsnetz sowie die Sicherung der Vertraulichkeit, Integrität und Authentizität der Radiologiedaten bei der Übermittlung.

Die Schlaganfalleinheiten sind Teil der jeweiligen Krankenhäuser; in datenschutzrechtlicher Hinsicht sind somit die Anforderungen zugrunde zu legen, die für die sonstigen eingesetzten Datenverarbeitungseinrichtungen gelten. Neben einer angemessenen räumlichen Absicherung betrifft dies insbesondere programmseitige Mechanismen für eine ausreichende Zugriffskontrolle wie die Möglichkeit, unterschiedliche Benutzer zu verwalten und differenzierte Zugriffsberechtigungen zu vergeben. Des Weiteren müssen Systemnutzung und Datenübertragungen anhand einer Protokollierung nachvollziehbar sein. Das im Radiologiebereich für den Austausch standardmäßig genutzte DICOM-Protokoll beschränkt sich ausschließlich auf Kommunikationsfunktionen und stellt keine Sicherheitsmechanismen zur Verfügung. Diese müssen damit in den darauf aufsetzenden Anwendungen für die Darstellung, Speicherung, Löschung und den Austausch der Radiologiedaten vorgesehen werden.

Beim Datenaustausch zwischen den Schlaganfalleinheiten bzw. Fachkliniken ist sicherzustellen, dass unbefugte Zugriffe aus dem genutzten Übertragungsnetz ausgeschlossen werden. Bei der Auswahl und Konfiguration der Netzzugangskomponenten sollten daher Funktionen vorgesehen werden, die unberechtigte Zugriffe verhindern (vgl. hierzu 17. Tb., Tz. 21.3.3).

Bei der Übertragung von Gesundheitsdaten auf öffentlichen Übertragungswegen bzw. auf Kommunikationsstrecken, die nicht unter der Kontrolle der beteiligten Stellen stehen, sind aus Sicht des LfD zur Wahrung der Vertraulichkeit und Integrität geeignete kryptografische Maßnahmen vorzusehen (Verschlüsselung bzw. Einsatz elektronischer Signaturlösungen). Die Auswahl geeigneter Algorithmen und Schlüssellängen sollte sich dabei an den Empfehlungen des BSI orientieren. Im Rahmen des Einsatzes asymmetrischer Kryptoverfahren ergibt sich in der Regel die Notwendigkeit, die verwendeten Teilnehmerschlüssel durch eine vertrauenswürdige Stelle zu zertifizieren. Angesichts des derzeit überschaubaren Teilnehmerkreises bestanden keine Bedenken, diese Aufgabe im Rahmen des Pilotprojekts von einem der beteiligten Krankenhäuser wahrnehmen zu lassen und die notwendigen Punkte zwischen den Beteiligten direkt abzustimmen. Bei einer dauerhaften Einrichtung des Verfahrens und der Ausweitung des Teilnehmerkreises sollten allerdings die Trust-Center-Funktionen auf der Grundlage verbindlicher Festlegungen zu Erzeugung, Verwaltung und Einsatz der kryptografischen Schlüssel, zu Gültigkeitszeiträumen und zur Verfahrensweise bei Kompromittierung oder Verlust wahrgenommen werden.

21.2.8 Einsatz von „Pretty Good Privacy“ im Rahmen des automatisierten Mahnverfahrens

Für das beim Amtsgericht Mayen zentralisierte automatisierte Mahnverfahren wurde die Möglichkeit der Beantragung von Mahnbescheiden per E-Mail über das Internet geschaffen. Die dabei vorgesehene Lösung „Pretty Good Privacy“ ist aus datenschutzrechtlicher Sicht grundsätzlich geeignet, eine ausreichende Vertraulichkeit und Zurechenbarkeit der elektronischen Mahnbescheidsanträge sicherzustellen. Das genutzte Programm erlaubt die Erzeugung kryptografischer Schlüssel von angemessener Güte (s. 17. Tb., Tz. 21.3.10). Aufgrund der zusätzlichen Beschränkung auf einen festgelegten Teilnehmerkreis und der in den organisatorischen Richtlinien enthaltenen Vorgaben bestanden aus Sicht des LfD gegen den Einsatz des Programms keine Bedenken.

Angesichts der technischen Entwicklung bedürfen Algorithmen und Schlüssellängen im Blick auf das durch sie verlässlich gewährleistete Sicherheitsniveau einer regelmäßigen Revision. Bei einem längerfristigen Einsatz des Verfahrens ist aus Sicht des LfD daher eine Überprüfung der Schlüsselparameter vorzusehen. Er hat angeregt, die Gültigkeit der vom zentralen Mahngericht in Mayen erstellten Schlüsselzertifikate grundsätzlich zu beschränken und insoweit auf die Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik verwiesen. Die Anregungen des LfD wurden berücksichtigt.

21.2.9 Datenkommunikation des DIZ mit dem Kraftfahrtbundesamt

Mit einer zentralen Kommunikationsverbindung des rlp-Netzes zum Kraftfahrtbundesamt (KBA) über eine Kopfstelle beim DIZ soll Fahrerlaubnis- und Zulassungsbehörden in Rheinland-Pfalz die Möglichkeit eröffnet werden, Datenübermittlungen und Abfragen im zentralen Verkehrsregister online vorzunehmen, ohne dass jeweils ein gesonderter Anschluss zum KBA eingerichtet werden muss.

Die dabei vorgesehene Einrichtung einer verschlüsselten ISDN-Festverbindung zwischen der Kopfstelle beim DIZ und dem KBA trägt den Vertraulichkeitsanforderungen Rechnung. Die Planungen des DIZ sehen künftig die Möglichkeit einer Verschlüsselung der Kommunikation innerhalb des Landesnetzes vor, so dass in Verbindung mit der Struktur des Landesnetzes eine Gleichwertigkeit mit der vom KBA für Einzelzugänge unterstützten Lösung erreicht werden kann. Gegen die Einrichtung eines entsprechenden Sammelzugangs über das rlp-Netz bestanden damit keine datenschutzrechtlichen Bedenken.

21.2.10 Kooperation des DIZ Rheinland-Pfalz mit TÜV-Einrichtungen

Im Rahmen einer geplanten Kooperation des DIZ mit TÜV-Einrichtungen wurde der LfD um Stellungnahme gebeten, inwieweit deren Anschluss an das Kfz-Zulassungsverfahren und eine Einbindung in die Struktur des rlp-Netzes möglich ist.

Soweit TÜV-Stellen hoheitliche Aufgaben wahrnehmen, sind sie öffentliche Stellen i. S. des § 2 Abs. 1 LDSG. Ihre Einbindung in das „VPN Verwaltung" des Landesnetzes ist damit möglich. Dabei ist ein dem Anschluss anderer Verwaltungsstellen entsprechendes Sicherheitsniveau zu gewährleisten, insbesondere ist der Zugriff durch nicht hoheitlich tätige Stellen des TÜV verlässlich auszuschließen. Mit den getroffenen Maßnahmen bei der Übertragung der TÜV-Daten zu einem Kommunikationsserver und der vom DIZ gesteuerten Übernahme in die Fachanwendungen wird dem entsprochen. Gleiches gilt für die Einrichtung von Festverbindungen im Rahmen der Aufgaben nach § 19 StVZO.

Aus datenschutzrechtlicher Sicht bestanden damit keine Bedenken gegen die vorgesehene technische Anbindung der TÜV-Stellen.

21.2.11 Beantragung von Kfz-Wunschkennzeichen über das Internet

Für die Zulassungsstelle einer Stadtverwaltung wurde ein interaktives Verfahren für die Beantragung von Wunschkennzeichen über das Internet entwickelt. Über ein Bildschirmformular sollte dabei vom Antragsteller das gewünschte Kennzeichen eingegeben und die Kommunikation zwischen dem Client-PC des Antragstellers und dem Anwendungsserver über das SSL-Protokoll abgesichert werden. Um Missbräuche zu vermeiden, sollten das Nutzungsinteresse und die Identität des Anfragenden bereits bei der elektronischen Antragstellung hinreichend plausibel dargelegt werden. Hierfür war vorgesehen, als Identifizierungsnachweis die Eingabe der Personalausweisnummer anzufordern und abzugleichen. Im Nachgang zu dem elektronischen Antrag war wie bisher die persönliche Vorsprache des Antragstellers bei der Zulassungsstelle erforderlich. Das die Anwendung entwickelnde Unternehmen bat den LfD im Namen des Auftraggebers um eine datenschutzrechtliche Stellungnahme zum vorgesehenen Konzept.

Bei der Beantragung eines Wunschkennzeichens über das Internet handelt es sich um einen Teledienst nach § 2 Abs. 2 Nr. 1 TDG. Die Verarbeitung personenbezogener Daten unterliegt neben allgemeinen Regelungen dabei den Vorschriften des Teledienstedatenschutzgesetzes (siehe hierzu 17. Tb., Anlage 22). Die nach § 3 Abs. 5 TDDSG vorgesehene Unterrichtung über Art, Umfang, Ort und Zweck der Verarbeitung und der Hinweis auf die Möglichkeit des Widerrufs nach § 3 Abs. 6 TDDSG kann in elektronischer Form, etwa durch das Einblenden eines entsprechenden Browserfensters, erfolgen. Der Inhalt der Unterrichtung und die Funktion zur Ausübung des Widerrufs müssen jederzeit, d. h. auch nachträglich abrufbar sein. Die entsprechenden Verknüpfungen sollten hierzu deutlich erkennbar auf der Eingangsseite der Anwendung platziert werden. Durch eine geeignete Verfahrensgestaltung ist sicherzustellen, dass von einem Widerruf betroffene Daten unverzüglich gelöscht werden.

Bei der Nutzung öffentlicher Übertragungswege bzw. von Kommunikationsstrecken, die nicht unter der Kontrolle der beteiligten öffentlichen Stellen stehen, sind personenbezogene Daten nach den Empfehlungen des LfD zu verschlüsseln. Für die Daten im Rahmen der Beantragung von Wunschkennzeichen ist, nicht zuletzt im Blick auf die Freiwilligkeit der Erhebung und Speicherung, grundsätzlich eine Verschlüsselung ausreichend, die einen Schutz vor zufälliger Kenntnisnahme gewährleistet.

Damit die Personalausweisnummer für die Prüfung der Plausibilität der Reservierung genutzt werden kann, muss ein entsprechender Abgleich erfolgen. Die Zulassungsstellen verfügen unter bestimmten Voraussetzungen zwar über einen Zugang zum Einwohnerinformationssystem, die Personalausweisnummer ist im Datenkatalog des § 3 MG allerdings nicht enthalten. Die Einrichtung eines Online-Zugriffs auf das Personalausweisregister oder eine regelmäßige Übermittlung der Ausweisnummern an die Zulassungsstelle war angesichts der voraussichtlich nur geringen Zahl von Missbrauchsfällen aus Sicht des LfD nicht erforderlich. Ein Rückgriff auf die Angaben, die der Zulassungsstelle bereits zur Verfügung stehen (Name, Anschrift, Geburtsdatum) reicht für einen Nachweis der Identität in der Regel aus. In Betracht käme auch, die Reservierung nur für einen bestimmten Zeitraum vorzuhalten und bei nach dieser Frist ausstehender Inanspruchnahme das betroffene Kennzeichen freizugeben.

21.2.12 Einheitliche Pflege von Steuerungsdaten in statistischen Verbundverfahren (SYST)

Zur einheitlichen Pflege organisatorischer Basisdaten und zur Steuerung von Verbundverfahren haben die statistischen Ämter des Bundes und der Länder das Verfahren SYST entwickelt. Im Rahmen der Federführung des Statistischen Landesamtes Rheinland-Pfalz wurde der LfD während der Entwicklung beteiligt.

In der gegenwärtigen Fassung handelt es sich bei SYST um eine Meta-Anwendung, über welche die Konfiguration vorhandener ADABAS/Natural-Verfahren möglich ist. Unter anderem erlaubt SYST die Umsetzung eines einheitlichen Schutzmodells hinsichtlich der Benutzerverwaltung und Protokollierung bei der Nutzung von Verbundverfahren. Gegen die Einführung bestanden damit aus datenschutzrechtlicher Sicht keine Bedenken. Es ist zu begrüßen, dass damit die Möglichkeit geschaffen wird, für statistische Verbundverfahren ein einheitliches Schutzkonzept abzubilden. Voraussetzung ist hierbei jedoch die ADABAS/Natural-Kompatibiltät mit den SYST-Konventionen. Dies ist gegenwärtig nicht bei allen statistischen Verbundanwendungen der Fall, so dass die Bedeutung von SYST zum Teil erst bei Neuentwicklungen vollständig zum Tragen kommt.

21.2.13 Zugangskontrolle im Bereich einer Anstalt des Landes

Im Rahmen von Umbauarbeiten bei einer Landesanstalt wurde der allgemeine Zugang des Gebäudes verlegt und der ursprüngliche Haupteingang als Baustellenzugang genutzt. Dieser war von der Straße aus unmittelbar zugänglich, die Außentür unverschlossen und eine Aufsicht nicht zugegen. Die im Erdgeschoss gelegenen EDV-Räume konnten ohne Kontrolle betreten werden. Die dort untergebrachten Einrichtungen waren für Manipulationen jedweder Art frei zugänglich; Verteiler- und Rechnerschränke waren unverschlossen. An einer Einheit war ein Hinweis auf den Aufbewahrungsort von Sicherungsdatenträgern angebracht. Über ebenfalls offene Übergänge war der Zutritt zu weiteren Räumlichkeiten möglich. Die Begleitumstände ließen vermuten, dass die Situation über einen längeren Zeitraum bestand und die Umbaumaßnahmen geplant und durchgeführt wurden, ohne dass im Vorfeld die für Sicherheitsfragen zuständigen Stellen der Einrichtung im erforderlichen Umfang einbezogen und Überlegungen zur Absicherung des Rechenzentrums während der Bauphase angestellt wurden.

Der LfD hat die vorgefundene Situation als Verstoß gegen die Regelungen in § 9 Abs. 2 Nr. 1, Nr. 4 und Nr. 10 LDSG bewertet und nach § 25 Abs. 1 Nr. 1 LDSG beanstandet. Mit den auf Veranlassung des LfD noch am gleichen Tag ergriffenen Maßnahmen wurde die Situation kurzfristig entschärft und für die weitere Bauzeit sichergestellt, dass ein unbefugter Zugang zu IT-Einrichtungen oder eine Beeinträchtigung deren Betriebs ausgeschlossen war. Der Vorfall bestätigt erneut, dass Gefährdungen des IT-Einsatzes nicht lediglich begrenzt auf die Risiken in den Blick genommen werden dürfen, die sich aus der Informationstechnik ergeben.

21.2.14 Verfahren MEDIKOS des Medizinischen Dienstes der Krankenversicherung

Der MDK Rheinland-Pfalz besteht aus einer Hauptstelle, sechs Beratungs- und Begutachtungszentren (BBZ) und deren acht Außenstellen. Die IT-Struktur ist weithin dezentral, alle Begutachtungszentren und Außenstellen verfügen über eigene LANs auf der Basis von Windows NT. Diese sind über Standleitungen der Deutschen Telekom AG sternförmig mit dem Netz der Hauptstelle verbunden. Zusammen bilden sie eine NT-Domäne. Deren Administration obliegt der Hauptstelle. Landesweit besteht das Netz aus ca. 20 Servern für diverse Anwendungen und rund 400 Arbeitsplatzrechnern. Hauptsächliche Anwendungen sind Office-Lösungen sowie die Eigenentwicklung MEDIKOS zur Erstellung und Verwaltung medizinischer Gutachten. Pro Jahr werden etwa 50 000 Begutachtungen durch den MDK vorgenommen, in der Hauptsache Pflege- und Arbeitsunfähigkeitsgutachten. Aus Datenschutzsicht ist in diesem Zusammenhang insbesondere die dezentrale Datenhaltung in den einzelnen Niederlassungen des MDK positiv zu bewerten. Gutachtendaten liegen in elektronischer Form sowie in Akten ausschließlich bei den jeweiligen Begutachtungs- und Beratungsstellen vor. Die Zentrale des MDK verfügt lediglich über Informationen, die bei Anfragen eine Klärung der zuständigen Niederlassung ermöglichen.

Im Rahmen örtlicher Feststellungen bei verschiedenen Niederlassungen des MDK wurden die Speicherung, Verarbeitung und Löschung von Patientendaten überprüft. Die in elektronischer Form gespeicherten Gutachtendaten werden danach im Anschluss an den Versand der Unterlagen an die auftraggebende Krankenkasse automatisiert gelöscht. Für Zwecke der Aktenverwaltung werden verschiedene Patientenstammdaten für die Dauer von fünf Jahren elektronisch gespeichert. Die Löschung dieser Daten erfolgt derzeit noch manuell im Rahmen der Aktenaussonderung; mit der vorgesehenen Erweiterung des MEDIKOS-Verfahrens soll dies künftig, ähnlich der Löschung der elektronischen Gutachtendaten, automatisiert erfolgen. Den Regelungen in § 276 Abs. 2 SGB V wird damit verfahrensmäßig entsprochen.

Im Rahmen der Benutzerverwaltung hatten die Feststellungen ergeben, dass für jede Beratungs- und Begutachtungsstelle eine Benutzergruppe eingerichtet war, innerhalb derer keine weitere Differenzierung der Zugriffsrechte vorgenommen wurde. Angesichts der verschiedenen Beschäftigtengruppen – Verwaltungs- und Sekretariatskräfte, Pflegefachkräfte und ärztliches Personal – hat der LfD empfohlen, für die verschiedenen Mitarbeiterbereiche separate Benutzergruppen zu bilden und die Zugriffsrechte entsprechend der Zuständigkeit zu unterscheiden. Dem wurde gefolgt, der MDK hat die entsprechenden Änderungen in der Benutzer- und Zugriffsverwaltung vorgenommen.

Örtliche Feststellungen wurden weiterhin bei einzelnen der vom MDK eingerichteten Heimarbeitsplätze getroffen. Neben einzelnen Empfehlungen hinsichtlich der technischen Ausgestaltung der Arbeitsplätze wurde dabei insbesondere eine pseudonymisierte Verarbeitung der Patientendaten thematisiert (siehe Tz. 17.3).

21.2.15 Sicherung des Beleg- und Datenträgertransports bei einer Kassenärztlichen Vereinigung

Im Blick auf die Erfassung ärztlicher Abrechnungsunterlagen im Wege der Datenverarbeitung im Auftrag wurde der LfD hinsichtlich der technisch-organisatorischen Anforderungen an den Transport von Belegen und Datenträgern um Stellungnahme gebeten. Im konkreten Fall war der Versand der Abrechnungsunterlagen zum Auftragnehmer, die dortige automatisierte Belegerfassung (OCR) und die Rücksendung der Belege sowie der erstellten Datenträger zum Auftraggeber vorgesehen.

Dabei wird der nach Nr. 9 der Anlage zu § 78 a SGB X vorgeschriebenen Transportkontrolle mit Verwendung verschließbarer Behältnisse beim Belegversand sowie der Übernahme und Aushändigung gegen Empfangsbekenntnis ausreichend Rechnung getragen. Grundsätzlich gilt dies auch für die Rücksendung der erfassten Belege in elektronischer Form auf Datenträger, soweit es sich hierbei um die Ursprungsbelege lediglich in Form von Grafikdateien (Images) handelt, und diese, vergleichbar der Mikroverfilmung, nicht nach inhaltlichen Merkmalen automatisiert verarbeitet oder ausgewertet werden können.

Falls neben der elektronischen Abbildung der Belege als Grafik auch die darauf enthaltenen Angaben OCR-erfasst und versichertenbezogene Datensätze auf Datenträger für die weitere automatisierte Verarbeitung zur Verfügung gestellt werden, reicht aus Sicht des LfD die Verwendung verschließbarer Behältnisse allein nicht aus. Angesichts der großen Zahl von Datensätzen in diesem Bereich (ca. 140 000 je Quartalsabrechnung) und der Sensibilität der Angaben sollte, um deren Vertraulichkeit auch im Verlustfall zu gewährleisten, der Datenbestand vor dem Versand verschlüsselt werden. Dies entspricht den Empfehlungen des LfD im 17. Tb., Tz. 21.3.10, wonach der Einsatz kryptografischer Verfahren empfohlen wird, wenn besondere Berufs- und Amtsgeheimnisse, hier das Arztgeheimnis, berührt sind.

Die Kassenärztliche Vereinigung hat die Empfehlungen des LfD aufgegriffen. Die Datenträger mit den OCR-erfassten Abrechnungsbelegen werden im Rahmen der Transportkontrolle künftig verschlüsselt. Die für die Beleglesung eingesetzte Software wurde entsprechend angepasst.

21.3 Allgemeine technisch-organisatorische Aspekte

21.3.1 Wählleitungszugänge zum Landesdaten- und Kommunikationsnetz

Nach der bisherigen Sicherheitspolitik des DIZ basierte die Struktur des LDKN ausschließlich auf fest geschalteten Verbindungen zwischen den einzelnen Netzknoten; Wählzugänge zu Anschlusskomponenten des LDKN waren ausgeschlossen. Aufgrund aktueller Anforderungen sollte die Möglichkeit von Zugängen über Wählverbindungen geschaffen werden.

In seiner Stellungnahme hat der LfD auf die mit der Einrichtung von Wählzugängen verbundenen besonderen Risiken hingewiesen. Im Gegensatz zu Festverbindungen ist bei Wählverbindungen der mögliche Teilnehmerkreis nicht zwingend festgelegt, d. h., jede Stelle, die über entsprechende Anschlusskomponenten verfügt, kann grundsätzlich eine Verbindung zum Einwahlpunkt herstellen. Die Administration der Komponenten durch Dritte birgt dabei Risiken für die Vertraulichkeit und Integrität der übermittelten Daten. 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 Wählverbindungen zum LDKN hat der LfD daher folgende Empfehlungen ausgesprochen:

Die Authentisierung der Teilnehmer muss bereits beim Verbindungsaufbau verlässlich über geeignete Verfahren erfolgen. Angesichts der Nutzung öffentlicher Übertragungswege sind lediglich auf Passworten basierende Mechanismen ohne zusätzliche Absicherung ungeeignet, da die Passworte hierbei in der Regel im Klartext übertragen werden. Der Nachweis der Identität des Teilnehmers sollte über Verfahren erfolgen, die entweder eine Passwortübermittlung in verschlüsselter Form vorsehen oder auf die Übertragung von Passworten gänzlich verzichten. Aus Sicht des LfD bietet insbesondere das standardisierte IPSec-Protokoll mit der Möglichkeit des „Tunnelings“ eine ausreichende Ende-zu-Ende-Sicherheit. Soweit diese gewährleistet ist, kann eine Wählverbindung zum LDKN grundsätzlich über jedes öffentliche Netz betrieben werden.

Inwieweit der für den allgemeinen Wählzugang erforderliche Einwahlknoten vom DIZ betrieben oder von einem Provider angemietet werden soll, ist aufgrund offener Technik- und Kostenfragen bislang noch nicht festgelegt. Soweit mit den genannten Mechanismen durchgängig eine verlässliche Authentisierung sowie eine ausreichende Vertraulichkeit und Integrität gewährleistet werden kann, kommen aus Datenschutzsicht beide Möglichkeiten in Betracht. In beiden Fällen müssen, da öffentliche Übertragungswege genutzt werden, verwaltungsseitig die für eine Ende-zu-Ende-Sicherheit erforderlichen Voraussetzungen geschaffen werden. Ein Unterschied ergibt sich u. U. lediglich in der Reichweite des durch ein „Tunneling“ aufgebauten sicheren Kanals. Bei der Einwahl über einen Provider muss sich der Tunnel vom Endgerät bzw. dem Router der Verwaltung über den Einwahlknoten des Providers hinweg bis zum Authentisierungsserver des DIZ erstrecken. Falls der Einwahlknoten im Bereich des DIZ betrieben und administriert wird, könnte der Tunnel bereits dort enden.

Das DIZ bietet zwischenzeitlich Zugänge zum LDKN über Wählverbindungen an, die den Empfehlungen des LfD entsprechen.

21.3.2 Anforderungen an den Einsatz elektronischer Signaturlösungen in der Verwaltung

Neben der Vertraulichkeit der Kommunikation sind unter Datenschutzaspekten die Vollständigkeit und Korrektheit der Daten (Integrität) und ihre verlässliche Zurechenbarkeit zu einer bestimmten Person oder Stelle (Authentizität) von Bedeutung. Dies ist insbesondere dort der Fall, wo Übertragungswege und ihre Eigenschaften den an der Kommunikation Beteiligten nicht bekannt oder durch sie beeinflussbar sind, die Vertrauenswürdigkeit des Transportwegs mithin nicht oder nur eingeschränkt gegeben ist.

Datenschutzrechtliche Grundlage hierfür sind die Anforderungen in § 9 Abs. 2 LDSG, wonach die unbefugte Veränderung bei der Speicherung (§ 9 Abs. 2 Nr. 3 LDSG) und Übertragung (§ 9 Abs. 2 Nr. 9 LDSG) verhindert werden muss. Soweit eine verlässliche Zurechenbarkeit elektronischer Nachrichten und deren Schutz vor unbefugten Veränderungen gewährleistet sein muss, sollte auf elektronische Signaturverfahren zurückgegriffen werden.

Soweit nicht bestimmte elektronische Signaturen durch Rechtsvorschrift vorgeschrieben sind, ist die Art der jeweiligen Lösung freigestellt (vgl. § 1 Abs. 3 SigG). Das mit einer qualifizierten elektronischen Signatur nach § 2 Nr. 3 SigG verbundene Schutzniveau ist vor allem dort von Bedeutung, wo besondere Anforderungen an die Authentizität und Integrität elektronischer Daten bestehen

und ein grundsätzlich offener Teilnehmerkreis vorliegt. Wenn ausschließlich festgelegte Stellen miteinander kommunizieren, z. B. im Rahmen einer geschlossenen Benutzergruppe von Verwaltungsstellen oder geringere Anforderungen an die Zurechenbarkeit und Unversehrtheit der Daten zu stellen sind, kann aus Sicht des LfD auch eine fortgeschrittene elektronische Signatur nach § 2 Nr. 2 SigG ausreichend sein.

Dabei ist es allerdings ebenfalls erforderlich, zwischen den Teilnehmern verbindliche Festlegungen über die Erzeugung, Vergabe, Gültigkeitsdauer und gegebenenfalls den Widerruf der eingesetzten kryptografischen Schlüssel zu treffen. Insbesondere muss die Schlüsselerzeugung durch eine vertrauenswürdige Stelle erfolgen. Im Blick auf eine einheitliche Handhabung und ein einheitliches Sicherheitsniveau der IT-Umgebung ist dabei eine zentrale Schlüsselgenerierung zu bevorzugen. Vorzugsweise sollten Chipkarten als Schlüsseldatenträger eingesetzt werden. Andere Lösungen sind je nach Einsatzumfeld möglich, soweit eine ausreichende Sicherheit gewährleistet wird.

Die Sicherheit elektronischer Signaturen hängt wesentlich von den zugrunde liegenden kryptografischen Verfahren ab. Deren Güte bemisst sich nach der Wahrscheinlichkeit, mit der sie aufgrund technischer Entwicklungen oder wissenschaftlicher Fortschritte kompromittiert werden können. Algorithmen und Schlüssellängen bedürfen daher einer regelmäßigen Überprüfung. Aus Sicht des Datenschutzes sind solche Algorithmen und Schlüssellängen zu verwenden, die nach den Anforderungen des BSI als geeignet anzusehen sind.

Die im Rahmen des Betriebs von Public Key-Infrastrukturen erforderlichen Dienste können unter den allgemeinen Voraussetzungen des § 4 LDSG grundsätzlich auch im Wege der Auftragsdatenverarbeitung erbracht werden. Bedeutsam sind in diesem Zusammenhang insbesondere die Bereiche Schlüsselerzeugung, Personalisierung, Zertifizierung und Verzeichnisdienst. Inwieweit diese für eine Auslagerung in Betracht kommen, ist u. a. nach den konkreten Sicherheitsanforderungen des jeweiligen Verfahrens und der beim vorgesehenen Auftragnehmer getroffenen Sicherungsmaßnahmen zu beurteilen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in ihrer Entschließung vom 24. Oktober 1997 (17. Tb., Anlage 3) gefordert, sich bei der Auswahl und Gestaltung von Verfahren datenschutzfreundlicher Technologien zu bedienen. Im Zusammenhang mit dem Einsatz elektronischer Signaturverfahren betrifft dies insbesondere die Möglichkeit, in geeigneten Fällen neben namentlich zugeordneten Zertifikaten auch Pseudonyme verwenden zu können.

21.3.3 Verschlüsselung und elektronische Signatur bei der Übertragung von Personaldaten

Als Kalkulationsgrundlage für die selbst gesteuerte Personalkostenbudgetierung werden den Ressorts durch das Ministerium der Finanzen Einzeldatensätze mit besoldungs-, vergütungs- und lohnbezogenen Daten zur Verfügung gestellt (Budgetierungsdatensätze). Die weitere Verteilung der Personaldatensätze an die bewirtschaftenden Dienststellen im nachgeordneten Bereich erfolgt u. a. per E-Mail über das LDKN.

Der LfD hat in diesem Zusammenhang den Einsatz von Verschlüsselungsverfahren empfohlen (siehe 17. Tb., Tz. 21.2.15). Für den Bereich des Ministeriums für Umwelt und Forsten wurde zwischenzeitlich eine chipkartenbasierte Lösung eingeführt, mit der die Budgetierungsdaten verschlüsselt und elektronisch signiert übertragen werden. Die verwendeten Algorithmen und Schlüssellängen (u. a. RSA 1024 Bit) entsprechen den datenschutzrechtlichen Anforderungen.

Ähnliches gilt für die Personalverwaltung im Bereich der Polizei. Auf der Grundlage der Empfehlungen des LfD wird für die vertrauliche Übermittlung von Personaldaten per E-Mail das vom Bundesamt für Sicherheit in der Informationstechnik für den Behördenbereich kostenfrei zur Verfügung gestellte Verschlüsselungsprogramm CHIASMUS eingesetzt.

21.3.4 Verschlüsselung und Elektronische Signatur bei der Befundübertragung per E-Mail

Im Bereich eines städtischen Krankenhauses war vorgesehen, im Rahmen der Einbindung in ein regionales Praxisnetz den Postversand von Kurzbefunden an den weiter behandelnden Arzt durch die elektronische Übermittlung per E-Mail über das Internet zu ersetzen bzw. zu ergänzen.

In seiner Stellungnahme hat der LfD darauf hingewiesen, dass die Übermittlung von Befunddaten an Dritte einer Rechtsgrundlage (z. B. § 36 Abs. 3 Nr. 2 LKG) oder der Einwilligung des Betroffenen bedarf. Soweit das vorgesehene Verfahren den bisherigen Postversand von Arztbriefen ersetzt, gelten die gleichen Anforderungen. Eine besondere Situation ergibt sich in den Fällen, in denen Befunde den Patienten ausgehändigt werden, und es damit – außerhalb des Entlassungsgesprächs – deren Entscheidung obliegt, inwieweit diese an einen nachbehandelnden Arzt weitergegeben werden. Soweit nicht seitens des Patienten etwas anderes bestimmt wird, sind derartige Fälle aus Sicht des LfD von der elektronischen Übermittlung auszunehmen.

Hinsichtlich der Datensicherungsmaßnahmen sind nach § 36 Abs. 1 und 8 LKG die Regelungen zum technisch-organisatorischen Datenschutz in § 9 Abs. 2 LDSG zugrunde zu legen. Danach ist u. a. sicherzustellen, dass Befunde bei der elektronischen Übertragung nicht unbefugt gelesen oder verändert werden können. Für die verlässliche Zurechenbarkeit von Nachrichten, deren Schutz vor unbefugten Veränderungen und unbefugter Kenntnisnahme hat der LfD empfohlen, auf elektronische Signaturverfahren zurückzugreifen. Den Empfehlungen wurde durch den Einsatz des Programms „Pretty Good Privacy“ Rechnung getragen. Die dabei ein-

gesetzten Algorithmen und Schlüssellängen entsprachen den Empfehlungen des BSI, damit bestanden aus datenschutzrechtlicher Sicht keine Bedenken gegen die Erprobung der elektronischen Befundübertragung zwischen den im Praxisnetz zusammengeschlossenen Stellen.

Ausdrücklich hat der LfD darauf hingewiesen, dass die genannten kryptografischen Maßnahmen keinen Schutz der angeschlossenen IT-Systeme gegenüber den sonstigen im Internet bestehenden Risiken bieten. Soweit diesen nicht durch den Einsatz von Firewall-Lösungen Rechnung getragen wird, darf die Befundkommunikation nur über Systeme erfolgen, die vom jeweiligen Praxis- bzw. Krankenhausnetz physikalisch getrennt sind.

21.3.5 Datenschutzrechtliche Probleme im Zusammenhang mit dem Einsatz des Betriebssystems Windows

In mehreren Bereichen der Landesverwaltung steht gegenwärtig die Ablösung bisheriger IT-Strukturen an. In weitaus größerem Umfang als bisher werden in den Verwaltungen lokale Netze in Verbindung mit Bürokommunikationslösungen und Standardsoftware eingesetzt. In den meisten Fällen handelt es sich, server- und netzwerkseitig sowie an den Arbeitsplätzen, um Produkte der Firma Microsoft, die auf den verschiedenen Varianten des Betriebssystems Windows basieren. Allein im Bereich der Polizei ist im Rahmen der Einführung von POLADIS-neu mittelfristig die Ausstattung mehrerer tausend Arbeitsplätze mit Personalcomputern vorgesehen. Ähnliches gilt für den Bereich der Meldeämter hinsichtlich des in der Entwicklung befindlichen Einwohnerinformationsystems EWOIS-neu sowie die Neuorganisation der Mittelinstanz und IT-Unterstützung der Verwaltungsabläufe. Windows-Betriebssysteme und windowsbasierte Anwendungen stellen in vielen Fällen die zentralen Plattformen des IT-Einsatzes in der Landesverwaltung dar. In den jeweiligen Fachanwendungen sind in der Regel Mechanismen enthalten, die innerhalb der Verfahren sicherstellen, dass Datenzugriffe nur von befugten Personen und im jeweils zulässigen Umfang erfolgen können, die Nutzung anhand einer Protokollierung angemessen nachvollzogen werden kann und nicht mehr erforderliche Daten gelöscht werden.

Datenschutzrechtliche Probleme ergeben sich dann, wenn mit Standardfunktionen des zugrunde liegenden Betriebssystems diese Schutzmechanismen unterlaufen werden können. Konkret betrifft dies z. B. die Möglichkeit, über die Windows-Zwischenablage Daten zwischen verschiedenen Anwendungen auszutauschen und gegebenenfalls außerhalb der Verfahren weiter zu verarbeiten. Diese in vielen Fällen sinnvolle Funktion birgt dabei die Gefahr, dass auf diesem Weg – auch abseits von Missbrauchsszenarien – vertrauliche Daten außerhalb der eigentlichen Verfahren in ungenügend gesicherten Umgebungen gespeichert werden. Weiterhin können Protokollierungs- und im Rahmen der Fachaufsicht vorgesehene Funktionen ins Leere laufen oder notwendige Löschungen unterbleiben. Die Problematik ist nicht grundsätzlich neu. Eine besondere Bedeutung ergibt sich jedoch aktuell dadurch, dass in größerem Maßstab entsprechende Umstrukturierungen der eingesetzten Informationstechnik anstehen.

Da letztlich Grundfunktionen der Betriebssysteme betroffen sind und diese sich in der Regel der Einflussmöglichkeit der einzelnen Anwender entziehen, ist gegenwärtig noch kein befriedigender und in der Praxis handhabbarer Ansatz gefunden. Damit sind zumeist nur Teillösungen, vielfach beschränkt auf organisatorische Maßnahmen und im Wege der Sensibilisierung der Anwender, möglich.

21.3.6 Einsatz des Betriebssystems Windows 2000 in der Landesverwaltung

Das Betriebssystem Windows 2000 der Firma Microsoft enthält eine Softwarekomponente namens Diskeeper zur Optimierung der Datenspeicherung. Es handelt sich hierbei um ein in das Betriebssystem integriertes Programm eines Dritthersteller. Aufgrund von dessen Verbindungen zur Scientology-Vereinigung sind Befürchtungen laut geworden, das Programm könnte genutzt werden, um unbemerkt Anwenderdaten auszuspähen.

In diesem Zusammenhang sind Prüfungen der Software durch das BSI erfolgt. Wegen der nach Verhandlungen mit Microsoft zur Verfügung gestellten Möglichkeit, die Komponente zu deaktivieren, wurde von der vom BSI ursprünglich beabsichtigten Quellcode-Prüfung abgesehen. Eine auf der Analyse des Programmcodes basierende, endgültige Bewertung der Vertrauenswürdigkeit der Software liegt damit nicht vor. Weiterhin sind Programme zum vollständigen Entfernen der Komponente verfügbar. Offen ist gegenwärtig noch, inwieweit bei Aktualisierungen des Betriebssystems durch Service Packs o. Ä. die durchgeführten Änderungen erhalten bleiben. Gegebenenfalls sollte daher eine Kontrolle der Einstellungen erfolgen.

Bislang haben sich keine Hinweise darauf ergeben, dass das Programm verborgene Funktionalitäten enthält oder für die unbemerkte Übermittlung von Daten missbraucht werden kann. Vor diesem Hintergrund hat der IT-Ausschuss der Landesregierung einen mit dem LfD abgestimmten Beschluss zum Einsatz von Windows 2000 in der Landesverwaltung gefasst. Danach bestehen gegen dessen Einsatz auch in sicherheitsrelevanten Bereichen keine Bedenken, wenn das Defragmentierungstool Diskeeper deinstalliert wird oder sicherheitsrelevante Daten verschlüsselt werden.

Der LfD hat dies zum Anlass genommen, darauf hinzuweisen, dass die Vertrauenswürdigkeit von Software allgemein durch die Anwender nur ausnahmsweise und sehr bedingt verlässlich eingeschätzt wird; eine Prüfung stößt zudem an praktische Grenzen. Dies betrifft, unabhängig vom vorliegenden Fall, grundsätzlich jede (systemnahe) Softwarekomponente. Bei der Verarbeitung sensibler Informationen muss dies bedacht werden. Soweit nicht durch den Einsatz zertifizierter Lösungen oder – notwendigerweise ebenfalls vertrauenswürdiger – kryptografischer Verfahren ein ausreichender Schutz erreicht werden kann, sollte gegebenenfalls auf den Einsatz einzelner Produkte oder die Nutzung bestimmter Funktionen verzichtet werden.

21.3.7 Einsatz von Laptops im Rahmen mobiler Bürger-Service-Büros

Im Aufgabenbereich des Landesamtes für Soziales, Jugend und Versorgung und der Ämter für soziale Angelegenheiten war die Einrichtung mobiler Service-Büros vorgesehen. Zu der Ausstattung der Service-Büro-Mitarbeiter mit tragbaren Rechnern hat der LfD die nachfolgenden Empfehlungen ausgesprochen (vgl. 13. Tb., Tz. 20.2 und 14. Tb. Tz. 21.6).

Der mobile Einsatz von Laptops unterliegt im Vergleich zum stationären Einsatz einem erhöhten Risiko der missbräuchlichen Nutzung, der unbefugten Kenntnisnahme gespeicherter Daten oder des Verlustes. Da auf die räumliche Absicherung ausgerichtete Vorkehrungen meist entfallen, sind systemseitige Hard- oder Softwarelösungen einzusetzen. Soweit personenbezogene Daten verarbeitet werden, sind insbesondere folgende Maßnahmen von zentraler Bedeutung:

Die Nutzung darf erst nach erfolgreicher Authentisierung der Benutzer möglich sein, z. B. durch entsprechende Software- (Sicherheitsoberfläche mit Passwortabfrage) oder Hardwarelösungen (Chipkarte, Token, o. Ä.). Wird das Gerät von mehreren Personen genutzt, ist für jeden Benutzer eine separate Zugriffsberechtigung einzurichten. Es muss sichergestellt sein, dass eine Authentisierung auch vor der erneuten Inbetriebnahme aus dem Stand-by-Betrieb erfolgt. Ein Systemstart von Diskette ist technisch zu unterbinden; falls dies nicht möglich ist, muss ein unbefugter Festplattenzugriff ausgeschlossen werden.

Die Benutzung des Geräts, insbesondere sicherheitsrelevante Ereignisse wie erfolglose Anmeldeversuche oder Verstöße gegen Zugriffsberechtigungen, sollte anhand einer Protokollierung nachvollzogen werden können.

Zum ausreichenden Schutz gegenüber Manipulationen und unbefugter Kenntnisnahme bei Diebstahl oder Verlust eines Gerätes sind personenbezogene Daten zu verschlüsseln. Nach Möglichkeit ist eine Online-Verschlüsselung vorzusehen, so dass auch bei einem unvorhergesehenen Arbeitsabbruch die Vertraulichkeit der Daten auf der Festplatte gewährleistet ist. Grundsätzlich empfiehlt sich die Verschlüsselung der kompletten Festplatte. Sollte dies aus darzulegenden Gründen nicht möglich sein, kommt eine Datei- oder Verzeichnisverschlüsselung in Betracht.

Die technischen Maßnahmen sind durch organisatorische Regelungen über Art und Umfang des Laptop-Einsatzes, Verantwortlichkeiten und die Aufbewahrung der Geräte zu ergänzen (Dienstanweisung).

Im Rahmen einer E-Mail-Kommunikation der Service-Mitarbeiter ergeben sich beim Versand anonymisierter Daten keine besonderen Anforderungen an die Vertraulichkeit der Nachrichten. Nach der Alltagserfahrung tauchen bei der Beratungsarbeit jedoch häufig Fragen auf, deren Klärung nur unter Verwendung personenbezogener Angaben möglich ist. Als Vorsorge für derartige Fälle hat der LfD daher empfohlen, auf den Systemen eine geeignete Möglichkeit zur Verschlüsselung von E-Mails vorzuhalten. Unverzichtbar ist dies spätestens dann, wenn Daten, die besonderen Berufs- und Amtsgeheimnissen nach § 203 StGB unterliegen, vorrangig Gesundheits- und Sozialdaten, in öffentlichen Netzen übertragen werden. Im Übrigen sind die gängigen Vorkehrungen gegenüber den mit der E-Mail-Kommunikation verbundenen Risiken zu treffen (insbesondere Schutz vor Viren und sonstigen Programmen mit Schadensfunktionen).

Bei Berücksichtigung der genannten Punkte bestanden gegen den Einsatz von Laptops im Rahmen der Beratungsarbeit des Landesamtes keine Bedenken.

21.3.8 Datenschutz am Informationsschalter eines Finanzamts

Durch eine Eingabe wurde der LfD darauf hingewiesen, dass am Informationsschalter eines Finanzamts die erforderliche Diskretion nicht gewährleistet sei.

Der Petent stellte dar, dass er in einer Steuerangelegenheit das Finanzamt und dort wegen der zuständigen Stelle zunächst den Informationsschalter aufgesucht habe, wobei sein Anliegen sowie sein Name nebst Steuernummer und Anschrift – trotz entsprechender Hinweise – vom Schalterbediensteten in einer Lautstärke verhandelt worden seien, dass seine Angaben auch von den übrigen in der Eingangshalle anwesenden Personen zur Kenntnis genommen werden konnten. Die Gestaltung des Informationsschalters erschwere ohnedies die Wahrung der Vertraulichkeit.

Aus datenschutzrechtlicher Sicht bestehen gegen die Einrichtung von Auskunftsschaltern im Blick auf die bürgerfreundliche und zügige Erbringung von Verwaltungsleistungen grundsätzlich keine Bedenken. Wenn erforderlich oder gewünscht, muss jedoch, ähnlich wie bei Bürgerbüros, eine angemessene Vertraulichkeit gewährleistet sein. Aufgrund eines entsprechenden Hinweises des LfD hat das Finanzamt raumgestaltende Maßnahmen getroffen und die Mitarbeiter nochmals auf die notwendige Diskretion bei Auskunftserteilung oder Nachfragen aufmerksam gemacht.

21.3.9 Struktur und Betreuung der Informationstechnik unter datenschutzrechtlichen Aspekten

Im Blick auf die jeweilige Neustrukturierung des IT-Einsatzes wurde der LfD mehrfach um Stellungnahme gebeten, inwieweit datenschutzrechtliche Gesichtspunkte eine zentrale bzw. dezentrale IT-Struktur erforderten.

Das Landesdatenschutzgesetz, hier vor allem § 9 LDSG als generelle gesetzliche Regelung der technisch-organisatorischen Maßnahmen, lässt die Struktur der eingesetzten Informationstechnik und die Art und Weise ihrer Betreuung grundsätzlich offen. Deren Bedeutung im Rahmen einer datenschutzrechtlichen Betrachtung ergibt sich letztlich im Zusammenhang mit der Sensibilität der Daten und den nach § 9 Abs. 2 LDSG getroffenen Maßnahmen. Daneben sind räumliche Gegebenheiten, organisatorische Strukturen oder personelle Kapazitäten für die Beurteilung von Belang. Den Vorteilen einer zentralen Administration ist gegenüberzustellen, dass diese häufig mit weit reichenden Zugriffsmöglichkeiten auf personenbezogene Daten verbunden ist; eine auf dezentralisierten Verantwortlichkeiten gründende Beschränkung administrativer Rechte kann datenschutzrechtlich daher von Vorteil sein.

In Einzelfällen kann sich zudem aus datenschutzrechtlicher Sicht die Notwendigkeit einer separaten bzw. separat betreuten IT-Struktur ergeben. So hat der LfD in Fällen, in welchen aufgrund der Sensibilität der Daten eine unbefugte Kenntnisnahme durch die zentrale IT-Betreuung ausgeschlossen werden muss und keine geeigneten Sicherungsmöglichkeiten, wie die Verschlüsselung der Daten bestehen, den Einsatz getrennter Systeme (z. B. bei dem Arztgeheimnis unterliegenden Daten des Gesundheitsamtes innerhalb einer Kreisverwaltung) empfohlen (vgl. 17. Tb. Tz. 2.12.12).

Dezentrale IT-Lösungen sind mithin nicht grundsätzlich auszuschließen. Bedenken bestehen dann, wenn sich daraus ein niedrigeres und unangemessenes Sicherheitsniveau ergäbe, als es – verglichen mit einer zentralen IT-Struktur – möglich wäre. Im Blick auf die Zugangskontrolle nach § 9 Abs. 2 Nr. 1 LDSG gilt dies z. B. für die Absicherung von Räumlichkeiten mit besonderer Bedeutung für den Einsatz der Informationstechnik. Hierunter fallen insbesondere Räume mit zentralen IT-Komponenten, Datenträgerarchive sowie die Arbeitsräume der Mitarbeiter der Systemverwaltung (vgl. hierzu 17. Tb., Tz. 21.3.9).

Soweit aus technischen, wirtschaftlichen oder organisatorischen Überlegungen heraus eine dezentrale IT-Struktur gewählt wird, ist sicherzustellen, dass datenschutzrelevante Aufgaben der Systemadministration in zentraler Verantwortung verbleiben bzw. nach einheitlichen Vorgaben wahrgenommen werden. Vorrangig betrifft dies die Benutzerverwaltung, die Festlegung von Zugriffsrechten und – in vernetzten Umgebungen – von Vertrauensbeziehungen, die grundsätzliche Datei- und Verzeichnisorganisation sowie die Vorgaben zur Protokollierung der Systemnutzung. Im Blick auf die Organisationskontrolle nach § 9 Abs. 2 Nr. 10 LDSG hat sich folgende Aufteilung administrativer Funktionen als geeignet erwiesen:

Die Einrichtung und Pflege von Benutzergruppen einschließlich der ihnen zugeordneten Zugriffsprofile für Anwendungen, Daten und Netzwerkressourcen erfolgt zentral. Gleiches gilt für die Festlegung wesentlicher Systemeinstellungen wie die Konfiguration der Passwortparameter oder die Einrichtung von Systemrichtlinien. Darauf aufbauend wird in dezentraler Verantwortung die konkrete Zuweisung von Benutzern zu Gruppen, die Ressourcenverwaltung innerhalb der vorgegebenen Datei- und Verzeichnisstruktur sowie die technische Betreuung und Systempflege wahrgenommen. Die verschiedenen administrativen Verantwortlichkeiten sind dabei in entsprechenden Benutzerprofilen abzubilden.

Neben der Verantwortung für die Administration und technische Betreuung der eingesetzten Systeme ist die übergreifende IT-Planung, -Steuerung und -Koordinierung von Bedeutung. Nach den Erfahrungen des LfD unterstützt hierbei die Festlegung zentraler Zuständigkeiten eine datenschutzrechtlichen Anforderungen entsprechende Organisation.

21.3.10 Zugriffsmöglichkeiten für Gemeinderatsmitglieder auf IT-Systeme der Gemeindeverwaltung

Eine Kommune bat den LfD im Blick auf die beabsichtigte Einrichtung von Zugriffsmöglichkeiten für Mitglieder des Gemeinderates auf IT-Verfahren der Gemeindeverwaltung um Stellungnahme. Betroffen waren Verfahren im Bereich Sitzungsdienst, E-Mail und Kalenderfunktionen sowie Finanzen/Haushaltswesen.

Unter der Voraussetzung, dass über das Sitzungsdienstverfahren nur Unterlagen zugänglich sind, die bisher in schriftlicher Form zur Verfügung gestellt wurden, bestanden keine datenschutzrechtlichen Bedenken. In jedem Fall muss sichergestellt werden, dass keine Zugriffe auf andere Verfahren innerhalb des Netzwerks der Gemeindeverwaltung möglich sind. Gleiches gilt für die Zugriffsmöglichkeiten auf E-Mail-Postfächer und Kalender.

Für das Haushaltsverfahren war fraglich, inwieweit Zugriffsrechte in gleicher Weise beschränkt werden können. Um zu vermeiden, dass unbefugte Zugriffe, z. B. auf Personenkonten, möglich werden, hat der LfD folgende Verfahrensweise vorgeschlagen: Die in Betracht kommenden Daten (Haushaltsübersichten) werden aus dem Verfahren extrahiert und in einem den Gemeinderatsmitgliedern zugänglichen Verzeichnis auf dem Server der Gemeindeverwaltung zur Verfügung gestellt. Auf diese Weise wird gewährleistet, dass nur die benötigten Informationen zur Verfügung gestellt werden.

Für die technische Umsetzung der Zugriffsmöglichkeiten wurden seitens der Gemeindeverwaltung drei Alternativen ins Auge gefasst:

- Aufstellung eines PC in den jeweiligen Fraktionsräumen innerhalb der Verwaltung

  Soweit durch geeignete Maßnahmen die Nutzung der Geräte durch Unbefugte ausgeschlossen wird, bestanden gegen diese Lösung keine Bedenken.

- Zugang zum IT-Netz der Gemeindeverwaltung über Wählleitungsverbindungen

  Für einen Teil der Gemeinderatsmitglieder sollte die Möglichkeit geschaffen werden, sich über das Telefonnetz der Deutschen Telekom in den Server der Gemeindeverwaltung einzuwählen. Die Einrichtung von Wählleitungsverbindungen und die Nutzung öffentlicher Übertragungswege sind aus datenschutzrechtlicher Sicht mit Risiken verbunden. Sie sollte daher nur bei Berücksichtigung der vom LfD ausgesprochenen Empfehlungen für die Einrichtung von Wählleitungsanschlüssen (17. Tb., Tz. 21.3.3) realisiert werden.

  Da seitens des Gemeinderats vorrangig die Möglichkeit angestrebt wurde, Sitzungsunterlagen in elektronischer Form zu erhalten, hat der LfD gebeten, vor der Einrichtung von Wählleitungsverbindungen zu prüfen, inwieweit dem Anliegen anstelle eines Direktzugriffs durch den Versand per E-Mail entsprochen werden kann. Die notwendige Absicherung wäre in diesem Fall mit geringerem technischen und kostenmäßigen Aufwand möglich und die mit der Einrichtung eines Wählanschlusses verbundenen Risiken würden vermieden.

- Zugangsmöglichkeit zum IT-Netz der Gemeindeverwaltung via Internet

  Der Betrieb eines separaten Internet-Servers und einer eigenen Firewall durch die Gemeindeverwaltung war aus Kosten- und Kapazitätsgründen nicht vorgesehen. Vor diesem Hintergrund hat der LfD empfohlen, angesichts der bestehenden Risiken von einer direkten Internet-Anbindung für den Zugriff auf die o. g. Verfahren abzusehen. Keine Bedenken bestanden gegen eine Lösung, bei der ausgewählte Daten auf einem vom DIZ betriebenen Internet-Server vorgehalten werden und der Zugriff an verlässliche Verfahren zur Identifikation und Authentifizierung (z. B. Benutzerkennung/Passwort) gebunden wird.

21.3.11 Preisgabe von Passworten bei Abwesenheit der zuständigen Mitarbeiter

Bei der Verwaltung einer Verbandsgemeinde war der Leiter der Finanzabteilung längerfristig abwesend, seine Vertreterin erkrankt. Während ihrer Erkrankung wurde sie mit dem Hinweis, dass „etwas kontrolliert werden solle", vom Leiter der Zentralabteilung telefonisch angewiesen, ihr Benutzerpasswort für das IT-System der Verbandsgemeinde preiszugeben. Nähere Angaben zur Art der Daten, auf die zugegriffen werden solle, und den Gründen wurden nicht gemacht. Die Bedienstete weigerte sich daraufhin, ihr Passwort zu nennen und hat sich mit der Frage, ob das Ansinnen des Verwaltungsleiters gerechtfertigt sei, an den LfD gewandt.

Der LfD hat darauf hingewiesen, dass ein Zugriff auf benötigte Daten dann zulässig sei, wenn er sachlich erforderlich, d. h. durch dienstliche Belange gerechtfertigt, und zeitlich erforderlich, d. h. dringend ist. Eine solche Notwendigkeit kann sich ergeben, wenn der Zugang aus dienstlichen Gründen benötigt wird, aber z. B. auch, wenn Anhaltspunkte für eine missbräuchliche Nutzung vorliegen und dem nachgegangen werden soll.

Die Preisgabe des Passwortes durch die Bediensteten kann in diesen Fällen nicht verweigert werden. Zumeist ist sie jedoch nicht erforderlich, da die benötigten Daten häufig unter Mithilfe der Systemverwaltung bereitgestellt werden können. Einer entsprechenden Anweisung muss die Systembetreuung, ggf. unter Prüfung der Remonstration nach § 66 LBG, Folge leisten. Der Zugriff ist mit Zeitpunkt, Art und Inhalt nachvollziehbar zu dokumentieren.

Häufig besteht die Möglichkeit, das Passwort eines Benutzers neu zu vergeben und unter Verwendung des neuen Passworts zuzugreifen. Die Passwortänderung bzw. die Tatsache des Zugriffs während ihrer Abwesenheit ist für die Mitarbeiter somit erkennbar. Dies gilt insbesondere im Hinblick auf für private Zwecke gespeicherte Daten, soweit dies zugelassen ist (vgl. 17. Tb., Tz. 5.10).

21.3.12 Speicherung von Personal- und Gesundheitsdaten auf zentralen Servern

Mehrfach wurde der LfD um Stellungnahme zur Frage der Speicherung von Daten, die einer besonderen Vertraulichkeit unterliegen, auf zentralen Servern im Netzwerk einer Verwaltung gebeten. Zumeist betraf dies Daten der in die Kreisverwaltungen eingegliederten Gesundheitsämter oder Daten aus der Beihilfebearbeitung.

Der im Blick auf § 9 Abs. 2 Nr. 3 LDSG (Speicherkontrolle) notwendigen Abschottung wird bei der Speicherung personenbezogener Daten auf zentralen Servern in der Regel ausreichend Rechnung getragen, wenn sich die Datei- und Verzeichnisstruktur an der Organisation der Dienststelle orientiert und Zugriffsrechte nur entsprechend der dienstlichen Zuständigkeit vergeben werden.

Im Rahmen der Benutzerverwaltung sollten daher abteilungs- bzw. sachgebietsbezogene Benutzergruppen eingerichtet und die Zugriffsbefugnisse an diese gebunden werden. Die konkreten Zugriffsrechte ergeben sich danach aus der Zuordnung der einzelnen Benutzer zur jeweiligen Benutzergruppe. Die gängigen Betriebssysteme stellen hierfür geeignete Funktionen zur Verfügung.

Diese Mechanismen stoßen jedoch an Grenzen, wenn auf der Grundlage erweiterter Berechtigungen Zugriffe außerhalb der eigentlichen Bearbeitung möglich oder erforderlich sind (z. B. System- und Netzwerkadministration, Wartung). In seinem 17. Tb., Tz. 21.2.12, hat der LfD darauf hingewiesen, dass bei der Speicherung von Gesundheitsdaten auf einem zentralen Server durch kryptografische Maßnahmen sichergestellt werden muss, dass auf die Daten im Klartext ausschließlich von den hierzu befugten Beschäftigten des Gesundheitsamtes zugegriffen werden kann. Für dem Arztgeheimnis unterliegende Daten muss eine Kenntnisnahme durch Personen außerhalb des ärztlichen Bereichs wirksam ausgeschlossen werden. Gleiches gilt für Bereiche, in denen vergleichbar sensible Daten im lokalen Netz gespeichert werden, z. B. im Rahmen der Beihilfebearbeitung.

Im Blick auf Vertretungsregelungen und einen ggf. erforderlichen Zugriff durch mehrere Personen bestehen keine Bedenken, dabei einen so genannten Gruppenschlüssel zu verwenden, soweit dessen vertrauliche Behandlung sichergestellt ist.

22. Datenverarbeitung bei Sparkassen

22.1 Änderung der Meldepflicht für öffentlich-rechtliche Kreditinstitute

Mit dem am 23. Mai 2001 in Kraft getretenen Gesetz zur Änderung des BDSG und anderer Gesetze (vgl. hierzu Tz. 2.1) haben sich die Voraussetzungen für die Meldepflichten öffentlich-rechtlicher Kreditinstitute geändert. Die Meldepflicht für Verfahren automatisierter Verarbeitungen sind nunmehr in § 4 d BDSG geregelt. Der Inhalt der Meldepflicht ergibt sich aus § 4 e BDSG. Die Meldepflicht entfällt gem. § 4 d Abs. 2 und 3 BDSG unter bestimmten Voraussetzungen. Eine Meldung ist danach insbesondere dann nicht erforderlich, wenn die verantwortliche Stelle einen Beauftragten für den Datenschutz bestellt hat. Da dies bei den meisten öffentlich-rechtlichen Kreditinstituten der Fall sein wird, sind diese zukünftig von der Meldepflicht befreit. Das beim LfD geführte Register wird sich dementsprechend reduzieren.

22.2 Datenweitergabe durch Sparkassen

Ein Petent warf seiner kontoführenden Sparkasse vor, sie habe seiner mit ihm in Scheidung lebenden Frau eine Liste mit allen seinen Konten ausgehändigt. Dies sei geschehen, obwohl das Kreditinstitut wusste, dass die Scheidung kurz bevorstand und der Petent alle Verfügungsberechtigungen zugunsten seiner Frau widerrufen und ausdrücklich einer Datenweitergabe widersprochen hatte. Dadurch seien ihm erhebliche Nachteile im Scheidungsverfahren entstanden.

Es stellte sich heraus, dass die damalige Ehefrau des Petenten einen Computerausdruck der unter ihrem Namen laufenden Konten erhalten hatte, der eigentlich nur bankintern genutzt wurde. Auf diesem Ausdruck waren einige Konten des Petenten verzeichnet mit dem Zusatz, dass die Verfügungsberechtigung der Ehefrau erloschen war. Der Ehefrau des Petenten wurden durch den Computerausdruck folglich nur Kontonummern der vom Petenten geführten Konten mitgeteilt, die ihr ohnehin aufgrund einer früheren Verfügungsberechtigung bekannt waren. Dies konnte nicht als datenschutzrechtlicher Verstoß gewertet werden. Daran änderte auch nichts, dass der Petent später der Datenweitergabe widersprochen hatte. Zu dem Zeitpunkt, zu dem er die Verfügungsberechtigung erteilt hatte, konnte er nicht mehr wirksam über die fraglichen Informationen disponieren. Da die Information, über welches der Konten die Ehefrau einmal verfügungsberechtigt war und wann diese Berechtigung erloschen ist, ein Datum mit Bezug auf die Ehefrau war, durfte sie als Betroffene über diese Daten verfügen.

22.3 Kontodaten des Überweisenden auf dem Kontoauszug des Empfängers

Aufgrund einer Anfrage hatte sich der LfD mit der Frage zu beschäftigen, ob das Erscheinen der Kontonummer und der Bankleitzahl auf dem Kontoauszug des Empfängers einer Geldüberweisung datenschutzrechtlich zu beanstanden war. Die Angaben über die Bankverbindung sind personenbezogene Daten. Das Erscheinen auf dem Kontoauszug des Empfängers stieß jedoch auf keine datenschutzrechtlichen Bedenken. Es war erforderlich, dass der Empfänger weiß, von wem die Zahlung stammt. Zu den erforderlichen Absenderangaben beim bargeldlosen Zahlungsverkehr gehören auch die Kontoinformationen des Überweisenden. Dadurch ist es möglich, eventuelle Fehler aufzuklären. Wenn man seine Kontoverbindung nicht preisgeben will, müsste man auf das bargeldlose Zahlungsverfahren verzichten.

22.4 Zustellung von Rechnungen

Ein Kunde der Stadtwerke einer rheinland-pfälzischen Stadt beschwerte sich darüber, dass ihm seine Wasser- und Abwasserrechnung ohne Kuvert durch einen Boten – in der Regel den Ableser selbst – in seinen Außenbriefkasten geworfen wurde. Dabei war die Abrechnung so gefaltet, dass es dritten Personen möglich gewesen wäre, die komplette Bankverbindung zu lesen.

Bei dieser Zustellungsart bestand die Gefahr, dass sich Unbefugte ohne weiteres Einblick in den Inhalt der Rechnungen mit personenbezogenen Daten verschafften, ohne Spuren zu hinterlassen. Nicht nur der Bote erhielt diese einfache Möglichkeit der Kenntnisnahme, sondern auch Hausangehörige, die nicht Rechnungsempfänger waren, und auch weitere Personen, die Zugang zum Briefkasten hatten. Zwar kannten die Boten, wenn sie den Zählerstand abgelesen hatten, die Verbrauchsdaten des Betroffenen, jedoch enthielt die Rechnung auch andere Angaben (z. B. die Kontonummer des Empfängers), die ihnen sonst nicht zugänglich waren. Unter diesen Gesichtspunkten hielt der LfD das Zustellungsverfahren nicht für datenschutzgerecht. Gegen eine Zustellung durch Boten war nichts einzuwenden, wenn die Abrechnungen in einem verschlossenen Umschlag eingeworfen wurden. Dies verhinderte zwar nicht die Kenntnisnahme durch Unbefugte, erhöhte jedoch die Hemmschwelle, Einsicht in die Rechnungen zu nehmen. Die Stadtwerke sagten daraufhin zu, Rechnungen künftig nur im verschlossenen Umschlag zuzustellen.

22.5 Datenübermittlung zur Kundenpflege

Ein rheinland-pfälzisches Versorgungsunternehmen übermittelte Kundendaten an einen Stromkonzern, der an dem Versorgungsunternehmen beteiligt war. Dabei handelte es sich um Kunden, die ihren Versorgungsvertrag gekündigt hatten. Diese Kundendaten sollten beim Stromkonzern ausgewertet werden, um Maßnahmen ergreifen zu können, die Betroffenen als Kunden zurückzugewinnen.

Da der Stromkonzern am Versorgungsunternehmen beteiligt war, bestanden zwischen beiden Unternehmen Geschäftsbeziehungen. Beiden war das Interesse zu unterstellen, die Kunden als solche halten zu wollen. Die fragliche Datenübermittlung war daher gem. § 28 Abs. 1 Nr. 2 BDSG zulässig. Danach ist das Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke zulässig, soweit es zur Wahrung berechtigter Interessen der speichernden Stelle erforderlich ist und kein Grund zur Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt.

Die berechtigten Interessen des Versorgungsunternehmens (nur dieses unterstand der datenschutzrechtlichen Kontrolle des LfD) zur Verfolgung eigener Geschäftszwecke bestanden im Hinblick auf individuelle Werbung, um Kunden besser auf die eigene Leistung aufmerksam zu machen und zugleich neue Abnehmer zu gewinnen oder ehemalige Kunden zeitnah zurückzugewinnen. Intensivere Beziehungen zu den jeweiligen Kunden zählen ebenso wie verstärkte Bemühungen, den Kundenkreis auszuweiten bzw. zu erhalten, zweifellos zu den legitimen geschäftspolitischen Zielen. Hierfür ist in der Regel eine gewisse Anzahl von personenbeziehbaren Daten erforderlich. Anhand des Jahresverbrauchs ließ sich z. B. entscheiden, ob der Betroffene aufgrund eines höheren Verbrauchs als Kunde eher zurückgewonnen werden sollte als ein Kunde mit niedrigerem Verbrauch. Der LfD betrachtete daher die vorliegende Datennutzung und -übermittlung als Mittel zur Wahrung berechtigter Interessen und zur Erfüllung eigener Geschäftszwecke des Versorgungsunternehmens.

Das Interesse der Betroffenen am Ausschluss der Verarbeitung überwog hier nicht. Diese Interessen bestanden beim Wechsel des Stromlieferanten in der Regel darin, den preiswertesten Anbieter zu wählen. Daher war auch ein Interesse daran zu unterstellen, sich vom ehemaligen Lieferanten evtl. ein günstigeres Angebot machen zu lassen. Unter Umständen konnte der Wechsel sogar Mittel sein, den alten Anbieter zu einem besseren Angebot zu bewegen. Daher hatte auch der ehemalige Kunde in der Regel ein Interesse daran, über Angebote des alten Stromlieferanten informiert zu werden.

Insgesamt war daher das Vorgehen des Versorgungsunternehmens nicht als datenschutzrechtlich unzulässig anzusehen, wenn mit Hilfe des Stromkonzerns als am Unternehmen Beteiligter versucht wurde, ehemalige Kunden zurückzugewinnen. Diese Beurteilung galt erst recht vor dem Hintergrund, dass zukünftig Daten ohne Name und Anschrift der Betroffenen übermittelt werden sollten und damit in erster Linie eine Einschätzung des Marktes ermöglicht werden sollte, die die Individualinteressen der ehemaligen Kunden zunächst nicht berührte.

22.6 Data Warehouse bei Sparkassen

Bei der Nutzung von Data Warehouses werden alle in einem Unternehmen bekannten Daten automatisiert gesammelt und evtl. durch externe Daten ergänzt. Dieser Datenbestand kann dann nach beliebigen thematischen oder statistischen Gesichtspunkten ausgewertet werden. Das hat zur Folge, dass Daten evtl. nicht mehr ihrem ursprünglichen Erhebungs- und Speicherungszweck dienen, da sie jetzt mit anderen Daten in Kombination andere Nutzungsmöglichkeiten eröffnen. Daran knüpft sich dann auch die Frage, ob die ursprünglich erteilte Einwilligung der Betroffenen zur Datenverarbeitung noch diese Datennutzung einschließt. Die rheinland-pfälzischen Sparkassen sind derzeit im Begriff, ein solches Data Warehouse aufzubauen.

Als Rechtsgrundlage für die Einrichtung und Nutzung eines Data Warehouses kommt § 28 Abs. 1 Nr. 1 BDSG in Betracht. Danach ist die Nutzung personenbezogener Daten als Mittel für die Erfüllung eigener Geschäftszwecke im Rahmen der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen zulässig. Es kommt daher darauf an, wie der Vertrag zwischen Sparkasse und Kunde ausgestaltet ist. Ist er auf eine Einzelleistung beschränkt (z. B. Führen eines Girokontos), legitimiert dies keine umfassende Beratung des Kunden, sondern lediglich eine Nutzung der bekannten Daten im Rahmen der Abwicklung des Einzelvertrages (im Beispiel also des Girovertrages). Eine darüber hinausgehende Nutzung im Sinne eines Data Warehouses ist hier nicht von § 28 Abs. 1 Nr. 1 BDSG gedeckt. Etwas anderes kann gelten, wenn mit dem Kunden ein umfassender Beratungsvertrag über alle Bankfragen abgeschlossen wurde. Fraglich ist allerdings, ob ein solcher Vertrag wirksam ist, da er womöglich nicht transparent genug für den Kunden die Datenverarbeitungsvorgänge erläutert.

Zurzeit befindet sich das Data Warehouse bei den rheinland-pfälzischen Sparkassen noch im Aufbau. Es werden nur Teilelemente eingesetzt und dies nur bei wenigen Sparkassen. Eine Auswertung erfolgt derzeit regelmäßig nicht in kundenbezogener Form. Derzeit liegt der Schwerpunkt auf der Auswertung der Umsatzzahlen einzelner Mitarbeiter. Dabei sind Kundendaten nicht personenbezogen vorhanden. Diese Art der Auswertung ist in einer speziellen Dienstvereinbarung geregelt, so dass hiergegen keine datenschutzrechtlichen Bedenken bestehen. Informationen über den Kunden selbst sind nicht viel anders als im herkömmlichen Kundeninformationssystem (KIS) gespeichert. Die Beratung bzw. das Ansprechen der Kunden erfolgt nach Aussage der Sparkassen auch nur im bisher üblichen Rahmen.

Der LfD hat daher zurzeit keine datenschutzrechtlichen Bedenken erhoben. Er wird das Projekt jedoch weiterhin begleiten. Die Sparkassen haben auch eine entsprechende Zusammenarbeit zugesagt.

23. Sonstiges

23.1 Weitergabe von Informationen im Rahmen einer Bauvoranfrage

Ein Petent warf einer Verbandsgemeindeverwaltung vor, Informationen über seine Bauvoranfrage an seine Mieter weitergegeben zu haben. Diese Mieter hätten zumindest genaue Informationen aus diesem Verfahren in einem Rechtsstreit mit dem Petenten angeführt. Die Verbandsgemeinde hat auf Nachfrage mitgeteilt, dass die Mieter zu keinem Zeitpunkt Akteneinsicht beantragt hätten und diese Akteneinsicht auch nicht erhalten hätten, da hierzu der Nachweis des berechtigten Interesses erforderlich gewesen wäre. Eine weitere Aufklärung war laut Auskunft der Verbandsgemeinde nicht möglich, da die zuständige Sachbearbeiterin nicht mehr in der Verwaltung tätig sei. Es war dem LfD daher nicht möglich aufzuklären, ob die Informationen durch ein Fehlverhalten der Verbandsgemeinde bzw. einer anderen öffentlichen Stelle an die Mieter gelangt waren.

23.2 Verpflichtung zur Übernahme des Amtes des behördlichen Datenschutzbeauftragten

Aus einer Verbandsgemeinde wurde an den LfD die Frage herangetragen, ob ein Mitarbeiter die Ausübung des Amtes des behördlichen Datenschutzbeauftragten verweigern bzw. ob er dieses Amt von sich aus aufgeben dürfe.

Nach dem Landesdatenschutzgesetz darf zum Datenschutzbeauftragten nur bestellt werden, wer die zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit besitzt. Die Mitbestimmung des Personalrats ist im Landespersonalvertretungsgesetz ausdrücklich vorgesehen. Darüber hinausgehende Anforderungen hat der Gesetzgeber nicht aufgestellt. Das bedeutet, dass für alle weiteren Fragen bei der Auswahl eines Datenschutzbeauftragten, die nicht die Fachkunde und Zuverlässigkeit betreffen, andere gesetzliche oder vertragliche Regeln eingreifen. Im Arbeitsverhältnis ist das in der Regel der Arbeitsvertrag, im Beamtenverhältnis das Landesbeamtengesetz. Demgemäß kann die Tätigkeit des Datenschutzbeauftragten wie jede andere Tätigkeit einem Beamten oder Angestellten zugewiesen werden; er hat diese im Rahmen seiner persönlichen Fähigkeiten auszuüben. Dabei hat der Dienstherr wie bei allen anderen Aufgabenzuweisungen seine Fürsorgepflicht zu beachten. Im Umkehrschluss bedeutet dies, dass der Beamte oder der Angestellte nicht von sich aus die Tätigkeit des Datenschutzbeauftragten aufgeben darf. Dies wäre als Nichterfüllung von Pflichten anzusehen und könnte als Dienstvergehen bei Beamten oder als Verletzung des Arbeitsvertrages bei Angestellten gewertet werden.

Sollte sich ein Mitarbeiter weigern, das Amt des Datenschutzbeauftragten zu übernehmen, bringt er damit möglicherweise mangelnde Motivation und eine dem Datenschutz gegenüber ablehnende Haltung zum Ausdruck. In diesen Fällen ist zu befürchten, dass der Mitarbeiter die Tätigkeit des Datenschutzbeauftragten nicht den gesetzlichen Anforderungen entsprechend ausführen wird. Daher sollte hier von einer Bestellung abgesehen werden.

Eine Abberufung durch die Behördenleitung ist jedenfalls in den Fällen zulässig, in denen der behördliche Datenschutzbeauftragte dies ausdrücklich wünscht oder dies im Rahmen personeller oder organisatorischer Veränderungen geboten ist.

23.3 Fernseh-Reportagen über behördliches Handeln und Datenschutz

Immer häufiger kommt es vor, dass Fernsehsender im Rahmen von Reportagen oder sonstigen Berichterstattungen Amtsträger bei ihrer täglichen Arbeit begleiten. Die Palette dieser Reportagen ist breit: Sie reicht von Berichten über die Tätigkeit von Polizeibeamten in verschiedenen Funktionen über die Arbeit von Gerichtsvollziehern bis zu den Tätigkeiten von Sozialhilfeermittlern. Zwangsläufig kommen bei solchen Berichten auch diejenigen Bürger mit den Fernsehjournalisten in Kontakt, die vom amtlichen Handeln der begleiteten Amtsträger betroffen sind.

Der LfD nahm eine Eingabe, in der sich ein Sozialhilfeempfänger darüber beschwerte, dass der Außendienstmitarbeiter des Sozialamtes im Rahmen einer örtlichen Feststellung von einem Fernsehteam begleitet wurde, zum Anlass, die Behörden des Landes auf Folgendes hinzuweisen:

Bereits die Information darüber, dass ein bestimmter Bürger (aus welchem Anlass auch immer) in Kontakt zu einem Amtsträger tritt bzw. dass ein Amtsträger aus dienstlichem Anlass Kontakt mit einem Bürger aufnimmt, ist eine datenschutzrechtlich geschützte Information. Dass ein Bediensteter eines Finanzamtes in amtlicher Eigenschaft gegenüber einem bestimmten Steuerpflichtigen tätig werden will, ist eine Information, die dem Steuergeheimnis unterliegt; wenn ein Bediensteter eines Sozialleistungsträgers gegenüber einem Sozialhilfeempfänger tätig werden will, unterliegt diese Information regelmäßig dem Sozialgeheimnis. Dem allgemeinen Datengeheimnis sind diese Informationen in der allgemeinen Verwaltung unterworfen, wenn keine speziellen Geheimhaltungsvorschriften gelten.

Es reicht in diesen Fällen nicht aus, die betroffenen Bürger vor dem Erstellen von Fernsehbildern in Anwesenheit der Journalisten um ihr Einverständnis zu bitten. Externe Personen dürfen ohne vorherige Zustimmung der Betroffenen gar nicht erfahren, dass eine Behörde und welche Behörde aus welchem Anlass mit ihnen in Kontakt tritt. Grundsätzlich ist also eine vorherige Kontaktaufnahme mit den betroffenen Bürgern ohne Anwesenheit von Reportern erforderlich, um abzuklären, ob ein Einverständnis erteilt wird.

Aus der Sicht des Grundrechtsschutzes ist dabei auch bedeutsam, dass es für keinen Bürger zumutbar ist, in Anwesenheit von filmbereiten Fernsehjournalisten unter erheblichem Zeitdruck eine Entscheidung darüber zu treffen, ob eine Zustimmung zur Fertigung solcher Filmaufnahmen erteilt wird. Dabei ist zu berücksichtigen, dass die betroffenen Bürger sich nicht selten in einer Drucksituation befinden, wenn sie über ihre Zustimmung in einer Situation entscheiden müssen, in der sie sich von amtlichen Maßnahmen des anwesenden Amtsträgers abhängig fühlen.

Die datenschutzrechtlichen Aspekte, die bei Fernseh-Reportagen über behördliches Handeln zu beachten sind, wurden in einer Orientierungshilfe zusammengefasst, die über das Internet-Angebot des LfD bezogen werden kann.

23.4 Videoüberwachung von Hauseingangsbereichen

Aus anderen Bundesländern wurde bekannt, dass dort Hauseingänge videoüberwacht wurden und die so aufgenommenen Bilder in den hauseigenen TV-Kabelkanal eingespeist wurden. Das ermöglichte jedem Bewohner, stets zu überprüfen, wer sich im Hauseingangsbereich aufhielt. Von Wohnungsgesellschaften in öffentlicher Trägerschaft in Rheinland-Pfalz ist ein solches Verfahren bisher nicht bekannt. Dies hält der LfD auch für datenschutzrechtlich bedenklich, weil dadurch eine dauerhafte Möglichkeit der unkontrollierten Speicherung und Verarbeitung personenbezogener Informationen gegeben ist, denn die Bildübertragungen können von Bewohnern aufgezeichnet werden.

Die Überwachung des Hauseinganges verfolgt zwei Ziele: Einmal soll der Bewohner bildlich informiert werden, wer an seiner Haustür klingelt, zum anderen soll gewährleistet werden, dass im Hauseingangsbereich keine rechtswidrigen Handlungen begangen werden bzw. solche aufgeklärt werden können. Für erstgenannten Zweck ist eine Aufzeichnung nicht erforderlich. Dieser Zweck wird dadurch erfüllt, dass das Bild des Besuchers beim Klingeln auf einen Bildschirm beim Bewohner übertragen wird. Im anderen Fall kann zwar eine Aufzeichnung von gewisser Dauer als erforderlich angesehen werden, dazu ist es aber nicht notwendig, dass den Bewohnern diese Aufzeichnungen zur Verfügung stehen. Vielmehr sollten diese von einer bestimmten Person oder einem überschaubaren Personenkreis im Auftrag der Hausverwaltung überprüft werden. Dabei ist auch sicherzustellen, dass die Aufzeichnungen unmittelbar nach Wegfall der Erforderlichkeit gelöscht werden. Ebenso ist es erforderlich, den Betroffenen vor Aufnahme durch eine Kamera auf die Aufzeichnung hinzuweisen.

23.5 Unterhaltssicherungsgesetz

Das Bundesministerium der Verteidigung hatte sich an alle für die Durchführung des Unterhaltssicherungsgesetzes zuständigen obersten Landesbehörden gewandt und die Frage aufgeworfen, ob die USG-Behörden den Truppenteilen die Höhe der für Selbstständige gewährten USG-Leistungen mitteilen dürfen, um das Kostenbewusstsein zu schärfen und bei künftigen Wehrübungen des betreffenden Reservisten die Notwendigkeit der Wehrübung auch unter dem Gesichtspunkt der Kosten- und Leistungsverantwortung einer kritischen Prüfung unterziehen zu können. Das Bundesministerium der Verteidigung hatte hierzu um Mitteilung der Auffassung der zuständigen Landesbehörden – insbesondere unter Berücksichtigung des Datenschutzes – gebeten.

Der LfD hat gegenüber dem Ministerium des Innern und für Sport die Auffassung vertreten, dass eine solche Datenübermittlung nicht zulässig ist. Eine entsprechende spezialgesetzliche Rechtsgrundlage für die Übermittlung besteht nicht, sodass sich deren Zulässigkeit nach § 14 LDSG richtet. Dies setzt voraus, dass die Datenweitergabe für die Aufgabenerfüllung der Truppenteile erforderlich ist. Die Durchführung von Wehrübungen und Ausnahmen hiervon sind im Wehrpflichtgesetz geregelt. Weder hieraus noch aus anderen Vorschriften ergibt sich, dass die Zahlung von USG-Leistungen ein entscheidendes Kriterium für die Auswahl ist. Vielmehr soll es gerade die USG-Leistung ermöglichen, alle Wehrpflichtigen unabhängig von ihrer wirtschaftlichen Situation zu Übungen heranzuziehen. Würde eine entsprechende Zahlung als Auswahlkriterium berücksichtigt, würde man den Sinn der Unterhaltssicherungsleistungen ins Gegenteil verkehren.

24. Schlussbemerkung

24.1 Zur Situation der Geschäftsstelle

Bereits im 16. und 17. Tb. (jeweils Tz. 24.1) hat der LfD zum Ausdruck gebracht, dass er in Bezug auf die Personalausstattung im Bereich des technischen Datenschutzes eine Verstärkung für unabdingbar halte. Die Notwendigkeit, auch angesichts der dramatischer werdenden Haushaltslage des Landes die Geschäftsstelle in diesem Sektor zu vergrößern, hat sich bestätigt. Für die anstehende Aufstellung des Doppelhaushalts 2002/2003 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 und der zunehmenden Bedeutung der digitalen Kommunikation in den letzten Jahren quantitativ und qualitativ erheblich erhöht hat. Die wesentlichen Bereiche sind zusammenfassend in der Vorbemerkung (Tz. 1.1) und ausführlicher unter der Überschrift „Technischer und organisatorischer Datenschutz“ (Tz. 21) dargestellt.

Im vorliegenden Entwurf des Haushaltsplans ist dieses zwingende Erfordernis mit der Ausweisung einer zusätzlichen Planstelle anerkannt worden. Der LfD hofft, dass damit die Realisierung seines Anliegens absehbar ist.

Die Unterstützung durch die Landtagsverwaltung (z. B. Druckerei, Personalabteilung, Poststelle etc.) und ihre Spitze bei der Wahrnehmung der Verwaltungsaufgaben des LfD hat sich im Berichtszeitraum erneut und wiederum bewährt. Dadurch konnten die vorhandenen Personalressourcen optimal für die Erfüllung seiner sachlichen Aufgaben eingesetzt werden. Besonderer Dank gilt dem Präsidenten des Landtags und dem ausgeschiedenen Direktor des Landtags Günter Diehl. Dass die größer werdenden Aufgaben trotz der „dünnen Personaldecke" bewältigt werden konnten, ist auf den engagierten Einsatz der Mitarbeiterinnen und Mitarbeiter der Dienststelle des LfD zurückzuführen, die mit Umsicht und Augenmaß ihre Arbeit zügig verrichtet haben. Dafür gebührt ihnen Dank und Anerkennung.

24.2 Zur Öffentlichkeitsarbeit des Landesbeauftragten für den Datenschutz

Das Internet-Angebot des LfD (www.datenschutz.rlp.de) wurde mit eigenen personellen Mitteln erweitert und ausgebaut, ohne dass im Berichtszeitraum nennenswerte Mittel aus dem Sachhaushalt zusätzlich dafür eingesetzt werden mussten. Die vorliegenden Rückmeldungen bestätigen den Ansatz, in erster Linie sachorientierte Informationen bereitzustellen. Sie zeigen weiterhin, dass der LfD als Institution zunehmend über seinen Internet-Auftritt wahrgenommen wird und der Stellenwert elektronisch verfügbar gemachter Informationen dem schriftlicher Veröffentlichungen häufig gleichwertig ist. Aufgrund der steigenden Bedeutung dieses Mediums ist im Blick auf eine bessere Erschließbarkeit der angebotenen Informationen und eine ansprechende Gestaltung eine Überarbeitung des Angebots unter Inanspruchnahme professioneller Hilfe vorgesehen.

Anlässlich des 25-jährigen Jubiläums des Datenschutzes in Rheinland-Pfalz wurde eine CD-ROM herausgegeben mit einschlägigen Informationen über den Datenschutz in unserem Lande.

Auch für den Bereich der Schulen wurde eine eigene CD-ROM herausgegeben, die wichtige Informationen für die schulischen Datenschutzbeauftragten enthält.

Die Schriftenreihe des LfD wurde aktualisiert; insbesondere die Sammlung der datenschutzrechtlichen Vorschriften wurde auf den neuesten Stand gebracht; auch sie ist im Internet abrufbar.

Mitarbeiter des LfD sind häufig als Dozenten, insbesondere bei Schulungen behördlicher Datenschutzbeauftragter, tätig geworden.

Die Dienststelle hat sich an zwei „Tagen der offenen Tür", die vom Landtag veranstaltet wurden, beteiligt. Viele der Besucher zeigten ein erstaunlich starkes Interesse für den Datenschutz.

Zu einer Vielzahl von Themen wurden Presseerklärungen herausgegeben. Diese werden zeitgleich im Internet unter der Rubrik „Aktuelles" der Allgemeinheit zur Verfügung gestellt.

Der LfD hat sich am „Virtuellen Datenschutzbüro" (vgl. Tz. 23.7), dem Internetportal der Datenschutzbeauftragten des Bundes und der Länder sowie assoziierter Stellen (ausländische Datenschutzbeauftragte, kirchliche Datenschutzbeauftragte und sonstige Institutionen aus dem öffentlichen Bereich) beteiligt.

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.

Im Dezember 2000 nahm ein neuer Service der Datenschutzbeauftragten aus Deutschland, der Schweiz, den Niederlanden und Kanada seinen Betrieb auf: das Virtuelle Datenschutzbüro. Neben einem umfassenden und vielschichtigen Informationsangebot finden sich dort Diskussionsforen zu aktuellen Datenschutzthemen sowie ein Informationsdienst („Newsticker"). Außerdem wird ein Bereich mit Datenschutz-Programmen eingerichtet, die sich jeder Internet-Nutzer installieren kann. Das Virtuelle Datenschutzbüro soll zudem als eine weltweite Plattform für Projekte und Entwicklungen zum Thema Datenschutz dienen, in dem sich auch Teams zusammenfinden, die gemeinsam neue datenschutzfördernde Techniken (Privacy-Enhancing Technologies) für die Nutzung entwickeln. Das Virtuelle Datenschutzbüro möchte den Herausforderungen für die Privatsphäre, die das grenzüberschreitende Internet mit sich bringt, begegnen. Zugleich soll durch Arbeitsteilung, Spezialisierung und systematische Bündelung ihrer Ressourcen die Effizienz der Datenschutzbeauftragten gesteigert werden.

Der LfD steuert zum Virtuellen Datenschutzbüro zunächst Folgendes bei:

- Moderation des Themas „Datenschutz und Europäische Union"
- Ausarbeitung zu datenschutzrechtlichen Aspekten im Krankenhausbereich
- Ausarbeitung zum Datenschutz in der wissenschaftlichen Forschung
- Datenschutzrechtliche Beurteilung von Einzelfällen der Video-Überwachung.

Im Berichtszeitraum hat auch ein Meinungsaustausch mit den Datenschutzbeauftragten des ZDF (Herrn Christoph Bach) und des SWR (Herrn Prof. Dr. Armin Herb) stattgefunden. Hier wurde weitgehend Übereinstimmung in der datenschutzrechtlichen Bewertung von Fragen erzielt, die von gemeinsamem Interesse sind.

Die zum 1. Juli 2001 in Kraft getretene Ergänzung des Bundesdatenschutzgesetzes hat einige datenschutzrechtliche Wünsche offen gelassen (s. o. Tz. 2.1). Weiter gehende datenschutzrechtliche Anliegen (z. B. Einführung eines Datenschutzaudits, Regelungen zum Selbstdatenschutz) sollen in einer zweiten Stufe realisiert werden. Zu diesem Zweck erfolgen intensive Diskussionen zwischen Sachverständigen und Politikern. Die Regierungsfraktionen im Deutschen Bundestag haben einen Beirat einberufen, in dem diese Erörterungen unmittelbar zu gesetzgeberischen Vorschlägen führen sollen. Der LfD ist Mitglied dieses Beirats und hat regelmäßig an entsprechenden Sitzungen teilgenommen.

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. In Folge des Ablaufs der Wahlperiode im Berichtszeitraum und der Neukonstituierung des Landtags sind langjährige Mitglieder ausgeschieden (Frau Abgeordnete Friedel Grützmacher, die Herren Abgeordnete Jürgen Creutzmann und Hendrik Hering, Herr Staatssekretär Dr. Ernst Theilen) und neue an ihre Stelle getreten (Frau Abgeordnete Beate Reich, die Herren Abgeordnete Dr. Peter Schmitz und Nils Wiechmann, Herr Staatssekretär Karl Peter Bruch), die mit den bisherigen Mitgliedern (die Herren Abgeordnete Johannes Berg, Carsten Pörksen und Axel Redmer sowie dem Vorsitzenden, Herrn Abgeordneten Franz Josef Bischel, der mit seiner nahezu 20-jährigen Erfahrung im Bereich des Datenschutzes stets seine große fachliche Kompetenz in die Beratungen einbringt) die Kommission beim Landesbeauftragten für den Datenschutz bilden. Der LfD dankt an dieser Stelle besonders auch den ausgeschiedenen 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

Zum Thema Datenschutz sind in unserer Gesellschaft die verschiedensten Tendenzen erkennbar:

Das Sendeformat „Big Brother" hat erneut verdeutlicht, dass eine nicht geringe Zahl von Personen den Schutz ihrer Privat-, sogar den ihrer Intimsphäre nicht für sonderlich erstrebenswert hält. Für eine kurzlebige Bekanntheit, für einen zweifelhaften Ruhm und für die Aussicht auf Geld werden körperliche und seelische Intimitäten der Öffentlichkeit zugänglich gemacht.

Andererseits werden Befürchtungen verbreitet, wonach z. B. jedes Gespräch über Satellit abhörgefährdet sei, wonach das Ende der Privatheit erreicht sei, und durch die Genanalyse der gläserne Mensch entstehe. Viele Gruppen und Publikationsorgane malen datenschutzrechtliche Horrorszenarien.

Die Tätigkeit des LfD und der hier vorliegende Bericht sollen einen Beitrag zur Versachlichung der Diskussion und zur realistischen Lageeinschätzung leisten. Der LfD hofft, dass ihm dies auch mit dem vorliegenden Bericht gelungen ist.

Die provokante These „Schafft den Datenschutz ab! Er schadet mehr als er nützt" (vgl. den Beitrag von Blatt, Datenschutznachrichten 3/2001, S. 8 f.) bringt sicher einen Maßstab zum Ausdruck, an dem sich die Datenschützer messen lassen müssen. Der LfD ist allerdings der Auffassung, dass gerade die amtlichen Datenschutzbeauftragten insgesamt dazu beitragen, dass der Staat seine Pflicht ernst nimmt, die schützenden Garantien zu schaffen, die für die Informationsgesellschaft wesentlich sind. Informationelle Selbstbestimmung durch staatliche Gewährleistung ist nach wie vor ein anzustrebendes und tendenziell erreichbares Ziel, dem die Tätigkeit der Datenschutzbeauftragten dient. Die vielen kleinen verteilten Informationspools, die durch die aktuelle Technikentwicklung entstanden sind und ständig neu entstehen, machen die Aufgabe des Datenschutzes gewiss immer komplexer und komplizierter. Neue Methoden des Datenschutzes, die im Zusammenhang mit der Novellierung des Bundesdatenschutzgesetzes erörtert werden, die Betonung des Informationsgleichgewichts zwischen dem Staat und den Bürgerinnen und Bürgern und die Entwicklung datenschutzfreundlicher Technologien könnten gegensteuern.

Richtig ist allerdings auch, dass der Staat das informationelle Selbstbestimmungsrecht nicht allein gewährleisten kann. Sowohl die privaten Anbieter von EDV-Verfahren und -Geräten wie die Nutzer müssen einen Bedarf an Datenschutz erkennen und realisieren. Wenn die Bürgerinnen und Bürger nicht selbst ein entsprechendes Interesse haben und im Rahmen des ihnen Möglichen daran mitwirken, Kommunikation und Datenverarbeitung zu sichern – etwa durch die Nachfrage nach abgesicherten Verfahren, durch den Einsatz von Verschlüsselungen, digitalen Unterschriften etc. –, wird der Datenschutz unter den Bedingungen der allgegenwärtigen Informationsverarbeitung unvollständig und unvollkommen bleiben.

Die Datenschutzbeauftragten haben deshalb unverändert die wichtige Aufgabe, durch Information und Aufklärung der Bürgerinnen und Bürger an einer Erhöhung des Datenschutzniveaus mitzuwirken. Auch dies wird ein künftiger Schwerpunkt der Datenschutzarbeit sein müssen.

Anlage 1

Entschließung
der 58. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 7./8. Oktober 1999
Patientenschutz durch Pseudonymisierung

Im Gesundheitsausschuss des Deutschen Bundestages wird derzeit der vom Bundesministerium für Gesundheit vorgelegte Gesetzentwurf zur Gesundheitsreform 2000 dahin gehend geändert, dass die Krankenkassen künftig von den Leistungserbringern (z. B. Ärztinnen und Ärzte, Krankenhäuser, Apotheken) die Patientendaten nicht in personenbezogener, sondern in pseudonymisierter Form erhalten. Dieses neue Modell nimmt eine zentrale Forderung der Datenschutzbeauftragten auf, für die Verarbeitung von Patientendaten solche technischen Verfahren zu nutzen, die die Persönlichkeitsrechte der Betroffenen wahren und so die Entstehung des „gläsernen Patienten" verhindern.

Auch anhand von pseudonymisierten Daten können die Krankenkassen ihre Aufgaben der Prüfung der Richtigkeit der Abrechnungen sowie der Wirtschaftlichkeit und der Qualität der Leistungen erfüllen.

Die Konferenz unterstützt den Bundesbeauftragten für den Datenschutz dabei, dass in den Ausschussberatungen die Wirksamkeit der Pseudonymisierung, die gesetzliche Festlegung von Voraussetzungen für die Identifizierung der Versicherten zu bestimmten Zwecken und die Definition strikter Zweckbindung dieser Daten durchgesetzt werden.

Anlage 2

Entschließung
der 58. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 7./8. Oktober 1999
DNA-Analysen zur künftigen Strafverfolgung auf der Grundlage von Einwilligungen

In der Strafprozessordnung ist der Einsatz der DNA-Analyse zur vorbeugenden Verbrechensbekämpfung nur mit richterlicher Anordnung vorgesehen.

In einigen deutschen Ländern werden DNA-Analysen ohne richterliche Anordnung gestützt allein auf die Einwilligung der Betroffenen durchgeführt. Soweit die dabei erhobenen Daten zum Zweck der Identitätsfeststellung in künftigen Strafverfahren genutzt werden sollen, bedürfen DNA-Analysen nach der klaren gesetzlichen Regelung des DNA-Identitätsfeststellungsgesetzes jedoch einer richterlichen Anordnung. Der Richter oder die Richterin hat u. a. die Prognose zu treffen, ob Grund zur Annahme besteht, dass gegen Betroffene künftig erneut Strafverfahren wegen des Verdachts erheblicher Straftaten zu führen sind. Wenn nunmehr auch DNA-Analysen gespeichert und zum Zweck der zukünftigen Strafverfolgung genutzt werden dürfen, die auf freiwilliger Basis – also ohne richterliche Anordnung – erstellt worden sind, und dies sogar durch die Errichtungsanordnung für die DNA-Analyse-Datei beim BKA festgeschrieben werden soll, werden damit die eindeutigen gesetzlichen Vorgaben des DNA-Identitätsfeststellungsgesetzes unterlaufen.

Die von Strafgefangenen erteilte Einwilligung zur Entnahme, Analyse und Speicherung kann keine Grundlage für einen derartigen Eingriff sein. Eine wirksame Einwilligung setzt voraus, dass sie frei von psychischem Zwang freiwillig erfolgt. Da Strafgefangene annehmen können, dass die Verweigerung der Einwilligung Auswirkungen z. B. auf die Gewährung von Vollzugslockerungen hat, kann hier von Freiwilligkeit keine Rede sein. Ausschlaggebend für die Beurteilung der Freiwilligkeit einer Einwilligung ist die subjektive Einschätzung des Betroffenen. Auch wenn im Einzelfall die Weigerung von Strafgefangenen, sich einer DNA-Analyse zu unterziehen, die Entscheidung über Vollzugslockerungen nicht beeinflusst, ist dennoch davon auszugehen, dass die Befürchtung, die Verweigerung habe negative Folgen, die freie Willensentscheidung beeinträchtigt.

Die Datenschutzbeauftragten des Bundes und der Länder halten deshalb die Praxis einiger Länder, DNA-Analysen – abweichend von den gesetzlich vorgesehenen Verfahren – systematisch auf der Grundlage von Einwilligungen durchzuführen, für eine Umgehung der gesetzlichen Regelung und damit für unzulässig. Die möglicherweise mit der Beantragung richterlicher Anordnungen verbundene Mehrarbeit ist im Interesse der Rechtmäßigkeit der Eingriffsmaßnahmen hinzunehmen. Die Datenschutzbeauftragten fordern daher, DNA-Analysen zum Zweck der Identitätsfeststellung für künftige Strafverfahren nur noch auf der Grundlage richterlicher Anordnungen durchzuführen.

Anlage 3

Entschließung
der 58. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 7./8. Oktober 1999
Beschluss des Europäischen Rates zur Erarbeitung einer Charta der Grundrechte der Europäischen Union

Der Europäische Rat hat anlässlich seiner Zusammenkunft am 4. Juni 1999 in Köln die Ausarbeitung einer Charta der Grundrechte der Europäischen Union beschlossen. In dem Ratsbeschluss heißt es: „Im gegenwärtigen Entwicklungszustand der Union ist es erforderlich, eine Charta dieser Rechte zu erstellen, um die überragende Bedeutung der Grundrechte und ihre Tragweite für die Unionsbürger sichtbar zu verankern."

Die Datenschutzbeauftragten des Bundes und der Länder unterstützen nachhaltig die Initiative des Europäischen Rates zur Ausarbeitung einer europäischen Grundrechtscharta. Sie fordern Bundesregierung, Bundestag und Bundesrat auf, sich für die Einfügung eines Grundrechts auf Datenschutz in den zu schaffenden Katalog europäischer Grundrechte und dessen Verankerung in den Verträgen der Europäischen Union einzusetzen. Damit würde der herausragenden Bedeutung des Datenschutzes in der Informationsgesellschaft Rechnung getragen.

Die europäische Datenschutzrichtlinie verpflichtet die Mitgliedstaaten zur Gewährleistung des Schutzes der Grundrechte und Grundfreiheiten und insbesondere des Schutzes der Privatsphäre (Art. 1 Abs. 1). Die Datenschutzbeauftragten weisen darauf hin, dass einige europäische Länder ein Datenschutzgrundrecht in ihre Verfassung aufgenommen haben; in einigen anderen Ländern wurde ihm durch die Rechtsprechung Grundrechtsgeltung zuerkannt. In Deutschland wird das vom Bundesverfassungsgericht aus dem Persönlichkeitsrecht (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG) abgeleitete Grundrecht auf Datenschutz als solches von zahlreichen Landesverfassungen ausdrücklich erwähnt.

Anlage 4

Entschließung
der 58. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 7./8. Oktober 1999
Eckpunkte der deutschen Kryptopolitik – ein Schritt in die richtige Richtung

Das Brief-, Post- und Fernmeldegeheimnis zählt zu den traditionellen und wichtigsten Garantien einer freiheitlichen Verfassung. Artikel 10 Grundgesetz gewährleistet deshalb die freie Entfaltung der Persönlichkeit durch einen privaten, vor Dritten verborgenen Austausch von Nachrichten, Gedanken und Informationen. Deshalb darf nur in Ausnahmefällen im überwiegenden Allgemeininteresse auf gesetzlicher Grundlage in dieses Grundrecht eingegriffen werden.

Im Zuge der Privatisierung der Telekom hat der Staat sein Post- und Fernmeldemonopol verloren, so dass zum Grundrechtsschutz die bloße Abwehr unrechtmäßiger staatlicher Eingriffe nicht mehr genügt. Darüber hinaus bestehen die Möglichkeiten der staatlichen Datenschutzkontrolle in offenen Netzen nur in eingeschränktem Maße. Der Schutz personenbezogener Daten während der Verarbeitung und Übertragung ist häufig nicht ausreichend gewährleistet. Deshalb sind ergänzende staatliche Maßnahmen zum Schutz aller gegen neugierige Dritte (z. B. Systembetreiber, Unternehmen mit wirtschaftlichen Interessen, Hacker und Hackerinnen, ausländische Geheimdienste) erforderlich.

Die Privatsphäre lässt sich jedoch nur mit Rechtsvorschriften nicht ausreichend schützen. Neben bestehenden Ge- und Verboten sind wirksame technische Vorkehrungen nötig. Systemdatenschutz und datenschutzfreundliche Technologien sind unverzichtbar. Den Bürgerinnen und Bürgern müssen effektive Instrumente zum Selbstschutz an die Hand gegeben werden. Der Datenverschlüsselung kommt deshalb in einem modernen Datenschutzkonzept eine herausragende Bedeutung zu.

Bislang musste befürchtet werden, dass auf Betreiben der staatlichen Sicherheitsbehörden in Deutschland das Recht auf Verschlüsselung eingeschränkt würde. Jetzt jedoch hat die Bundesregierung mit dem Eckpunktepapier vom 2. Juni 1999 die Diskussion auf eine völlig neue Basis gestellt. Richtigerweise wird darin die Kryptografie als „eine entscheidende Voraussetzung für den Datenschutz der Bürger" besonders hervorgehoben.

Die Position der Bundesregierung, die freie Verfügbarkeit von Verschlüsselungsprodukten nicht einschränken zu wollen, wird von den Datenschutzbeauftragten des Bundes und der Länder ausdrücklich begrüßt. Damit wurde ein erster wichtiger Schritt in die richtige Richtung getan, dem jedoch weitere folgen müssen. Der im Sinne des Artikels 10 des Grundgesetzes legitime und grund-

rechtlich geschützte Anspruch aller auf unbeobachtete Telekommunikation und auf den Schutz ihrer personenbezogenen Daten sollte von der Bundesregierung noch stärker unterstützt werden. Um der Bedeutung geschützter Telekommunikation unter den Bedingungen der Informationsgesellschaft gerecht zu werden, sind konkrete Maßnahmen notwendig. Vorrangig sind zu nennen:

- Aktive Förderung des Einsatzes von Verschlüsselungstechniken in der öffentlichen Verwaltung, bei Privatpersonen und in Wirtschaftsunternehmen,
- Erbringung von Serviceleistungen, die den Gebrauch von effektiven Verschlüsselungsprogrammen für jedermann erleichtern,
- Maßnahmen zum besonderen Schutz der Telekommunikation von Berufsgruppen, die besonderen Verschwiegenheitspflichten unterliegen (z. B. Ärzte und Ärztinnen, Anwälte und Anwältinnen, Psychologen und Psychologinnen),
- Unterstützung von Wirtschaftsunternehmen beim Schutz ihrer geschäftlichen Telekommunikation,
- Förderung einer neutralen Bewertung von Verschlüsselungsprodukten mit dem Ziel, den Verbrauchern Empfehlungen für ihren Gebrauch zu geben,
- Förderung der Entwicklung europäischer Verschlüsselungsprodukte mit offen gelegten Algorithmen.

Vor diesem Hintergrund fordern die Datenschutzbeauftragten die öffentlichen Stellen auf, mit gutem Beispiel voranzugehen. Sie sollten vorbehaltlos die technischen Möglichkeiten des Einsatzes kryptografischer Verfahren zum Schutz personenbezogener Daten prüfen und derartige Lösungen häufiger als bisher einsetzen. Künftig muss Kryptografie der Standard in der Informations- und Kommunikationstechnik werden, auf deren Einsatz nur dann verzichtet wird, wenn wichtige Gründe dagegen sprechen.

Hersteller von Produkten der Informations- und Telekommunikationstechnik werden aufgefordert, die guten Voraussetzungen zur Entwicklung von Verschlüsselungsprodukten in Deutschland zu nutzen, um sichere, leicht bedienbare und interoperable Produkte zu entwickeln und den Anwendern kostengünstig anzubieten. Die Datenschutzbeauftragten des Bundes und der Länder bieten hierfür ihre Kooperation an.

Anlage 5

Entschließung
der 58. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 7./8. Oktober 1999
Aufbewahrung des Schriftguts der ordentlichen Gerichtsbarkeit und Staatsanwaltschaften

Die Datenschutzbeauftragten des Bundes und der Länder haben bereits in ihrer Entschließung zu Aufbewahrungsbestimmungen und Dateiregelungen im Justizbereich am 9./10. März 1995 gefordert, dass insbesondere die Dauer der Aufbewahrung von Strafakten nach rechtskräftigem Abschluss eines Strafverfahrens, ihre Aussonderung und Vernichtung einer Regelung durch formelles, den Grundsätzen des Volkszählungsurteils entsprechendes Gesetz bedarf.

Mit Beschluss vom 16. August 1998 hat das Oberlandesgericht Frankfurt am Main festgestellt, dass der derzeitige Zustand zwar für eine Übergangsfrist noch hinzunehmen sei, dass die Schaffung einer gesetzlichen Grundlage für die Aufbewahrung von Akten jedoch nicht als nur mittelfristige Aufgabenstellung des Gesetzgebers betrachtet werden dürfe, sondern alsbald in Angriff zu nehmen sei. In gleicher Weise hat auch das OLG Hamm mit Beschluss vom 17. September 1998 darauf hingewiesen, dass die Aufbewahrung von Strafakten einer gesetzlichen Grundlage bedarf. Auch der Entwurf des Strafverfahrensänderungsgesetzes 1999 enthält insoweit keine Regelung.

Die Datenschutzbeauftragten des Bundes und der Länder halten es daher für dringend geboten, dass unverzüglich mit der Umsetzung dieser Aufgabe begonnen wird. Sie weisen ferner darauf hin, dass auch für die Aufbewahrung von Zivilakten und Akten im Bereich der freiwilligen Gerichtsbarkeit umgehend gesetzliche Regelungen zu schaffen sind, die die Dauer der Aufbewahrung auf das erforderliche Maß festlegen.

Anlage 6

Entschließung
der 58. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 7./8. Oktober 1999
Täter-Opfer-Ausgleich und Datenschutz

Kernstück datenschutzrechtlicher Überlegungen zum Täter-Opfer-Ausgleich ist die Frage, ob Institutionen zur Durchführung des Ausgleichsverfahrens umfassende Informationen insbesondere über Opfer von Straftaten erhalten dürfen, ohne dass diese davon Kenntnis erlangt und eingewilligt haben.

Darin wäre ein unverhältnismäßiger Eingriff in das Recht auf informationelle Selbstbestimmung der Betroffenen zu sehen. Dies ist nach geltendem Recht unzulässig.

Der nunmehr vorliegende Gesetzentwurf der Bundesregierung (BR-Drs. 325/99 vom 28. Mai 1999) sieht in § 155 a Satz 3 StPO-Entwurf vor, dass nur der ausdrücklich geäußerte entgegenstehende Wille der oder des Verletzten dazu führt, dass keine Datenübermittlungen an Schlichtungsstellen erfolgen sollen. Das bedeutet, dass solche im Einzelfall gleichwohl möglich sind. Dies halten die Datenschutzbeauftragten nicht für ausreichend.

Der Bundesrat ist sogar dem Gesetzentwurf der Bundesregierung nicht gefolgt; er hat vielmehr angeregt, im Gesetz klarzustellen, dass es für solche Datenübermittlungen auf den Willen der Opfer nicht ankommen soll. Folgende Argumente werden dafür genannt: Eine vor der Einschaltung von Schlichtungsstellen durch die Justiz einzuholende Einwilligung führe dazu, dass das kriminalpolitisch wichtige Institut des „Täter-Opfer-Ausgleichs" nicht ausreichend genutzt werde. Erst die professionelle Tätigkeit der Schlichtungsstellen mit ihrem Selbstverständnis als „objektive Dritte mit dem Gebot der Unterstützung jeder Partei" könnte 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".

Dieser Argumentation widersprechen die Datenschutzbeauftragten entschieden: Die Achtung und wirksame Unterstützung der Opfer ist ein wesentliches Anliegen des Strafverfahrens. Rechtsfriede und Toleranz können nur verwirklicht werden, wenn die Strafverfolgungsbehörden bei Datenübermittlungen an Schlichtungsstellen (z. B. in der Rechtsform von Vereinen) den Willen und die Eigenverantwortung der Opfer uneingeschränkt respektieren. Auch die Sicht der Beschuldigten, ohne deren Mitwirkung der Täter-Opfer-Ausgleich nicht durchgeführt werden kann, sollte von den Strafverfolgungsbehörden dabei berücksichtigt werden. Die Konferenz der Datenschutzbeauftragten fordert deshalb, dass an der Voraussetzung der unzweifelhaften Einwilligung vor solchen Datenübermittlungen festgehalten wird.

Ferner sollte der Gesetzgeber festlegen, dass die Berichte der Schlichtungsstellen an Staatsanwaltschaft und Gericht nur für Zwecke der Rechtspflege verwendet werden dürfen. Das besondere Vertrauensverhältnis zwischen den Schlichtungsstellen und den am „Täter-Opfer-Ausgleich" Beteiligten muss gesetzlich geschützt werden.

Anlage 7

Entschließung
der 58. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 7./8. Oktober 1999
Zugriff der Strafverfolgungsbehörden auf Verbindungsdaten in der Telekommunikation

Die Ausbreitung moderner Telekommunikationsnetze und die Fortentwicklung der Informationstechnologie erfolgen in großen Schritten. Dieser technische Fortschritt hat einerseits zu einer massenhaften Nutzung der neuen Möglichkeiten der Telekommunikation und damit zu einer grundlegenden Veränderung des Kommunikationsverhaltens der Bevölkerung geführt. Andererseits erhalten dadurch die herkömmlichen Befugnisse der Strafverfolgungsbehörden zur Überwachung des Fernmeldeverkehrs eine neue Dimension, weil aufgrund der weitreichenden Digitalisierung immer mehr personenbezogene Daten elektronisch übertragen und gespeichert werden.

Die bei der Telekommunikation anfallenden Daten können mit geringem Aufwand in großem Umfang kontrolliert und ausgewertet werden. Anhand von Verbindungsdaten lässt sich nachvollziehen, wer wann mit wem kommuniziert hat, wer welches Medium genutzt hat und wer welchen weltanschaulichen, religiösen und sonstigen persönlichen Interessen und Neigungen nach-

geht. Bereits auf der Ebene der bloßen Verbindungsdaten können so Verhaltensprofile erstellt werden, die die Aussagekraft von Inhaltsdaten erreichen oder im Einzelfall sogar übertreffen. Eine staatliche Überwachung dieser Vorgänge greift daher tief in das Telekommunikationsgeheimnis der Betroffenen ein und berührt auf empfindliche Weise die Informationsfreiheit und den Schutz besonderer Vertrauensverhältnisse.

Die bisherige rechtliche Grundlage für den Zugriff der Strafverfolgungsbehörden auf Verbindungsdaten in § 12 des Fernmeldeanlagengesetzes (FAG) stammt noch aus einer Zeit, in der die analoge Vermittlungstechnik vorherrschte, nicht für jedes Gespräch personenbezogene Verbindungsdaten erzeugt wurden und die Telekommunikationsdienste in wesentlich geringerem Maße als heute genutzt wurden. Die Vorschrift erlaubt auch Zugriffe auf Verbindungsdaten wegen unbedeutender Straftaten, bei denen eine inhaltliche Überwachung der Telekommunikation unzulässig wäre. Unter Berücksichtigung der Digitaltechnik, der vollständigen Datenerfassung und der Möglichkeit zur Bildung von Verhaltensprofilen verstößt § 12 FAG daher gegen den Verhältnismäßigkeitsgrundsatz und ist somit nicht mehr geeignet, Eingriffe in das Telekommunikationsgeheimnis zu rechtfertigen.

In einem früheren Gesetzentwurf war vorgesehen, den Zugriff auf Verbindungsdaten grundsätzlich auf nicht unerhebliche Straftaten zu beschränken. Beschlossen wurde aber lediglich die unveränderte Fortgeltung des § 12 FAG, zuletzt befristet bis zum 31. Dezember 1999. Nunmehr wollen der Bundesrat und die Justizministerkonferenz die Befristung für die Weitergeltung dieser Vorschrift aufheben und es damit beim bisherigen, verfassungsrechtlich bedenklichen Rechtszustand belassen.

Die Datenschutzbeauftragten des Bundes und der Länder wenden sich entschieden gegen eine Verlängerung der Geltungsdauer des § 12 FAG und fordern stattdessen eine Neufassung der Eingriffsbefugnis unter Beachtung der grundrechtlichen Bindungen und Anforderungen, die sich aus dem von Art. 10 Grundgesetz geschützten Telekommunikationsgeheimnis ergeben.

Die gesetzliche Ermächtigung für den Zugriff auf Verbindungsdaten gehört sachlich in die Strafprozessordnung. Die gesetzlichen Zugriffsvoraussetzungen sollten in Abstimmung mit § 100 a StPO neu geregelt werden.

Anlage 8

Entschließung
der 59. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14./15. März 2000
Konsequenzen aus dem Urteil des Bundesverfassungsgerichtes zu den Abhörmaßnahmen des BND

Das Bundesverfassungsgericht hat für die Verwendung von Daten, die aus der Fernmeldeüberwachung gewonnen wurden, deutliche Schranken gezogen, die weit über den Gegenstand des Verfahrens hinaus bedeutsam sind.

Das Gericht betont die Bedeutung des Fernmeldegeheimnisses zur Aufrechterhaltung einer freien Telekommunikation, die eine Grundvoraussetzung der Informationsgesellschaft darstellt. Dieses Grundrecht erstreckt sich nach dem Urteil des Bundesverfassungsgerichtes zu den verdachtslosen Abhörmaßnahmen des BND auf jede Verwendung von Kommunikationsdaten bis hin zur Löschung, gleich welche Kommunikationstechnik genutzt wird (Telefon, E-Mail, Telefax, Internet-Abrufe o. Ä.).

Die Anforderungen des Urteils müssen auch Konsequenzen für Fallgestaltungen enthalten, bei denen personenbezogene Daten durch Maßnahmen erlangt werden, die in ihrer Art und Schwere einer Beschränkung des Fernmeldegeheimnisses gleichkommen, insbesondere etwa bei einer Erhebung durch Abhören und Aufzeichnen des nicht öffentlich gesprochenen Wortes mit dem Einsatz technischer Mittel.

Die Anforderungen aus dem Urteil sind unverzüglich umzusetzen:

- Zur Sicherung der Zweckbindung der erlangten Daten und für die Kontrolle ihrer Verwendung muss ihre Herkunft aus Eingriffen in das Fernmeldegeheimnis oder vergleichbaren Eingriffen durch eine entsprechende Kennzeichnung nach der Erfassung auch bei den Übermittlungsempfängern erkennbar bleiben.

- Die erlangten Daten müssen bei allen speichernden Stellen unverzüglich gelöscht werden, wenn sie nicht mehr erforderlich sind – es sei denn, der Rechtsschutz der Betroffenen würde dadurch verkürzt. Die Praxis von Verfassungsschutzämtern, nicht (mehr) erforderliche Daten, wenn sie sich in Unterlagen befinden, nicht zu schwärzen, kann – zumindest bei Daten, die durch Eingriffe in das Fernmeldegeheimnis oder vergleichbare Eingriffe erlangt wurden – nicht mehr aufrechterhalten werden. Um die Notwendigkeit einer späteren Schwärzung zu vermeiden, sollte bereichsspezifischen Vernichtungsregelungen bereits bei der Aktenführung Rechnung getragen werden.

Die Vernichtungspflicht ist im Licht von Art. 19 Abs. 4 GG zu verstehen. Danach sind Maßnahmen unzulässig, die darauf abzielen oder geeignet sind, den Rechtsschutz der Betroffenen zu vereiteln. Eine Löschung oder Vernichtung ist nach einem Auskunftsantrag bei allen personenbezogenen Daten unzulässig. Zudem sind personenbezogene Daten, die durch die o. g. Maßnahmen erlangt wurden, nach einer Unterrichtung der Betroffenen für einen angemessenen Zeitraum – ausschließlich zum Zweck der Sicherung des Rechtsschutzes – aufzubewahren.

- Überwachte Personen müssen von Eingriffen unterrichtet werden, sobald dadurch der Zweck der Maßnahme nicht mehr gefährdet wird. Dies gilt auch für weitere Betroffene, es sei denn, überwiegende schutzwürdige Belange der überwachten Person stehen dem entgegen (Schutz vor unnötiger Bloßstellung).

  Wie bei Eingriffen in das Fernmeldegeheimnis ist dies auch bei anderen verdeckten Maßnahmen Voraussetzung dafür, dass die Betroffenen von den ihnen zustehenden Rechten Gebrauch machen können, und daher von Art. 19 Abs. 4 GG geboten. Speicherfristen können die Unterrichtungspflicht nicht beseitigen, irrelevante Daten sind umgehend zu löschen.

  Damit sind Regelungen z. B. in Landesverfassungsschutz- und Polizeigesetzen nicht zu vereinbaren, wonach eine Unterrichtung der Betroffenen über Datenerhebungen, die in ihrer Art und Schwere einem Eingriff in das Fernmeldegeheimnis gleichkommen, unterbleibt, wenn sich auch nach fünf Jahren nicht abschließend beurteilen lässt, ob eine Gefährdung des Zweckes des Eingriffes ausgeschlossen werden kann. Zusätzlich zur unbefristeten Benachrichtigungspflicht ist eine Mitteilung an die Datenschutzkontrollstelle für den Fall vorzusehen, dass die Unterrichtung der Betroffenen länger als fünf Jahre zurückgestellt wird.

- Der Umgang des Verfassungsschutzes mit personenbezogenen Daten, die in Durchbrechung des Fernmeldegeheimnisses erhoben worden sind, ist durch eine unabhängige Datenschutzkontrollstelle lückenlos zu überprüfen.

- Eine Kontrolllücke bei personenbezogenen Daten, die durch G 10-Maßnahmen erlangt wurden, wäre verfassungswidrig. Das Bundesverfassungsgericht hat hervorgehoben, dass Art. 10 GG eine umfassende Kontrolle durch unabhängige und an keine Weisung gebundene staatliche Organe und Hilfsorgane gebietet.

- Die Kontrolle muss sich auf den gesamten Prozess der Erfassung und Verwertung der Daten einschließlich der Benachrichtigung – bei Datenübermittlungen auch bei den Datenempfängern – erstrecken.

- Der Gesetzgeber sollte festlegen, dass die Übermittlung der Daten, die Prüfung der Erforderlichkeit weiterer Speicherung sowie die Durchführung der Vernichtung und Löschung der Daten aus G 10-Maßnahmen zu protokollieren sind.

- Für eine effektive Kontrolle sind die zuständigen Stellen personell und sachlich angemessen auszustatten.

- Die Ausführungsgesetze zum G 10 müssen hinsichtlich der Kontrolle eindeutig sein. Es ist klarzustellen, inwieweit die G 10-Kommissionen auch für die Kontrolle der weiter gehenden Datenverarbeitung zuständig sind oder inwieweit die Kontrolle von den Datenschutzbeauftragten wahrzunehmen ist. Das Bundesverfassungsgericht hat gefordert, dass auch im Bereich der Landesverwaltung eine ausreichende Kontrolle existieren muss.

Anlage 9

Entschließung
der 59. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14./15. März 2000
Data Warehouse, Data Mining und Datenschutz

Mit der ständig zunehmenden Leistungsfähigkeit der Informations- und Kommunikationstechnik wächst die Menge gespeicherter personenbezogener Daten in Wirtschaft und Verwaltung weiter an. Zunehmend kommen automatisierte Verfahren zum Einsatz, die das gesammelte Datenmaterial effektiv verwalten und analysieren. Im „Data Warehouse“ werden alle verwendbaren Daten in einem einheitlichen Datenpool losgelöst von ihrer ursprünglichen Verwendung zusammengeführt. „Data Mining“ bietet Werkzeuge, die die scheinbar zusammenhanglosen Daten nach noch nicht bekannten, wissenswerten Zusammenhängen durchsuchen, Daten aufspüren, kombinieren und neue Informationen zur Verfügung stellen.

Diese Entwicklung schafft neben Vorteilen neue Gefahren und Risiken für das Grundrecht auf informationelle Selbstbestimmung und für den Schutz der Privatheit: Persönlichkeitsprofile, automatisierte Vorhersagen von Verhaltens- und Handlungsweisen, Manipulationsmöglichkeiten und zu lange Speicherung sind befürchtete Gefahren.

Die Konferenz der Datenschutzbeauftragten weist auf Folgendes hin:

- Nach dem grundrechtlichen Gebot der Zweckbindung dürfen personenbezogene Daten nur im Rahmen der gesetzlich zugelassenen Zwecke oder der gegenseitigen Vereinbarungen verwendet werden. Eine personenbezogene Speicherung in einem allgemein verwendbaren Data Warehouse entfernt sich vom ursprünglichen Verwendungszweck und stellt eine Speicherung auf Vorrat ohne Zweckbindung dar. Personenbezogene Daten, die bei der öffentlichen Verwaltung vorhanden sind, sind in ihrer Zweckbestimmung grundrechtlich geschützt und dürfen nicht für unbestimmte Zwecke in einem „Daten-Lagerhaus" gesammelt werden. Eine Zweckänderung ist nur mit Einwilligung der Betroffenen zulässig, nachdem diese über die Tragweite der Einwilligung aufgeklärt worden sind. Eine Einwilligung in unbestimmte und zeitlich unbegrenzte Zweckänderungen ist deswegen unwirksam.

- Gestaltung und Auswahl von Datenverarbeitungs-Systemen haben sich an dem Ziel auszurichten, keine oder so wenig personenbezogene Daten wie möglich zu verarbeiten. Anonyme und pseudonyme Verfahren sind datenschutzrechtlich unbedenklich.

- Verfahren sind so zu gestalten, dass die Betroffenen hinreichend unterrichtet werden, damit sie jederzeit die Risiken abschätzen und ihre Rechte wahrnehmen können. Sie haben insbesondere das Recht, eine erteilte Einwilligung jederzeit zurückzuziehen.

- Die gesetzlichen Speicherfristen, nach deren Ablauf die Daten zwingend archiviert oder gelöscht werden müssen, sind strikt zu beachten. Deswegen ist die Einrichtung von permanenten „Daten-Lagerhäusern" rechtswidrig. Die Europäische Datenschutzrichtlinie spricht grundsätzlich jeder Person das Recht zu, keiner belastenden automatisierten Einzelentscheidung unterworfen zu werden (Art. 15). „Data Mining" ist ein Instrument, das für solche Entscheidungen herangezogen werden kann.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder ruft die Hersteller und Anwender von „Data Warehouse"- und „Data Mining"-Verfahren dazu auf, solchen Programmen den Vorzug zu geben, die unter Einsatz von datenschutzfreundlichen Technologien die Speicherung von personenbezogenen Daten durch Anonymisierung oder Pseudonymisierung vermeiden.

Anlage 10

Entschließung
der 59. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14./15. März 2000
Für eine freie Telekommunikation in einer freien Gesellschaft

Umfang und Intensität der Eingriffe in das von Art. 10 Grundgesetz geschützte Fernmeldegeheimnis haben in den letzten Jahren deutlich zugenommen. Ursächlich hierfür sind zum einen folgende Aspekte:

- Erhebliche Zunahme der Telekommunikationsvorgänge

  Die Zahl der Telekommunikationsvorgänge hat sich vervielfacht. Darüber hinaus werden neben dem traditionellen Telefon neue Kommunikationsmöglichkeiten wie Fax und PC-Fax, das Mobiltelefon, E-Mail und Mail-Boxen sowie das Internet genutzt.

- Stark angestiegener Umfang und wesentlich verbesserte Aussagequalität der Daten
  - Die digitale Datenverarbeitung ermöglicht detaillierte Auswertungen großer Datenmengen.
  - Die Datenverarbeitungsnetze bieten mehr und mehr aussagekräftige Bestandsdaten, wozu auch E-Mail-Adresse, IP-Nummer oder domain name gehören. So können sich bei Mitgliedschaft in geschlossenen Netzen sogar Rückschlüsse auf Lebensanschauungen oder bestimmte Problemlagen ergeben, z. B. bei der Mitgliedschaft in bestimmten Interessengemeinschaften, etwa Aids-Selbsthilfegruppen.
  - Die Verbindungsdaten geben in der Regel Auskunft, wer wann mit wem wie lange und wie häufig kommuniziert hat; werden fremde Geräte verwendet, geraten Unbeteiligte in Verdacht.
  - Aus den Nutzungsdaten von Tele- und Mediendiensten lassen sich Rückschlüsse auf Interessengebiete und damit auf persönliche Eigenheiten und das Verhalten der Nutzenden ziehen.
  - Mobiltelefone ermöglichen schon im Stand-by-Modus die Bestimmung ihres Standorts.

- Erleichterte Kenntnisnahme und Weiterverarbeitung dieser Daten

  Die wesentlich erweiterten und einfacher nutzbaren technischen Möglichkeiten erlauben es, an verschiedenen Orten gespeicherte Daten zur Kenntnis zu nehmen und zu verarbeiten.

- Entwicklung des Internets zum Massenkommunikationsmittel

  Über das Netz werden immer mehr Alltagsgeschäfte abgewickelt: Wahrnehmung verschiedenartiger Informationsangebote, Erledigung von Bankgeschäften, Buchung von Reisen oder Bestellung von Waren und Dienstleistungen in virtuellen Kaufhäusern (E-Commerce). Dadurch fallen immer mehr auswertbare Informationen über Lebensgewohnheiten und Bedürfnisse der Bürgerinnen und Bürger an.

- Schwer durchschaubare Rechtslage

  Die Zersplitterung der Regelungen in Strafprozess-, Telekommunikations- und Multimediarecht machen diese wenig transparent und schwer anwendbar.

Zum anderen ist dieser größere, leichter auswert- und verarbeitbare Datenpool wachsenden Zugriffswünschen der Sicherheitsbehörden im weitesten Sinn auf nationaler und internationaler Ebene ausgesetzt:

- Die Zahlen der Telekommunikations-Überwachungsanordnungen in den letzten Jahren sind kontinuierlich angestiegen: 1995: 3 667, 1996: 6 428, 1997: 7 776, 1998: 9 802.

- Immer mehr Straftatbestände wurden als Grund für eine Telekommunikationsüberwachung in § 100 a der Strafprozessordnung (StPO) einbezogen – der Katalog wurde seit Einführung 11-mal erweitert und damit bis heute nahezu verdoppelt. Neue Erweiterungen sind im Gespräch.

- Die Telekommunikationsanbieter werden verpflichtet, technische Einrichtungen zur Umsetzung der Überwachungsanordnungen zu installieren und Kundendateien für Abfragen durch die Sicherheitsbehörden vorzuhalten zur Feststellung, mit welchen Anbietern verdächtige Personen einen Vertrag haben. Diese Verpflichtung wurde auch auf die Anbieter nicht gewerblicher Netze ausgedehnt und kann nach dem Gesetzeswortlaut auch Hotels, Betriebe, Behörden oder möglicherweise sogar Krankenhäuser betreffen.

- Ein europäischer Anforderungskatalog für Überwachungsmöglichkeiten unter dem Namen „ENFOPOL", befasst sich u. a. mit der Frage, welchen Anforderungen die Netzbetreiber bzw. Diensteanbieter genügen müssen, damit die auf der Grundlage nationaler Ermächtigungsgrundlagen zulässige Telekommunikationsüberwachung technisch durchführbar ist. Die G-8-Staaten haben noch weiter gehende Beschlüsse gefasst.

Forderungen zur Gewährleistung der freien Telekommunikation

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat bereits 1996 ein Positionspapier erarbeitet. Vor diesem Hintergrund fordert die Konferenz:

- Freie Telekommunikation ist unabdingbar für eine freiheitliche demokratische Kommunikationsgesellschaft. Sie wird durch das Fernmeldegeheimnis geschützt. Dieses Grundrecht erstreckt sich nach dem Urteil des Bundesverfassungsgerichts zu den verdachtslosen Abhörmaßnahmen des BND (BVerfG, Urt. v. 14. Juli 1999, 1 BvR 2226/94 u. a.) auf jede Verwendung von Kommunikationsdaten bis hin zur Löschung, gleich welche Kommunikationstechnik genutzt wird. Die Geltung des Fernmeldegeheimnisses ist deshalb auch für den Bereich der Tele- und Mediendienste ausdrücklich klarzustellen.

- Notwendig ist eine bürgerrechtsfreundliche technische Infrastruktur nach dem Grundsatz der Datenvermeidung und dem Datensparsamkeitsprinzip. Dabei ist der Einsatz datenschutzfreundlicher Technologien besonders zu fördern. Anonyme und pseudonyme Nutzungsmöglichkeiten müssen nach dem Vorbild des Teledienstedatenschutzgesetzes als Pflichtangebote vorgehalten werden. Die Nutzung dieser Angebote darf nicht von der Speicherung von Bestandsdaten abhängig gemacht werden. Eine Vorratshaltung von Daten Unverdächtiger über den Betriebszweck hinaus zu Zwecken der Verfolgung eventueller, noch gar nicht absehbarer zukünftiger Straftaten ist als Überwachung auf Vorrat abzulehnen.

- Notwendig ist deshalb ein zusammenfassendes, in sich schlüssiges System von Regelungen staatlicher Eingriffe in das Kommunikationsverhalten, das dem besonderen Gewicht des Grundrechts auf eine unbeobachtete Telekommunikation unter Beachtung der legitimen staatlichen Sicherheitsinteressen Rechnung trägt.

- Als Grundlage hierfür ist eine Evaluierung der bestehenden Eingriffsregelungen nach objektiven, nicht zielorientierten Maßstäben vorzunehmen hinsichtlich Effektivität auf der einen und Eingriffsumfang auf der anderen Seite. Eine gesetzliche Berichtspflicht über Anlass, Verlauf, Ergebnisse und Anzahl der Betroffenen ist auch für Telekommunikationsüberwachungen einzuführen. Dass auch Unverdächtige von Abhör- und Kontrollmaßnahmen betroffen sein können, ist dabei besonders zu berücksichtigen.

- Der aus der Frühzeit der analogen Fernsprechtechnik stammende § 12 Fernmeldeanlagengesetz, der die Herausgabe von Verbindungsdaten vergangener, nach bestrittener Rechtsprechung sogar zukünftiger Telekommunikationsvorgänge ohne Beschränkung auf schwerere Straftaten ermöglicht, muss wegen der erheblich höheren Aussagefähigkeit der digitalen Verbindungsdaten und des damit verbundenen Eingriffs in das Fernmeldegeheimnis zügig durch eine weniger weit reichende Regelung in der StPO ersetzt werden.

- Die Anforderungen aus dem bereits zitierten Urteil des Bundesverfassungsgerichts zur Telekommunikationsüberwachung sind unverzüglich umzusetzen.

- Die Ausweitung der Mitwirkungspflichten bei Überwachungsmaßnahmen auf Nebenstellenanlagen in Hotels, Krankenhäusern oder Betrieben wäre unverhältnismäßig. Es muss deshalb verbindlich klargestellt werden, dass die Betreiber dieser Nebenstellenanlagen nicht zur Bereitstellung entsprechender technischer Einrichtungen verpflichtet werden. Das Eckpunktepapier des Bundesministeriums für Wirtschaft und Technologie, das als Grundlage für einen Entwurf der Telekommunikations-Überwachungverordnung dient und nach verschiedenen Gruppen von Betreibern differenziert, ist dazu ein erster Schritt. Auch muss möglichst durch eine Gesetzesänderung verhindert werden, dass die Verpflichtung, Kundendateien zu führen, auch für die o. g. Nebenstellenanlagen gilt.

  Darüber hinaus dürfen Anbieter von Guthabenkarten zur Mobiltelefonie nicht dazu verpflichtet werden, Identifikationsdaten ihrer Kunden, die sie für betriebliche Zwecke nicht benötigen, ausschließlich für Zwecke der Strafverfolgungsbehörden und der Nachrichtendienste zu erheben und zum Abruf bereitzuhalten.

- Die Beachtung des Fernmeldegeheimnisses erfordert zwingend die Verschlüsselung von elektronischen Mitteilungen in offenen Netzen. Das Eckpunktepapier der Bundesregierung zur deutschen Kryptopolitik, das eine Kryptoregulierung ablehnt, ist ein wichtiger Schritt in die richtige Richtung. Gewerbliche Telekommunikationsdienstleister sollten gesetzlich verpflichtet werden, die Möglichkeit der verschlüsselten Kommunikation kostenlos zu unterstützen.

- Berufsgruppen, die besonderen Verschwiegenheitspflichten unterliegen, wie Ärztinnen und Ärzte, Anwältinnen und Anwälte, Psychologinnen und Psychologen, bedürfen besonders im Interesse ihrer Klientel eines umfassenden Schutzes ihrer Telekommunikation.

- Straftaten gegen den Schutz der Privatsphäre ist wirksamer entgegenzutreten. Notwendig sind z. B. die Prüfung eines Verbots des freien Verkaufs von Abhörtechnik, eine Verbesserung der Strafverfolgung im Bereich illegaler Abhörmaßnahmen und eine Verschärfung des strafrechtlichen Schutzes des Fernmeldegeheimnisses.

Anlage 11

Entschließung
der 59. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14./15. März 2000
Unzulässiger Speicherungsumfang in „INPOL-neu“ geplant

Das Bundeskriminalamt und die Polizeien der Bundesländer konzipieren seit geraumer Zeit unter der Bezeichnung „INPOL-neu“ eine Fortentwicklung des gemeinsamen Informationssystems. Inzwischen steht der Beginn der schrittweisen Einführung des neuen Datenaustauschsystems kurz bevor.

Das Informationssystem INPOL wirft in vielfacher Hinsicht datenschutzrechtliche Probleme auf. Die Datenschutzbeauftragten des Bundes und der Länder haben mehrfach aus konkretem Anlass darauf hingewiesen, dass nicht jede mit den heutigen technischen Möglichkeiten realisierbare oder mit polizeifachlicher Erforderlichkeit begründete Verarbeitung personenbezogener Daten zulässig ist. Bereits bei der Konzeption des INPOL-Systems muss vielmehr dafür Sorge getragen werden, dass in das Recht der Bürgerinnen und Bürger auf informationelle Selbstbestimmung nur so weit eingegriffen wird, wie dies im Rahmen der Erforderlichkeit für die polizeiliche Aufgabenerfüllung durch Rechtsvorschriften erlaubt wird.

Es besteht jedoch Grund zu der Sorge, dass es bei der Neugestaltung des INPOL-Systems zu falschen Weichenstellungen mit der Folge unzulässiger Verarbeitung personenbezogener Daten kommt. Die zu befürchtende Fehlentwicklung liegt darin, dass das Bundeskriminalamt und die Landeskriminalämter planen, künftig im Bundes-Kriminalaktennachweis (KAN) die „gesamte kriminelle Karriere“ jeder Person abzubilden, die aus Anlass eines INPOL-relevanten Delikts erfasst ist. Es sollen in diesen Fällen auch Daten über solche Straftaten gespeichert und zum Abruf bereitgehalten werden, die weder von länderübergreifender oder internationaler noch von besonderer Bedeutung sind.

§ 2 Abs. 1 BKAG beschränkt die Zuständigkeit des BKA (als Zentralstelle des polizeilichen Informationssystems) sowohl im präventiven als auch im repressiven Bereich auf „Straftaten mit länderübergreifender, internationaler oder erheblichen Bedeutung". Der Wortlaut ist eindeutig. Anknüpfungspunkt und Gegenstand der Einteilung in INPOL-relevante Informationen einerseits und INPOL-irrelevante Informationen andererseits sind die „Straftaten", nicht die einzelne Person und auch nicht das „Gesamtbild einer Person". Der Gesetzeswortlaut bildet die Grenze der Auslegung; eine über den Wortsinn hinausgehende Anwendung verstößt gegen das Gesetz. Daher ist es unzulässig, die Frage der INPOL-Relevanz unabhängig von der konkreten einzelnen Straftat zu beurteilen. Vielmehr dürfen im Bundes-KAN nur Informationen zu solchen Straftaten verarbeitet werden, die im Einzelfall die in § 2 Abs. 1 BKAG aufgestellte Bedeutungsschwelle überschreiten.

Die Datenschutzbeauftragten des Bundes und der Länder fordern das Bundesinnenministerium und die Innenministerien der Länder auf, von der geschilderten KAN-Erweiterung abzusehen.

Anlage 12

Entschließung
der 59. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14./15. März 2000
Strafverfahrensänderungsgesetz 1999 (StVÄG 1999)

Die Datenschutzbeauftragten des Bundes und der Länder begrüßen es, dass mit dem Entwurf für ein Strafverfahrensänderungsgesetz 1999 die Strafprozessordnung endlich die seit fast zwei Jahrzehnten überfälligen datenschutzrechtlichen Regelungen erhalten soll. Sie stellen jedoch fest, dass der nunmehr vorliegende Gesetzesbeschluss des Bundestages nicht alle wichtigen Forderungen des Datenschutzes erfüllt.

Darüber hinaus will der Bundesrat das Datenschutzniveau weiter absenken und hat auch zu diesem Zweck den Vermittlungsausschuss angerufen. Zu kritisieren ist, dass

- Zeuginnen und Zeugen auch bei Straftaten ohne erhebliche Bedeutung durch Öffentlichkeitsfahndung im Fernsehen oder Internet gesucht werden können,

- Zweckbindungen präventivpolizeilicher Daten, darunter auch der Erkenntnisse aus verdeckten Datenerhebungsmaßnahmen, wie z. B. einem Großen Lauschangriff oder einem Einsatz verdeckter Ermittler, völlig aufgehoben werden, so dass sie uneingeschränkt zur Strafverfolgung genutzt werden können,

- umgekehrt aber auch Informationen aus Strafverfahren über die Gefahrenabwehr hinaus uneingeschränkt zur Gefahrenvorsorge genutzt werden können,

- nicht am Verfahren beteiligte Dritte schon bei „berechtigtem Interesse" Einsicht in Strafverfahrensakten bekommen können.

Die Datenschutzbeauftragten des Bundes und der Länder sehen den verfassungsrechtlich gebotenen Ausgleich zwischen Persönlichkeitsschutz und Interessen der Strafverfolgungsbehörden nicht mehr als gewährleistet an, falls die Vorschläge des Bundesrates Eingang in die Strafprozessordnung finden sollten. Die Datenschutzbeauftragten fordern daher den Vermittlungsausschuss auf, die Änderungsanträge zurückzuweisen. Stattdessen sind Regelungen in der Strafprozessordnung vorzusehen, die geeignet sind, bei einer effektiven Strafverfolgung die Persönlichkeitsrechte der Betroffenen angemessen zu gewährleisten.

Anlage 13

Entschließung der 59. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14./15. März 2000 Risiken und Grenzen der Videoüberwachung

Immer häufiger werden Videokameras eingesetzt, die für Zwecke der Überwachung genutzt werden können. Ob auf Flughäfen, Bahnhöfen, in Ladenpassagen, Kaufhäusern oder Schalterhallen von Banken oder anderen der Öffentlichkeit zugänglichen Einrichtungen, überall müssen Bürgerinnen und Bürger damit rechnen, dass sie auf Schritt und Tritt offen oder heimlich von einer Videokamera aufgenommen werden. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder sieht darin die Gefahr, dass diese Entwicklung zur einer Überwachungsinfrastruktur führt.

Mit der Videoüberwachung sind besondere Risiken für das Recht auf informationelle Selbstbestimmung verbunden. Weil eine Videokamera alle Personen erfasst, die in ihren Bereich kommen, werden von der Videoüberwachung unvermeidbar völlig unverdächtige Menschen mit ihren individuellen Verhaltensweisen betroffen. Erfassung, Aufzeichnung und Übertragung von Bildern sind für die Einzelnen in aller Regel nicht durchschaubar. Schon gar nicht können sie die durch die fortschreitende Technik geschaffenen Bearbeitungs- und Verwendungsmöglichkeiten abschätzen und überblicken. Die daraus resultierende Ungewissheit, ob und von wem sie beobachtet werden und zu welchen Zwecken dies geschieht, erzeugt einen latenten Anpassungsdruck. Dies beeinträchtigt nicht nur die grundrechtlich garantierten individuellen Entfaltungsmöglichkeiten, sondern auch das gesellschaftliche Klima in unserem freiheitlichen und demokratischen Gemeinwesen insgesamt. Alle Menschen haben das Grundrecht, sich in der Öffentlichkeit zu bewegen, ohne dass ihr Verhalten durch Kameras aufgezeichnet wird.

Daher müssen

- eine strenge Zweckbindung,
- eine differenzierte Abstufung zwischen Übersichtsaufnahmen, dem gezielten Beobachten einzelner Personen, dem Aufzeichnen von Bilddaten und dem Zuordnen dieser Daten zu bestimmten Personen,
- die deutliche Erkennbarkeit der Videoüberwachung für die betroffenen Personen,
- die Unterrichtung identifizierter Personen über die Verarbeitung ihrer Daten
- sowie die Löschung der Daten binnen kurzer Fristen

strikt sichergestellt werden.

Jede Einrichtung einer Videoüberwachung sollte der datenschutzrechtlichen Vorabkontrolle unterzogen werden. Das heimliche Beobachten und Aufzeichnen, die gezielte Überwachung bestimmter Personen sowie die Suche nach Personen mit bestimmten Verhaltensmustern müssen grundsätzlich verboten sein. Ausnahmen müssen im Strafprozessrecht und im Polizeirecht präzise geregelt werden. Videoüberwachung darf nicht großflächig oder flächendeckend installiert werden, selbst wenn jeder Einsatz für sich gesehen gerechtfertigt wäre. Auch ein zeitlich unbegrenzter Einsatz ohne regelmäßige Erforderlichkeitsprüfung ist abzulehnen. Der Schutz der Freiheitsrechte erfordert überdies, dass heimliches Aufzeichnen und unbefugte Weitergabe oder Verbreitung von Aufnahmen ebenso strafbewehrt sein müssen wie der Missbrauch video-technisch gewonnener – insbesondere biometrischer – Daten und deren Abgleiche.

Dies bedeutet:

1. Bei einer gesetzlichen Regelung der Videoüberwachung durch öffentliche Stellen dürfen Einschränkungen nur aufgrund einer klaren Rechtsgrundlage erfolgen, die dem Grundsatz der Verhältnismäßigkeit Rechnung trägt.
   - Die Voraussetzungen einer Videoüberwachung und der mit ihr verfolgte Zweck müssen eindeutig bestimmt werden. *Dafür kommen – soweit nicht überwiegende schutzwürdige Belange von Betroffenen entgegenstehen – unter anderem in Betracht**)*:*
   - *die Beobachtung einzelner öffentlicher Straßen und Plätze oder anderer öffentlich zugänglicher Orte, auf denen wiederholt Straftaten begangen worden sind, solange tatsächliche Anhaltspunkte dafür bestehen, dass dort weitere Straftaten begangen werden (Kriminalitätsschwerpunkte) und mit der Beobachtung neben der Sicherung von Beweisen eine Präventionswirkung erreicht werden kann; der Grundsatz der Verhältnismäßigkeit ist dabei strikt zu beachten. Ungezielte Verlagerungsprozesse sollten vermieden werden;*

- *für die Verkehrslenkung nur Übersichtsaufnahmen,*
- *der Schutz öffentlicher Einrichtungen im Rahmen der ordnungsbehördlichen Gefahrenabwehr, solange eine besondere Gefahrenlage besteht.*
- Maßnahmen im Rahmen des Hausrechts dürfen den grundsätzlich unbeobachteten Besuch öffentlicher Gebäude nicht unverhältnismäßig einschränken.
- Die Videoüberwachung ist für die Betroffenen durch entsprechende Hinweise erkennbar zu machen.
- Bildaufzeichnungen sind nur zulässig, wenn und solange sie zum Erreichen des verfolgten Zweckes unverzichtbar sind. Die Anlässe, aus denen eine Bildaufzeichnung ausnahmsweise zulässig sein soll, sind im Einzelnen zu bezeichnen. Die Aufzeichnungen sind unverzüglich zu löschen, wenn sie hierzu nicht mehr erforderlich sind oder überwiegende schutzwürdige Belange von Betroffenen entgegenstehen.
- Werden die Aufnahmen einer bestimmten Person zugeordnet, ist diese zu benachrichtigen, sobald der Zweck der Speicherung dadurch nicht gefährdet wird.
- Zur Prüfung der Normeffizienz ist festzulegen, dass das jeweils zuständige Parlament jährlich über die angeordneten Maßnahmen, soweit sie mit einer Speicherung der erhobenen Daten verbunden sind, und die mit ihnen erreichten Ergebnisse unterrichtet wird.
- Bei der Videoüberwachung muss in besonderer Weise den Grundsätzen der Datensparsamkeit und Datenvermeidung Rechnung getragen werden. Die Chancen, die die modernen Technologien für die Umsetzung dieser Grundsätze, insbesondere für die Reduzierung auf tatsächlich erforderliche Daten bieten, sind zu nutzen.

2. Der Gesetzgeber ist auch aufgefordert, für die Videoüberwachung durch Private Regelungen zu schaffen, die den für die optisch-elektronische Beobachtung durch öffentliche Stellen geltenden Grundsätzen entsprechen. Dabei muss sichergestellt werden, dass optisch-elektronische Systeme, die die Identifizierung einzelner Personen ermöglichen, nur zur Abwehr von Gefahren für Personen und zum Schutz gewichtiger privater Rechte eingesetzt werden dürfen. Die privatrechtlichen Regelungen zum Schutz des eigenen Bildes durch das Vertragsrecht, das Deliktsrecht, das Besitz- und Eigentumsrecht, das Kunsturheberrecht und die dazu ergangene Rechtsprechung reichen nicht aus.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder erwartet, dass die Gesetzgeber bei der Novellierung der Datenschutzgesetze und anderer Gesetze diese Grundsätze berücksichtigen.

Anlage 14

Entschließung
der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26. Juni 2000
Effektive parlamentarische Kontrolle von Lauschangriffen durch aussagekräftige jährliche Berichte der Bundesregierung

Die Bundesregierung hat den Bundestag jährlich über die nach Art. 13 Abs. 6 Satz 1 GG zur Strafverfolgung eingesetzten „Großen Lauschangriffe“ zu unterrichten. § 100 e StPO konkretisiert die Berichtspflicht dahin gehend, dass die Bundesregierung aufgrund von Mitteilungen der Staatsanwaltschaften der Länder den Bundestag über Anlass, Umfang, Dauer, Ergebnis und Kosten der Maßnahmen zu unterrichten hat.

Diese Berichte sollen eine laufende parlamentarische Kontrolle dieser mit intensiven Grundrechtseingriffen verbundenen Maßnahmen ermöglichen. Der Bundestag soll aufgrund der Berichte in die Lage versetzt werden, die Angemessenheit und Eignung der Maßnahme zu überprüfen.

Diesen Anforderungen wird der erste von der Bundesregierung vorgelegte Bericht nicht in vollem Umfang gerecht. So wurde nur die Gesamtzahl der von der Anordnung Betroffenen erfasst, wobei zwischen Beschuldigten und nicht beschuldigten Wohnungsinhabern unterschieden wird.

Nach § 100 e Abs. 1 StPO muss über den Umfang der Maßnahme berichtet werden. Hierzu zählt die Angabe über die Anzahl aller von der Maßnahme betroffenen Personen, nicht nur der in der gerichtlichen Anordnung genannten. Von dem „Großen Lauschangriff" ist jeder betroffen, dessen gesprochenes Wort in der Wohnung abgehört wird. Er greift auch in die grundrechtlich geschützten Rechte der am Verfahren Unbeteiligten, wie z. B. unverdächtige Familienangehörige, Bekannte, Besucherinnen und Besucher sowie sonstige Personen, die nicht selbst Wohnungsinhaber sind, ein. Dem wollte der Gesetzgeber mit der Einführung der Berichtspflicht Rechnung tragen.

Die Beschränkung der Berichtspflicht auf Wohnungsinhaber und Beschuldigte gibt nicht den wirklichen Umfang der von der Maßnahme betroffenen Personen wieder. Somit erfüllt sie den Zweck der im Grundgesetz vorgesehenen Berichtspflicht nicht.

Darüber hinaus wäre es wünschenswert, wenn – wie in den „Wire-tap-Reports" der USA – die Anzahl der abgehörten Gespräche und die Anzahl der Gespräche, die mit dem Ermittlungsverfahren in Zusammenhang stehen, die Art der betroffenen Räume (Geschäftsräume, Wohnung, Restaurant etc.), die Anzahl und Dauer der angeordneten Verlängerungen der Maßnahme, die Zahl der Verhaftungen, Anklageerhebungen und Verurteilungen, zu denen die Maßnahme beigetragen hat, angegeben werden.

Die Länder haben nach Art. 13 Abs. 6 Satz 3 GG eine gleichwertige parlamentarische Kontrolle zu gewährleisten. Die oben genannten Forderungen gelten deshalb gleichermaßen bzw. in entsprechender Weise für die den Landesparlamenten vorzulegenden jährlichen Berichte über die nach § 100 c Abs. 1 Nr. 3 StPO durchgeführten Maßnahmen bzw. über die von der Polizei zur Gefahrenabwehr veranlassten „Großen Lauschangriffe".

Anlage 15

Entschließung
der 60. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 12./13. Oktober 2000
Datenschutzrechtliche Konsequenzen aus der Entschlüsselung des menschlichen Genoms

Bei der Entschlüsselung des menschlichen Genoms sind in den letzten Monaten wohl entscheidende Durchbrüche gelungen. Für mehr als 20, oft vererbliche Krankheiten sind bereits Gentests zu erwerben, mit denen in Labors analysiert werden kann, ob eine Erkrankung vorliegt bzw. in welchem Umfang ein Erkrankungsrisiko besteht. Viele dieser Krankheiten sind allerdings bisher nicht heil- oder behandelbar.

Gentechnische Untersuchungen beim Menschen eröffnen den Zugang zu höchstpersönlichen und hochsensiblen Informationen in einem Maße, das die Intensität bisheriger personenbezogener Informationen ganz erheblich übersteigt. Durch den genetischen Einblick in den Kernbereich der Privatsphäre, etwa in Gesundheitsdisposition, Anlagen der Persönlichkeitsstruktur oder den voraussichtlichen Lebensverlauf, entsteht eine ganz neue Qualität des Wissens und des Offenlegens von persönlichsten Daten. Sowohl für die Betroffenen als auch für dritte Personen, insbesondere Familienangehörige, ist es von entscheidender Bedeutung, ob und inwieweit sie selbst und wer außer ihnen von den Ergebnissen Kenntnis bekommt. Davor steht die Frage, ob und aus welchen Anlässen überhaupt genetische Untersuchungen am Menschen vorgenommen werden dürfen. Zur informationellen Selbstbestimmung gehört auch das Recht auf Nichtwissen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert, dass für die Zulässigkeit gentechnischer Untersuchungen beim Menschen und für den Umgang mit den dabei gewonnenen Informationen sehr schnell klare und verbindliche Prinzipien entwickelt werden, um auch die informationelle Selbstbestimmung in diesem Kernbereich zu sichern und zugleich eine „genetische Diskriminierung" bei der Gewinnung oder Verwendung genetischer Informationen, etwa im Arbeitsverhältnis oder beim Abschluss von Versicherungsverträgen zu verhindern. Auf der Grundlage dieser und in der „Entschließung über Genomanalyse und informationelle Selbstbestimmung" vom 26. Oktober 1989 formulierten Grundsätze wird die Konferenz an der Ausgestaltung mitwirken.

Die Datenschutzbeauftragten erinnern an ihre Grundsätze aus der Entschließung von 1989 bezüglich der Genomanalyse:

1. Die Genomanalyse darf grundsätzlich nur auf freiwilliger Basis nach umfassender Aufklärung der Betroffenen vorgenommen werden; ausgenommen sind Straf- und Abstammungsverfahren.
2. Die jederzeit widerrufliche Einwilligung muss sich auch auf die weitere Verwendung der gentechnischen Informationen erstrecken. Im Falle eines Widerrufs sind die gewonnenen Informationen zu löschen oder an den Betroffenen herauszugeben.
3. Jede Genomanalyse muss zweckorientiert vorgenommen werden. Es ist diejenige genomanalytische Methode zu wählen, die keine oder die geringste Menge an Überschussinformationen bringt. Überschussinformationen sind unverzüglich zu vernichten.

4. Es ist zu prüfen, inwieweit genomanalytische Untersuchungsmethoden einer staatlichen Zulassung bedürfen. Für DNA-Sonden ist dies jedenfalls zu bejahen.

5. Die Genomanalyse im gerichtlichen Verfahren muss auf die reine Identitätsfeststellung beschränkt werden; es dürfen keine genomanalytischen Methoden angewandt werden, die Überschussinformationen zur Person liefern. Die Nutzung der Genomanalyse im Strafverfahren setzt eine normenklare gesetzliche Ermächtigung voraus. Präzise Regelungen müssen u. a. sicherstellen, dass genomanalytische Befunde einer strengen Zweckbindung unterworfen werden.

6. Im Arbeitsverhältnis sind die Anordnung von Genomanalysen oder die Verwendung ihrer Ergebnisse grundsätzlich zu verbieten. Ausnahmen bedürfen der gesetzlichen Regelung. Eine bloße Einwilligung des Arbeitnehmers ist wegen der faktischen Zwangssituation, der er im Arbeitsleben häufig unterliegt, nicht ausreichend.

7. Genomanalysen im Versicherungswesen sind grundsätzlich nicht erforderlich und mit dem Prinzip der Versicherungen, Risiken abzudecken und nicht auszuschließen, unvereinbar. Dies sollte durch eine Klarstellung im Versicherungsvertragsgesetz deutlich gemacht werden.

8. Im Rahmen der pränatalen Diagnostik dürfen nur Informationen über das Vorhandensein oder Fehlen von Erbanlagen erhoben werden, bei denen eine Schädigung heilbar ist oder die zu einer so schwer wiegenden Gesundheitsschädigung des Kindes führen würden, dass ein Schwangerschaftsabbruch straffrei bliebe.
   Reihenuntersuchungen an Neugeborenen dürfen sich nur auf solche Erbkrankheiten erstrecken, die bei frühzeitiger Erkennung eines genetischen Defekts geheilt oder zumindest spürbar therapeutisch begleitet werden können.
   Die Eltern müssen nach umfassender fachkundiger Beratung in voller Freiheit über die Anwendung genomanalytischer Methoden entscheiden können. Jegliche Beeinflussung, insbesondere jeder individuelle und gesellschaftliche Druck, muss vermieden werden.

Die informationelle Selbstbestimmung Dritter, zu der auch das Recht auf Nichtwissen gehört, muss berücksichtigt werden. Demnächst werden nicht nur – wie bisher – Gensequenzen aufgedeckt und verglichen, sondern auch die mit dem Genom verbundenen Wirkungszusammenhänge für die menschliche Gesundheit und für die Persönlichkeitsstruktur entschlüsselt werden können.

Anlage 16

Entschließung
der 60. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 12./13. Oktober 2000
Entschließung zur Novellierung des BDSG

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert an Bundestag und Bundesrat, das Gesetzgebungsverfahren eines novellierten Bundesdatenschutzgesetzes zügig und ohne Abstriche zum Abschluss zu bringen. Damit wird die längst überfällige Anpassung des deutschen Datenschutzrechts an die Vorgaben der EG-Richtlinie vorgenommen. Die Novelle enthält verschiedene innovative Ansätze, insbesondere das Gebot zur Datenvermeidung und Datensparsamkeit bei der Systemgestaltung (Systemdatenschutz – § 3 a E-BDSG) und die Einführung des Datenschutzaudits (§ 9 a), die von den Datenschutzbeauftragten schon seit langem befürwortet werden.

Sowohl der Systemdatenschutz als auch das Datenschutzaudit werden die Durchsetzung datenschutzfreundlicher Lösungen im Wettbewerb erleichtern und tragen auf diese Weise zur Selbstregulierung des Marktes bei. Das Datenschutzaudit fügt sich in die bewährten Strukturen des betrieblichen Datenschutzes ein und ermöglicht es den Unternehmen, datenschutzkonforme Angebote und Verhaltensweisen nachprüfbar zu dokumentieren und damit einen Wettbewerbsvorsprung zu gewinnen.

Die Konferenz fordert den Bundesrat auf, die Aufnahme des Datenschutzaudits in das BDSG nicht zu blockieren. Sie geht weiter davon aus, dass die angekündigte zweite Stufe der Novellierung des BDSG noch in dieser Legislaturperiode realisiert wird, und erklärt ihre Bereitschaft, hieran konstruktiv mitzuwirken.

Anlage 17

Entschließung der 60. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 12./13. Oktober 2000 Datensparsamkeit bei der Rundfunkfinanzierung

Die Finanzierung des öffentlich-rechtlichen Rundfunks ist derzeit Gegenstand öffentlicher Diskussion in der Politik und unter den Rundfunkanstalten selbst. Erörtert wird hierbei auch, ob die Erhebung von Rundfunkgebühren, die an das „Bereithalten eines Rundfunkempfangsgerätes" anknüpfen, im Hinblick auf veränderte Gerätetechniken und bestehende Mängel im Verfahren modifiziert oder durch andere Finanzierungsformen ersetzt bzw. ergänzt werden sollte.

Künftig wird kaum noch überschaubar sein, welche Geräte zum Rundfunkempfang geeignet sind. Über die eigentlichen Fernseh- und Rundfunkgeräte hinaus ist dies bereits heute beispielsweise mit Personalcomputern, die über einen Internetzugang verfügen, oder mit bestimmten Mobiltelefonen möglich. In naher Zukunft werden neue Technologien wie UMTS weitere Empfangsmöglichkeiten eröffnen. Sofern der Besitz derartiger multifunktionaler Geräte zum Kriterium für die Rundfunkgebührenpflicht gemacht wird, würde das zu einer erheblichen Ausweitung von Datenabgleichen führen. Schon das gegenwärtig praktizierte Gebühreneinzugsverfahren erfordert in großem Umfang die Verarbeitung personenbezogener Daten. Nach den Angaben der Rundfunkanstalten meldet ein signifikanter Teil der Rundfunkteilnehmerinnen und -teilnehmer trotz der Verpflichtung hierzu seine Geräte nicht an. Um möglichst alle Gebührenpflichtigen zu erfassen, nutzen die Rundfunkanstalten Daten aus dem Melderegister vom privaten Adresshandel und setzen vor Ort Rundfunkgebührenbeauftragte ein, die einzelne Haushalte aufsuchen. Damit wird in unverhältnismäßiger Weise in das Recht auf informationelle Selbstbestimmung vieler gesetzestreuer Bürgerinnen und Bürger eingegriffen.

Die Datenschutzbeauftragten des Bundes und der Länder fordern die Bundesländer auf, einer Neuordnung ein Modell zu Grunde zu legen, das sich stärker als das bestehende System der Rundfunkfinanzierung an den Prinzipien der Datenvermeidung, Datensparsamkeit und Dezentralisierung orientiert. Nach ihrer Überzeugung lässt sich die verfassungsrechtlich gebotene Staatsferne und Funktionsfähigkeit des öffentlich-rechtlichen Rundfunks auch mit anderen, das Recht auf informationelle Selbstbestimmung weniger stark einschränkenden Finanzierungsmodellen als dem derzeit praktizierten gewährleisten.

Anlage 18

Entschließung der 60. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 12./13. Oktober 2000 Vom Bürgerbüro zum Internet – Empfehlungen zum Datenschutz für eine serviceorientierte Verwaltung –

Bei der Modernisierung der öffentlichen Verwaltung soll insbesondere die Dienstleistungs- und Serviceorientierung verbessert werden. Dazu sollen unter anderem Dienstleistungen in multifunktionalen Servicecentern (Bürgeramt, Bürgerbüro, Bürgerladen, Kundencenter) gebündelt und die Möglichkeiten der modernen Informations- und Kommunikations-Technik intensiver genutzt werden (Information, Kommunikation und Transaktion über das Internet, Einrichtung von Call-Centern).

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder unterstützt alle Bemühungen, den Kontakt von Bürgerinnen und Bürgern mit den Verwaltungen schneller, einfacher, effektiver und insbesondere transparenter zu machen. Die Datenschutzbeauftragten erklären daher ihre ausdrückliche Bereitschaft, solche Entwicklungsprozesse konstruktiv zu begleiten.

Es ist aber unerlässlich, dass bei allen Lösungen eine sichere und vertrauliche Kommunikation zwischen Verwaltung und Bürgern sowie ein angemessener Schutz personenbezogener Daten gewährleistet wird. Nur Serviceangebote, die dem Recht auf informationelle Selbstbestimmung gerecht werden, nützen letztlich sowohl Bürgerinnen und Bürgern als auch der Verwaltung selbst.

Eine Arbeitsgruppe der Konferenz der Datenschutzbeauftragten des Bundes und der Länder erarbeitet deshalb Empfehlungen zum Datenschutz für eine serviceorientierte Verwaltung. Diese Empfehlungen sollen den Verwaltungen helfen, bei der Verbesserung ihrer Dienstleistungs- und Serviceorientierung den Forderungen nach Datenschutz und Datensicherheit gerecht zu werden. Diese Empfehlungen werden demnächst veröffentlicht und entsprechend der rechtlichen und technischen Entwicklung fortgeschrieben.

Anlage 19

Entschließung
der 60. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 12./13. Oktober 2000
Auftragsdatenverarbeitung durch das Bundeskriminalamt (Umlaufbeschluss)

Im Rahmen der Neukonzeption des polizeilichen Informationssystems INPOL ist geplant, neben bundesweit verfügbaren Verbunddaten auch Landesdatenbestände im Wege der Auftragsdatenverarbeitung logisch getrennt in der INPOL-Datenbank zu speichern. Zudem sollen aufgrund bilateraler Absprachen landesspezifische Informationen in bestimmtem Umfang gespeichert werden können und ebenso gegenseitige Zugriffe einzelner Länder auf die Datenbestände ermöglicht werden.

§ 2 Abs. 5 des Bundeskriminalamtgesetzes lässt grundsätzlich eine Unterstützung der Länder bei deren Datenverarbeitung auf Ersuchen, also in Einzelfällen, zu. Diese Vorschrift kann auch herangezogen werden, wenn aufgrund besonderer Dringlichkeit, wie gegenwärtig bei der Realisierung von INPOL-neu, eine zeitlich befristete Auftragsdatenverarbeitung von Landesdaten geplant ist. Hierzu sind Ende vergangenen Jahres entsprechende Beschlüsse des Arbeitskreises II und der Innenministerkonferenz gefasst worden.

Diese Entwicklung birgt aus der Sicht der Datenschutzbeauftragten die Gefahr, dass weitere Beschlüsse folgen werden, die die dauerhafte Speicherung von Landesdaten beim BKA begründen; bereits jetzt sind Tendenzen deutlich, die zentralisierte Speicherung der Daten auch zur Erleichterung der gegenseitigen Zugriffe auf Landesdaten zu nutzen.

Die Notwendigkeit der zentralen Datenspeicherung beim Bundeskriminalamt wird im Wesentlichen mit Kosten- und Zeitargumenten begründet. Diese sind jedoch aus datenschutzrechtlicher Sicht nicht geeignet, eine Erweiterung der zentralen Datenverarbeitung beim Bundeskriminalamt zu begründen. Die dauerhafte zentrale Datenhaltung beim BKA würde die informationelle Trennung von Landesdaten und Verbunddaten aufweichen; die in § 2 Abs. 1 BKA-Gesetz statuierte Schwelle, dass nur Daten über Straftaten von länderübergreifender, internationaler oder sonst erheblicher Bedeutung beim BKA verarbeitet werden dürfen, würde schleichend umgangen.

Eine dauerhafte zentrale Landesdatenhaltung beim Bundeskriminalamt beinhaltet eine neue, bei der augenblicklichen Rechtslage unakzeptable Qualität polizeilicher Datenverarbeitung.

Die Datenschutzbeauftragten des Bundes und der Länder fordern dazu auf, die für die Datenverarbeitung beim Bundeskriminalamt gesetzlich gezogenen Grenzen strikt zu beachten. Sie appellieren an die Innenminister/-senatoren von Bund und Ländern, an den bisherigen Beschlüssen festzuhalten und die Polizeien der Länder, wie ursprünglich geplant, aufzufordern, unverzüglich eigene Datenverarbeitungsverfahren zu entwickeln. Bis zur Realisierung dieser Verfahren könnte allenfalls eine übergangsweise Lösung als Auftragsdatenverarbeitung unter Wahrung datenschutzrechtlicher Anforderungen ermöglicht werden. Daneben steht das Angebot des Bundeskriminalamtes, kostenlos Software von INPOL-neu zur Verfügung zu stellen. Diese Lösung würde auch das vorgetragene Kostenargument entkräften.

Anlage 20

Entschließung
der 61. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8./9. März 2001
Äußerungsrecht der Datenschutzbeauftragten

Die Datenschutzbeauftragten des Bundes und der Länder sind verpflichtet, Einzelne – wie es die Rechtsprechung des Bundesverfassungsgerichts und die Richtlinie der Europäischen Gemeinschaft zum Datenschutz von 1995 vorsehen – vor rechtswidrigem Umgang mit ihren personenbezogenen Daten wirksam zu schützen. Die damit verbundenen Beratungs- und Kontrollaufgaben verleihen den Datenschutzbeauftragten ein öffentliches Wächteramt, das die Befugnis einschließt, Behördenverhalten auch im Detail und, soweit der Bedeutung der Sache angemessen, auch unter Bezeichnung der Amtsträgerinnen und Amtsträger öffentlich zu rügen.

Aus gegebenem Anlass wendet sich die Konferenz der Datenschutzbeauftragten des Bundes und der Länder energisch gegen Versuche im Land Sachsen, durch gesetzgeberische Maßnahmen dieses Recht zu beschneiden und die Arbeit des Sächsischen Datenschutzbeauftragten zu behindern.

Anlage 21

Entschließung
der 61. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8./9. März 2001
Informationszugangsgesetz

Die Konferenz verfolgt mit Interesse die Bestrebungen des Bundes, ein Informationszugangsgesetz zu schaffen und dem Bundesbeauftragten für den Datenschutz die Aufgaben zur Sicherung des Informationszugangs zu übertragen. Die Bundesregierung nimmt damit die Überlegungen auf, die in Artikel 255 EU-Vertrag und Artikel 42 EU-Grundrechte-Charta zum Ausdruck kommen. Die Konferenz betont, dass das Recht auf informationelle Selbstbestimmung der Einzelnen dem freien Zugang zu behördeninternen, amtlichen Informationen nicht entgegensteht, wenn die Privatsphäre der Betroffenen sowie Betriebsgeheimnisse gesetzlich geschützt bleiben. Die Berichte aus den Ländern Berlin, Brandenburg und Schleswig-Holstein zeigen, dass die datenschutzrechtlichen Gewährleistungen für die informationelle Selbstbestimmung sich mit dem erweiterten Zugangsrecht zu den Informationen öffentlicher Stellen unter der Voraussetzung entsprechender Schutzmechanismen vereinbaren lassen. Die Zusammenführung von Datenschutz- und Informationszugangskontrolle kann diese Gewährleistung institutionell absichern.

Anlage 22

Entschließung
der 61. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8./9. März 2001
Datenschutz bei der Bekämpfung von Datennetzkriminalität

Der Europarat entwirft gegenwärtig zusammen mit anderen Staaten, insbesondere den USA und Japan, eine Konvention über Datennetzkriminalität (Cyber-crime-Konvention), die über ihren Titel hinaus auch die automatisierte Speicherung von Daten im Zusammenhang mit anderen Straftaten regeln soll.[1)]

Die Datenschutzbeauftragten des Bundes und der Länder verkennen nicht, dass das Internet – ebenso wie andere technische Hilfsmittel – für Straftaten missbraucht wird. Sie teilen daher die Auffassung des Europarats, dass der Kriminalität auch im Internet wirksam begegnet werden muss. Allerdings ist zu beachten, dass sich die weit überwiegende Anzahl der Nutzenden an die gesetzlichen Vorgaben hält. Insoweit stellt sich die Frage der Verhältnismäßigkeit von Maßnahmen, die alle Nutzenden betreffen.

Die Datenschutzbeauftragten des Bundes und der Länder teilen die Auffassung der Europäischen Kommission, dass zur Schaffung einer sichereren Informationsgesellschaft in erster Linie die Sicherheit der Informationsinfrastruktur verbessert werden und anonyme wie pseudonyme Nutzungsmöglichkeiten erhalten bleiben müssen; über Fragen der Bekämpfung der Datennetzkriminalität sollte ein offener Diskussionsprozess unter Einbeziehung der Betreiberinnen und Betreiber, Bürgerrechtsorganisationen, Verbraucherverbände und Datenschutzbeauftragten geführt werden.[2)]

Die Konferenz regt eine entsprechende Debatte auch auf nationaler Ebene an und bittet die Bundesregierung, hierfür den erforderlichen Rahmen zu schaffen.

Die Konferenz der Datenschutzbeauftragten fordert die Bundesregierung auf, sich bei der Schaffung von nationalen und internationalen Regelungen zur Bekämpfung von Datennetzkriminalität dafür einzusetzen, dass

- Maßnahmen zur Identifikation von Internet-Nutzenden, zur Registrierung des Nutzungsverhaltens und Übermittlung der dabei gewonnenen Daten für Zwecke der Strafverfolgung erst dann erfolgen dürfen, wenn ein konkreter Verdacht besteht,
- der Datenschutz und das Fernmeldegeheimnis gewährleistet und Grundrechtseingriffe auf das unabdingbare Maß begrenzt werden,
- der Zugriff und die Nutzung personenbezogener Daten einer strikten und eindeutigen Zweckbindung unterworfen werden,
- Daten von Internet-Nutzenden nur in Länder übermittelt werden dürfen, in denen ein angemessenes Niveau des Datenschutzes, des Fernmeldegeheimnisses und der Informationsfreiheit gewährleistet ist sowie verfahrensmäßige Garantien bei entsprechenden Eingriffen bestehen.

Anlage 23

Entschließung der 61. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8./9. März 2001 Novellierung des G 10-Gesetzes

Die Datenschutzbeauftragten des Bundes und der Länder sehen mit großer Sorge, dass die Empfehlungen des Rechts- und des Innenausschusses des Bundesrates erhebliche Einschränkungen der Persönlichkeitsrechte der Bürgerinnen und Bürger zur Folge hätten, die über den Gesetzentwurf der Bundesregierung teilweise weit hinausgehen. Die Datenschutzbeauftragten wenden sich insbesondere entschieden dagegen, dass

- die Befugnisse der Nachrichtendienste zur Übermittlung und Verwendung von G 10-Daten an Strafverfolgungsbehörden gegenüber dem Gesetzentwurf noch deutlich erweitert werden sollen, indem Erkenntnisse der Nachrichtendienste u. a. zur Strafverfolgung weit über die Schwerkriminalität hinaus genutzt werden dürften,
- der Verzicht auf die Kennzeichnung von G 10-Daten sogar ohne vorherige Zustimmung der G 10-Kommission zulässig sein und
- die Schwelle dafür, endgültig von der Benachrichtigung Betroffener abzusehen, deutlich herabgesetzt werden soll.

Darüber hinaus kritisieren die Datenschutzbeauftragten des Bundes und der Länder, dass die Bundesregierung mit der Gesetzesnovelle über die Vorgaben des BVerfG hinaus weitere Änderungen im G 10-Bereich erreichen will, die neue grundrechtliche Beschränkungen vorsehen:

- Die Anforderungen an die halbjährlichen Berichte des zuständigen Bundesministers an die PKG müssen so gefasst werden, dass eine wirksame parlamentarische Kontrolle erreicht wird. Dies ist derzeit nicht gewährleistet. Deshalb muss über Anlass, Umfang, Dauer, Ergebnis und Kosten aller Maßnahmen nach dem G 10-Gesetz sowie über die Benachrichtigung der Beteiligten berichtet werden. Die gleichen Anforderungen müssen auch für die Berichte der PKG an den Bundestag gelten.

- Die Neuregelung, nach der auch außerhalb der Staatsschutzdelikte mutmaßliche Einzeltäter und lose Gruppierungen den Maßnahmen nach dem G 10-Gesetz unterliegen sollen, stellt das Trennungsgebot nach Art. 87 Abs. 1 Satz 2 GG weiter in Frage. Ermittlungen von der Eingriffsschwelle eines konkreten Anfangsverdachts zu lösen und nach nachrichtendienstlicher Art schon im Vorfeld zur Verdachtsgewinnung durchzuführen, weitet die Gefahr unverhältnismäßig aus, dass auch gegen Unbescholtene strafrechtlich ermittelt wird.

- Alle Neuregelungen wie z. B. zum Parteienverbotsverfahren, zur Verwendung von G 10-Erkenntnissen bei Gefahren für Leib oder Leben einer Person im Ausland und zu Spontanübermittlungen an den BND müssen befristet und einer effizienten Erfolgskontrolle unterzogen worden.

- Bei der internen Datenverarbeitung durch die Nachrichtendienste ist die Zweckbindung so zu formulieren, dass die erhobenen Daten nicht zur Erforschung und Verfolgung anderer als der in § 3 und § 5 G 10-E genannten Straftaten genutzt werden dürfen.

- Die vorgesehenen Ausnahmen von der vom BVerfG geforderten Kennzeichnungspflicht bei der Übermittlung von Daten, die aus G 10-Maßnahmen stammen, begegnen schwer wiegenden datenschutzrechtlichen Bedenken.

- Im Gesetzentwurf fehlt die Regelung, dass eine Weiterübermittlung an andere Stellen und Dritte nicht zulässig ist. Sie darf nur durch die erhebende Stelle erfolgen. Die Weitergabe von G 10-Daten an andere Dienststellen ist bei der übermittelnden Stelle stets zu dokumentieren und zu kennzeichnen.

- Eine dauerhafte Ausnahme von der Benachrichtigungspflicht ist abzulehnen. Sie würde für die Betroffenen zu einem Ausschluss des Rechtsweges führen.

  Dem BND wird nicht mehr nur die „strategische Überwachung“ des nicht leitungsgebundenen, sondern künftig des gesamten internationalen Telekommunikationsverkehrs ermöglicht. Dies setzt den Zugriff deutscher Stellen auf Telekommunikationssysteme in fremden Hoheitsbereichen voraus. Dabei muss sichergestellt werden, dass die Anforderungen des Völkerrechts eingehalten werden.

- Die Überwachung internationaler Telekommunikationsbeziehungen im Falle einer Gefahr für Leib oder Leben einer Person im Ausland (§ 8 G 10-E) ermöglicht sehr intensive Grundrechtseingriffe in großer Zahl und mit einer hohen Dichte, die höher sein kann als bei „strategischer Überwachung“ nach § 5 G 10-E. Dies setzt eine hohe Eingriffsschwelle und enge zeitliche Befristungen voraus, die der Entwurf nicht hinreichend vorsieht.

Anlage 24

Entschließung der 61. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8./9. März 2001 Novellierung des Melderechtsrahmengesetzes *)

Die Datenschutzbeauftragten des Bundes und der Länder begrüßen die Absicht der Bundesregierung, das Melderechtsrahmengesetz im Hinblick auf die neuen Informations- und Kommunikationstechnologien zu modernisieren und einzelne unnötige Meldepflichten abzuschaffen.

1. Allerdings sind aus dem vorliegenden Gesetzentwurf Tendenzen zu erkennen, dass durch den Zusammenschluss mehrerer Melderegister übergreifende Dateien entstehen können, die letztlich sogar zu einem zentralen Melderegister führen würden. Eine solche Entwicklung wäre aus datenschutzrechtlicher Sicht nicht hinnehmbar, weil damit das Recht auf informationelle Selbstbestimmung der Bürgerinnen und Bürger unverhältnismäßig eingeschränkt werden würde.

2. Bereits die bisherige Rechtslage, nach der nahezu jedermann eine einfache Melderegisterauskunft von der Meldebehörde erhalten kann, ist äußerst unbefriedigend. Dies wird dadurch verschärft, dass der Gesetzentwurf – wie in seiner Begründung ausdrücklich betont wird – nunmehr vorsieht, einfache Melderegisterauskünfte mit Hilfe des Internets durch jedermann auch elektronisch abrufen zu können. Um sich gegen eine unkontrollierte Weitergabe solcher über das Internet zum Abruf bereitgehaltener Daten schützen zu können und weil beim Internet-gestützten Abruf die gesetzlich vorgeschriebene Berücksichtigung der schutzwürdigen Belange Betroffener nicht möglich ist, sollte für die Bürgerin oder den Bürger in diesen Fällen ein ausdrückliches Einwilligungsrecht oder mindestens ein Widerspruchsrecht geschaffen werden. Es handelt sich hier um personenbezogene Daten, die auf der Grundlage einer gesetzlichen Auskunftspflicht erhoben wurden.

3. Auch für öffentliche Stellen sollte in das Gesetz eine Bestimmung aufgenommen werden, wonach bei elektronischen Abrufverfahren über das Internet zur Wahrung der schutzwürdigen Interessen der Betroffenen zumindest Verfahren der fortgeschrittenen elektronischen Signatur gemäß den Regelungen des Signaturgesetzes einzusetzen sind.

4. Nach geltendem Recht ist jede Melderegisterauskunft unzulässig, wenn eine Gefahr für Leben, Gesundheit, persönliche Freiheit oder ähnliche schutzwürdige Belange glaubhaft gemacht wird. Diese Regelung hat sich bewährt. Die Datenschutzbeauftragten treten angesichts des in diesen Fällen bestehenden hohen Schutzbedarfs dem Vorhaben entschieden entgegen, diese Regelung durch eine Risikoabwägung im Einzelfall aufzuweichen.

5. Bislang dürfen Meldebehörden an Parteien, Wählergruppen und andere Träger von Wahlvorschlägen Auskunft über Daten von Gruppen von Wahlberechtigten erteilen, sofern die Wahlberechtigten dieser Auskunftserteilung nicht widersprochen haben. Die Datenschutzbeauftragten bekräftigen ihre bereits in der Vergangenheit erhobene Forderung, gesetzlich zu regeln, dass eine Einwilligung der Betroffenen Voraussetzung für solche Datenweitergaben sein muss. Die bisherige Widerspruchslösung ist in weiten Kreisen der Bevölkerung unbekannt.

6. Außerdem fordern die Datenschutzbeauftragten, die Hotelmeldepflicht abzuschaffen, da die hiermit verbundene millionenfache Datenerhebung auf Vorrat unverhältnismäßig ist.

*) Bei Enthaltung Thüringens zu Ziffer 6.

Anlage 25

Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 12. März 2001 Anlasslose DNA-Analyse aller Männer verfassungswidrig

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist entschieden den Vorschlag zurück, den „genetischen Fingerabdruck" aller Männer zu erheben und rein vorsorglich zu speichern. Die Erhebung personenbezogener Daten ist auch im Rahmen der Strafverfolgung an rechtsstaatliche Grundsätze gebunden. Eine Datenerhebung auf Vorrat, die die Hälfte der Bevölkerung als potentielle Straftäter behandelt, ist verfassungsrechtlich unzulässig. Darüber hinaus erscheint der erwartete Abschreckungseffekt äußerst fragwürdig.

Anlage 26

Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 10. Mai 2001 Zum Entwurf der Telekommunikations-Überwachungsverordnung

Das Bundesministerium für Wirtschaft hat Ende Januar 2001 den Entwurf für eine Telekommunikations-Überwachungsverordnung (TKÜV) vorgelegt, der in Kürze dem Bundeskabinett zugeleitet wird. Der Entwurf basiert auf dem Telekommunikationsgesetz, das den Begriff der Telekommunikation weit fasst. Da er technikneutral formuliert ist, werden von den Überwachungsmaßnahmen nicht nur die Sprachtelefonie und der Telefaxverkehr, sondern auch alle anderen elektronischen Kommunikationsplattformen und damit insbesondere auch das Internet erfasst.

Sobald ein Internet-Provider einen E-Mail-Dienst anbietet, muss er technische Einrichtungen zur Umsetzung der Überwachungsmaßnahmen vorhalten, obwohl die Vermittlung des Zugangs zum Internet als anmelde- und zulassungsfreier Teledienst nicht zu den Telekommunikationsdiensten gehört. Diese Verpflichtung der Internet-Provider macht es technisch möglich, künftig den gesamten Internet-Verkehr, also auch das bloße „Surfen" zu überwachen. Dies ist aber nach deutschem Recht so nicht vorgesehen. Bedenklich ist in diesem Zusammenhang, dass das European Telecommunications Standards Institute (ETSI) gegenwärtig an einem technischen Standard arbeitet, der den Lauschangriff auf IP-Netze (Internet) und die Überwachung des gesamten Internet-Verkehrs europaweit vereinheitlichen soll.

Die Datenschutzbeauftragten des Bundes und der Länder wenden sich entschieden dagegen, eine technische Infrastruktur zu schaffen, die jederzeit eine umfassende Überwachung des Internet-Verkehrs möglich macht. Eine derartige Überwachung würde einen unverhältnismäßigen Eingriff in das Grundrecht auf Persönlichkeitsschutz darstellen und darüber hinaus den im Teledienstedatenschutzgesetz und im Mediendienstestaatsvertrag normierten Grundsätzen der Datenvermeidung und der Datensparsamkeit zuwiderlaufen.

Es muss sichergestellt werden, dass die zunehmende Nutzung von Telediensten zu Alltagsgeschäften auch künftig generell überwachungsfrei bleibt. Die bestehenden materiellen Befugnisse zur Telekommunikationsüberwachung im Strafprozessrecht, G 10-Gesetz und im Außenwirtschaftsgesetz bedürfen zudem insgesamt dringend einer kritischen Evaluation und Bereinigung, die die Bundesregierung durch eine wissenschaftliche Untersuchung der Effektivität bisheriger Überwachungsanordnungen bereits eingeleitet hat.

Die Datenschutzbeauftragten des Bundes und der Länder fordern ebenso eine Evaluation der Telekommunikations-Überwachungsverordnung, die im Lichte der Ergebnisse der Untersuchung über die Effektivität von Telekommunikations-Überwachungsmaßnahmen vorzunehmen ist.

Anlage 27

Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 24. April 2001 – Umlaufbeschluss – Veröffentlichung von Insolvenzinformationen im Internet

Dem Bundestag liegt ein Gesetzentwurf der Bundesregierung zur Änderung der Insolvenzordnung (BT-Drs. 14/5680) vor. Danach sollen gerichtliche Entscheidungen – vor allem in Verbraucherinsolvenzverfahren – künftig auch über das Internet veröffentlicht werden können, um Kosten für Bekanntmachungen in Printmedien zu sparen.

Die Datenschutzbeauftragten des Bundes und der Länder weisen darauf hin, dass Informationen aus Insolvenzverfahren, die in das Internet eingestellt sind, durch die Justiz nicht räumlich begrenzt werden können. Darüber hinaus ist deren Speicherung zeitlich nicht beherrschbar, und die Daten können vielfältig ausgewertet werden. Dies kann dazu führen, dass Dritte, etwa Auskunfteien oder Wirtschaftsinformationsdienste, die Daten auch nach Abschluss eines Insolvenzverfahrens speichern und diese über längere Zeit im Internet verfügbar sind. Die mit der Insolvenzordnung bezweckte Chance der Schuldner auf einen wirtschaftlichen Neubeginn würde letztlich auf Dauer beeinträchtigt, wenn sie zeitlebens weltweit abrufbar am Schulden-Pranger stehen.

Der Gesetzgeber muss das Risiko für die betroffenen Verbraucherinnen und Verbraucher, auf Grund einer möglichen Auswertung justizieller Veröffentlichungen im Internet dauerhaft Einbußen bei der Teilnahme am Wirtschaftsverkehr zu erleiden, sorgfältig mit dem Interesse an der beabsichtigten Senkung von Bekanntmachungskosten abwägen. Hierbei ist auch die gesetzgeberische Wertung zu berücksichtigen, dass Personen, für die ein Insolvenzverfahren eröffnet wurde, gerade nicht in das Schuldnerverzeichnis beim Amtsgericht aufgenommen werden. Das Internet bietet im Gegensatz zu einem gerichtlichen Verzeichnis letztlich keine Gewähr, die ordnungsgemäße Pflege und die Löschung personenbezogener Daten sicherzustellen, die für die Betroffenen von entscheidender wirtschaftlicher Bedeutung sein können. Die Datenschutzbeauftragten appellieren daher an den Gesetzgeber und an die Justizverwaltungen der Länder, die aufgezeigten Risiken insbesondere für Verbraucherinsolvenzen neu zu bewerten. Die vorgenannten Überlegungen sind im Gesetzgebungsverfahren bisher nicht in ausreichendem Maße berücksichtigt worden. Dabei sollten die Erwägungen des Bundesverfassungsgerichts im Beschluss vom 9. März 1988 – 1 BvL 49/86 – zu einem vergleichbaren Sachverhalt einbezogen werden.

Es erscheint zu einfach, die Informationen im Internet in gleicher Weise abzubilden wie in der Zeitung. Gerade das Internet bietet neue Chancen und Möglichkeiten, Informationen gezielt nur denen zugänglich zu machen, die es angeht. Gerade hier sind neue Wege möglich, die mit herkömmlichen Medien nicht erreicht werden konnten. Es gilt deshalb, insbesondere zu untersuchen, ob dem Prinzip der Publizität bei Veröffentlichungen im Internet nicht ein anderer Stellenwert zukommt und wie gravierende Nachteile für die Betroffenen vermieden werden können.

Bevor die geplante Änderung des § 9 InsO verabschiedet wird, ist daher vorrangig zu klären, wie das Recht auf informationelle Selbstbestimmung der Betroffenen besser geschützt werden kann.

Auch in anderen Bereichen wird das Internet bereits genutzt, erprobt oder die Nutzung erwogen, um justizielle Informationen bereitzustellen, z. B. die Handels-, Vereins-, Genossenschafts- und Partnerschaftsregister oder in Zwangsvollstreckungsverfahren. Inwieweit das Internet als Medium der im Ergebnis unbegrenzbaren Informationsverarbeitung datenschutzrechtlich angemessen ist und welches Datenprofil ins Internet eingestellt werden darf, muss differenziert in Übereinstimmung mit dem gesetzlich bezweckten Grad der Publizität der jeweiligen Daten entschieden werden. Jede gesetzgeberische Entscheidung für eine Veröffentlichung über das Internet sollte aber im Hinblick auf deren besondere Risiken regeln, dass Veröffentlichungen befristet sind und dass spezielle Vorkehrungen getroffen werden, um die Identität und die Authentizität zu sichern sowie eine automatische Übernahme der Daten zu verhindern (Kopierschutz).

Sollte sich der Gesetzgeber nach sorgfältiger Abwägung für eine Veröffentlichung über das Internet entscheiden, so muss er die Auswirkungen der Regelung auf Grund aussagefähiger Berichte der Landesjustizverwaltungen überprüfen. Gegenstand dieser Überprüfung muss auch sein, ob die eingetretene Kostensenkung tatsächlich, wie von der Bundesregierung erwartet, einer größeren Anzahl von Schuldnerinnen und Schuldnern den Weg zur Restschuldbefreiung eröffnet hat.

Anlage 28

Entschließung
der 47. Konferenz der Datenschutzbeauftragten des Bundes und der Länder
vom 9./10. März 1994
zu
Chipkarten im Gesundheitswesen (A)

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

Chipkarte als gesetzliche Krankenversicherungskarte

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

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

Chipkarte als freiwillige Gesundheitskarte

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

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

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

So stellt beispielsweise eine Kasse ihren Mitgliedern Bonuspunkte in Aussicht, wenn sie auf sog. Aktionstagen der Kasse Werte wie Blutzucker, Sauerstoffdynamik, Cholesterol sowie weitere spezielle medizinische Daten ohne ärztliche Konsultation messen und auf der Karte speichern und aktualisieren lassen. In Abhängigkeit von der Veränderung dieser Werte wird von der Kasse gegebenenfalls ein Arztbesuch empfohlen. Die Vergabe solcher Bonuspunkte widerspricht dem Prinzip der Freiwilligkeit bei der Erhebung der Daten für die Patienten-Chipkarte. Der Effekt wird noch verstärkt, indem die Kasse die „Möglichkeit einer Beitragsrückerstattung" in Aussicht stellt. Die Datenschutzbeauftragten des Bundes und der Länder sehen in dieser Art der Anwendung der Chipkarten-Technik das Risiko eines Mißbrauchs, solange der Inhalt und die Nutzung der Daten nicht mit den zuständigen Fachleuten – wie den Medizinern – und den Krankenkassen abgestimmt ist.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hält für den Einsatz und die Nutzung freiwilliger Patienten-Chipkarten zumindest – vorbehaltlich weiterer Punkte – die Gewährleistung folgender Voraussetzungen für erforderlich:

- Die Zuteilung einer Gesundheitskarte und die damit verbundene Speicherung von Gesundheitsdaten bedarf der schriftlichen Einwilligung des Betroffenen. Er ist vor der Erteilung der Einwilligung umfassend über Zweck, Inhalt und Verwendung der angebotenen Gesundheitskarte zu informieren.

- Die freiwillige Gesundheitskarte darf nicht – etwa durch Integration auf einem Chip – die Krankenversichertenkarte nach dem Sozialgesetzbuch verdrängen oder ersetzen.

- Die Karte ist technisch so zu gestalten, daß für die einzelnen Nutzungsarten nur die jeweils erforderlichen Daten zur Verfügung gestellt werden.

- Der Betroffene muß von Fall zu Fall frei und ohne Benachteiligung – z. B. gegenüber dem Arzt, der Krankenkasse oder der Versicherung – entscheiden können, die Gesundheitskarte zum Lesen der Gesundheitsdaten vorzulegen und ggf. den Zugriff auf bestimmte Daten zu beschränken. Er muß ferner frei entscheiden können, wer welche Daten in seinen Datenbestand übernehmen darf. Der Umfang der Daten, die gelesen oder übernommen werden dürfen, ist außerdem durch die gesetzliche Aufgabenstellung bzw. den Vertragszweck der Nutzer beschränkt.

- Der Kartenaussteller muß sicherstellen, daß der Betroffene jederzeit vom Inhalt der Gesundheitskarte unentgeltlich Kenntnis nehmen kann.

- Der Betroffene muß jederzeit Änderungen und Löschungen der gespeicherten Daten veranlassen können.

Die Datenschutzbeauftragten des Bundes und der Länder sprechen sich dafür aus, daß der Gesetzgeber dies durch bereichsspezifische Rechtsgrundlagen sicherstellt.

Entschließung
der 50. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 9./10. Oktober 1995
Datenschutzrechtliche Anforderungen an den Einsatz von Chipkarten im Gesundheitswesen (B)

Die Datenschutzbeauftragten des Bundes und der Länder haben auf ihrer 47. Konferenz am 9./10. März 1994 kritisch zum Einsatz von Chipkarten im Gesundheitswesen Stellung genommen. In dem Beschluß wird die Nutzung von Patientenkarten von mehreren Voraussetzungen zur Sicherung des Persönlichkeitsrechts abhängig gemacht.

Seitdem werden in mehreren Ländern Modellversuche und Pilotprojekte durchgeführt. Die Bandbreite reicht von allgemeinen Patientenkarten, die an möglichst viele Patienten/Versicherte ausgegeben werden, eine Vielzahl von Krankheitsdaten enthalten und von einem unbestimmten Kreis von Personen und Institutionen des Gesundheitswesens zu vielfältigen Zwecken verwendet werden können (z. B. Vital-Card der AOK Leipzig, Persönliche Patientenkarte Neuwied, BKK-Patientenkarte Berlin) bis zu krankheitsspezifischen Karten für bestimmte Patientengruppen mit reduziertem Datensatz und einer Definition der Verwendung (z. B. Dialyse-Card, Diab-Card, Krebsnachsorgekarte, Defi-Card).

Datenschutzrechtlich stellen sich vor allem folgende Probleme:

Die massenhafte Einführung der Karten erzeugt einen sozialen Druck auf die Betroffenen, sie mitzuführen und vorzuzeigen. Diesen Erwartungen wird sich der Betroffene vielfach nur unter Befremden des Arztes oder sogar der Gefahr, daß dieser die Behandlung ablehnt, verweigern können.

Die Verwendung von allgemeinen Patientenkarten bringt die Gefahr einer pauschalen Offenbarung von medizinischen Daten mit sich.

Dem Patienten wird die Last aufgebürdet, für die Sicherheit seiner medizinischen Daten selbst zu sorgen.

Die Datenschutzbeauftragten fordern alle für Kartenprojekte im Gesundheitswesen Verantwortlichen in Politik, Industrie, Ärzteschaft, Wissenschaft und in den Krankenversicherungen auf, das Recht auf informationelle Selbstbestimmung der betroffenen Patienten bzw. Versicherten zu gewährleisten. Die 50. Konferenz hält folgende Voraussetzungen für elementar:

1. Besondere Schutzwürdigkeit medizinischer Daten

   Medizinische Daten sind besonders schutzwürdig, unabhängig davon, welche Technologien eingesetzt werden, ob die Patientendaten beim Arzt gespeichert und versandt oder über ein Netz abgerufen werden oder ob der Patient die Daten auf einer Chipkarte bei sich hat. Es handelt sich oftmals um belastende, schicksalhafte Daten. Zudem geht es nicht nur um Daten des Patienten, sondern auch um fremde Einblicke in die ärztliche Tätigkeit.

2. Wirksame Entscheidung der Betroffenen über die Verwendung einer Karte

   Die freie Entscheidung der Betroffenen (Patienten/Versicherten), eine Chipkarte zu verwenden, muß gewährleistet sein. Dies umfaßt die Entscheidung,
   - ob Daten auf einer Chipkarte gespeichert werden,
   - welche der Gesundheitsdaten auf die Karte aufgenommen werden,
   - welche Daten auf der Karte wieder gelöscht werden,
   - ob die Karte bei einem Arztbesuch bzw. einem Apothekenbesuch vorgelegt wird und
   - welche Daten im Einzelfall zugänglich gemacht werden.

Ein Widerruf der Entscheidung muß ohne Nachteile für die Betroffenen möglich sein. Die gleiche Freiheit der Entscheidung für oder gegen die Verwendung der Chipkarte muß für Ärzte und Apotheker gewährleistet sein. Eine wirksame Entscheidung für oder gegen die Verwendung einer Chipkarte setzt eine schriftliche, objektive, vollständige und nachvollziehbare Information über Zweck, Art, Umfang und Beteiligte der Chipkarten-Kommunikation voraus. Das Gesamtkonzept des Chipkarteneinsatzes und der damit verbundenen Datenverarbeitung muß für die Betroffenen überschaubar sein.

Auf der Karte darf nicht der Datensatz der Krankenversichertenkarte nach § 291 Abs. 2 SGB V, insbesondere nicht die Krankenversicherung und die Krankenversicherungsnummer gespeichert werden, da andernfalls – zumal bei allgemeinen Patientenkarten mit hohem Verbreitungsgrad – die Krankenversichertenkarte verdrängt und deren Nutzungsbeschränkungen umgangen werden.

3. Freiheit der Entscheidung

Die uneingeschränkte Freiheit der Entscheidung der Betroffenen für oder gegen die Verwendung einer Chipkarte muß gewährleistet sein, denn der Einsatz von Chipkarten im Gesundheitswesen führt keineswegs zwangsläufig zu größerer Autonomie der Patienten. Neue Technologien können sich auch als Verführung erweisen, deren Preis erst langfristig erkennbar wird. Die individuelle Entscheidung des Bürgers über die Verarbeitung seiner Daten war und bleibt ein zentrales Recht gegenüber Eingriffen in seine Freiheitssphäre. Mit der Chipkarte können sich jedoch Situationen ergeben, in denen wirkliche Freiheit, tatsächliche Wahlmöglichkeit der Betroffenen nicht mehr gewährleistet sind und durch technische und organisatorische, rechtliche und soziale Rahmenbedingungen wiederhergestellt werden müssen.

Dem Staat kommt hier eine veränderte Rolle zu: Freiheitsrechte nicht einzuschränken, sondern sie zu sichern, wo Entwicklungen des Marktes und der Technologien sowie Gruppeninteressen die Entscheidungsfreiheit des Bürgers bedrohen. Die Technologie selbst kann für die Sicherung der Freiheitsrechte ein wertvolles Hilfsmittel sein. Darüber hinaus kommt der Informiertheit der Betroffenen ein zentraler Stellenwert zu. Ihre Kompetenz zur Entscheidung und zum praktischen Umgang mit der Karte muß gestärkt werden, damit sie auch langfristig die größtmöglichen Chancen haben, ihre Interessen durchzusetzen.

Mit der Ausstellung der Karte dürfen nur die Vorteile verknüpft werden, die sich unmittelbar aus den Nutzungspraktiken der Karte selbst ergeben. Die freie Entscheidung der Betroffenen, eine Karte zu nutzen oder dies abzulehnen, darf nicht durch einen Nutzungszwang oder eine Bevorzugung von Karten-Nutzern (z. B. durch Bonuspunkte) bzw. von Karten-Verweigerern eingeschränkt werden.

4. Keine Verschlechterung der Situation der Betroffenen

Durch die Einführung von Kommunikationssystemen mit Chipkarten dürfen die Betroffenen nicht schlechter gestellt werden als im konventionellen Verfahren. Die medizinische Versorgung, der Schutz der Gesundheitsdaten und die Mitentscheidungsrechte der Betroffenen müssen in Umfang und Qualität erhalten bleiben.

Das therapeutische Verhältnis Arzt/Patient darf sich durch den Einsatz von Chipkarten nicht verschlechtern. Freiheit und Vertrauen innerhalb des Arzt-Patienten-Verhältnisses sowie der Grundsatz der Abschottung der dem Arzt anvertrauten Informationen und der ärztlichen Erkenntnisse nach außen, gegen die Kenntnisnahme durch Dritte, müssen erhalten bleiben. Insbesondere muß der Gesetzgeber sicherstellen, daß die auf der beim Patienten befindlichen Chipkarte gespeicherten medizinischen Daten ebenso gegen Beschlagnahme und unbefugte Kenntnisnahme geschützt sind wie die beim Arzt gespeicherten Daten. Eine Kommunikation unter Vorlage der Karte mit Personen oder Stellen außerhalb des Arzt-Patienten-Verhältnisses, z. B. Arbeitgebern oder Versicherungen, muß vom Gesetzgeber untersagt werden.

Das sich im Gespräch entwickelnde Vertrauensverhältnis zwischen Arzt und Patient darf nicht durch eine chipkartenermittelte Kommunikation verdrängt werden. Verkürzte Darstellungen medizinischer Sachverhalte auf der Chipkarte – z. B. mit Hilfe von Schlüsselbegriffen – dürfen nicht zu einer Minderung der Qualität des therapeutischen Verhältnisses führen; das liegt auch im Interesse des Arztes. Der Patient muß auch weiterhin die Möglichkeit des individuellen Dialogs wählen können. Dies schließt insbesondere die Freiheit des Betroffenen ein, eine Chipkarte im Einzelfall nicht vorzulegen, auf der Chipkarte nur einen begrenzten Datensatz speichern zu lassen oder zu entscheiden, welchem Arzt welche Informationen oder Informationsbereiche offenbart werden. Der Patient darf durch die Ausgestaltung und den Verwendungszusammenhang der Chipkarte nicht zur pauschalen Offenbarung seiner Daten gezwungen sein. So sind Daten auf der Chipkarte so zu ordnen, daß z. B. beim Zahnarzt die gynäkologische Behandlung geheim bleiben kann.

Es darf keine „Einwilligung“ in Chipkarten und Chipkartensysteme mit verminderter Datensicherheit geben. Der Gesetzgeber muß die Patienten vor „billigen Gesundheitskarten“ ohne ausreichende Sicherung vor einer Nutzung durch Dritte schützen.

5. Sicherstellung der Integrität und Authentizität der Daten

Zur Sicherstellung der Vertraulichkeit, Integrität und Authentizität der Daten auf Chipkarten im Gesundheitswesen und zur Differenzierung der Zugriffsmöglichkeiten nach dem Grundsatz der Erforderlichkeit in unterschiedlichen Situationen sind kryptographische Verfahren sowie geeignete Betriebssysteme zur Abschottung unterschiedlicher Anwendungsbereiche nach dem Stand der Technik in Chipkarten und Schreib-/Lese-Terminals zu implementieren. Eine Protokollierung der Lösch- und Schreibvorgänge auf der Karte ist unverzichtbar.

Darüber hinaus ist für das infrastrukturelle Kartenumfeld (Herstellung, Verteilung, Personalisierung, ..., Rücknahme) sicherzustellen, daß ausreichende technische und organisatorische Maßnahmen Berücksichtigung finden. Für die zur Erstellung und Personalisierung von Gesundheits-Chipkarten dienenden Systeme sowie die informationstechnischen Systeme und Verfahren, mit denen Daten auf der Chipkarte gelesen, eingetragen, verändert, gelöscht oder verarbeitet werden, muß der gleiche hohe Sicherheitsstandard erreicht werden.

6. Keine neuen zentralen medizinischen Datensammlungen

Der Einsatz von Chipkarten im Gesundheitswesen darf nicht zur Entstehung neuer zentraler Dateien von Patientendaten bei Kassenärztlicher Vereinigung, Krankenkassen, Kartenherstellern oder sonstigen Stellen führen. Dies gilt auch für das Hinterlegen von Sicherungskopien der auf der Karte gespeicherten medizinischen Daten. Es steht in der freien Entscheidung der Betroffenen, ob sie dem Arzt ihres Vertrauens eine umfassende Pflege aller Chipkarten-Daten – einschließlich der Sicherungskopien – übertragen oder nicht.

7. Leserecht des Karteninhabers

Der Karteninhaber muß das Recht und die Möglichkeit haben, seine auf der Chipkarte gespeicherten Daten vollständig zu lesen.

8. Suche nach datenschutzfreundlichen Alternativen

Angesichts der aufgezeigten Gefährdungen der informationellen Selbstbestimmung im Gesundheitswesen muß die Suche nach datenschutzfreundlichen Alternativen zur Chipkarte fortgesetzt werden.

Vorstehende Kriterien sind der Maßstab für die datenschutzrechtliche Bewertung von Projekten für die Einführung von Chipkarten im Gesundheitswesen.

Die Datenschutzbeauftragten von Bund und Ländern fordern die Gesetzgeber auf, die dringend notwendigen Regelungen zur Sicherung der Rechte von Patienten und Ärzten zu schaffen. Ebenso ist durch die Gesetzgeber den Besonderheiten der Datenverarbeitung auf Chipkarten durch bereichsspezifische Regelungen Rechnung zu tragen.

Anlage 29

Entschließung der Europäischen Kommission vom 27. Juli 2000 zum Datentransfer in die USA

Grundsätze des „Sicheren Hafens" zum Datenschutz

Die umfassende Rechtsvorschrift der Europäischen Union zum Schutz personenbezogener Daten, die Datenschutzrichtlinie (nachstehend „die Richtlinie" genannt), trat am 25. Oktober 1998 in Kraft. Sie legt fest, dass personenbezogene Daten nur in Nicht-EU-Länder übermittelt werden können, die einen „angemessenen" Schutz der Privatsphäre gewährleisten. Die Vereinigten Staaten und die Europäische Union haben beide das Ziel, den Datenschutz für ihre Staatsbürger zu verstärken, wobei die Vereinigten Staaten jedoch einen anderen Ansatz verfolgen als die Europäische Gemeinschaft. Die USA verwenden einen sektoralen Ansatz, der auf einer Mischung von Rechtsvorschriften, Verordnungen und Selbstregulierung basiert. Angesichts dieser Unterschiede fühlen sich viele US-Organisationen verunsichert bezüglich der Auswirkung des seitens der EU geforderten „Angemessenheits-Standards" für die Übermittlung personenbezogener Daten aus der Europäischen Union in die Vereinigten Staaten. (...)

Die Entscheidung der einzelnen Organisationen, sich für den „sicheren Hafen" zu qualifizieren, ist vollkommen freiwillig, und die Organisationen können sich für das Konzept des „sicheren Hafens" auf verschiedene Arten qualifizieren. Organisationen, die sich dazu entschließen, den Grundsätzen beizutreten, müssen die Grundsätze einhalten, um die Vorteile des „sicheren Hafens" erhalten und behalten zu können, und sie müssen diese Absicht öffentlich bekannt machen. Wenn sich eine Organisation beispielsweise einem vom Privatsektor entwickelten Datenschutzprogramm anschließt, das sich an diese Grundsätze hält, qualifiziert sie sich für den „sicheren Hafen". Darüber hinaus können sich Organisationen auch qualifizieren, wenn sie eigene Maßnahmen zum Schutz personenbezogener Daten entwickeln, sofern diese den Grundsätzen entsprechen. Verstößt eine Organisation, deren Datenschutzmaßnahmen ganz oder teilweise auf Selbstregulierung beruhen, gegen diese Selbstregulierung, muss dieser Verstoß auch gemäß Abschnitt 5 des Federal Trade Commission Act zur Verhinderung unlauterer und irreführender Praktiken oder ähnlichen Rechtsvorschriften verfolgbar sein (der Anhang enthält die Liste der von der EU anerkannten staatlichen Einrichtungen in den Vereinigten Staaten). Zudem können Organisationen, die Gesetzen, Regulierungs-, Verwaltungs- oder anderen Rechtsvorschriften (oder Regeln) unterliegen, die wirksam personenbezogene Daten schützen, ebenfalls in den Genuss der Vorteile des „sicheren Hafens" gelangen. In allen Fällen gelten die Vorteile des Konzepts des „sicheren Hafens" ab dem Tag, an dem die Organisation, die sich für die Grundsätze des sicheren Hafens qualifizieren möchte, gegenüber dem Handelsministerium (oder einer von ihm benannten Stelle) erklärt, dass sie den Grundsätzen beitritt.

Die Geltung dieser Grundsätze kann begrenzt werden:

a) insoweit, als Erfordernissen der nationalen Sicherheit, des öffentlichen Interesses oder der Durchführung von Gesetzen Rechnung getragen werden muss,

b) durch Gesetzesrecht, staatliche Regulierungsvorschriften oder Fallrecht, die unvereinbare Verpflichtungen oder ausdrückliche Ermächtigungen schaffen, vorausgesetzt, die Organisation kann in Wahrnehmung dieser Ermächtigungen nachweisen, dass die Nichteinhaltung der Grundsätze sich auf das Ausmaß beschränkte, das die Einhaltung übergeordneter berechtigter Interessen aufgrund eben dieser Ermächtigung erforderte, oder

c) wenn die Richtlinie oder das nationale Recht Ausnahmeregelungen vorsieht, sofern diese Ausnahmeregelungen unter vergleichbaren Voraussetzungen getroffen werden. Im Hinblick auf das Ziel eines wirksameren Schutzes der Privatsphäre sollen die Organisationen die Grundsätze in vollem Umfang und in transparenter Weise anwenden, unter anderem indem sie angeben, in welchen Fällen Abweichungen von den Grundsätzen, die nach b) zulässig sind, bei ihren Datenschutzmaßnahmen regelmäßig Anwendung finden werden. Aus demselben Grund wird, wenn die Wahlmöglichkeit nach den Grundsätzen und/oder nach dem US-Recht besteht, von den Organisationen erwartet, dass sie sich, sofern möglich, für das höhere Schutzniveau entscheiden.

Organisationen können aus praktischen oder anderen Gründen die Grundsätze auf alle Datenverarbeitungsverfahren anwenden, die Verpflichtung zur Anwendung der Grundsätze entsteht jedoch erst mit dem Beitritt zum „sicheren Hafen". Bei manuell verarbeiteten Daten ist die Einhaltung der Grundsätze zur Qualifizierung für den „sicheren Hafen" nicht erforderlich. Organisationen, die vom „sicheren Hafen" profitieren wollen, um manuell verarbeitete Daten aus der EU zu erhalten, müssen die Grundsätze auf alle Daten anwenden, die nach ihrem Beitritt übermittelt werden. Organisationen können auch die in Artikel 26 der Richtlinie geforderten Garantien bieten, wenn sie in schriftlichen Vereinbarungen mit Stellen, die Daten aus der EU übermitteln, die Grundsätze für die materiellen Datenschutzvorschriften anwenden, sobald die weiteren Vorschriften für derartige Musterverträge von der Kommission und den Mitgliedstaaten genehmigt sind.

Für Fragen der Auslegung und der Einhaltung der Grundsätze des „sicheren Hafens" (einschließlich der FAQ) und der einschlägigen Geschäftsbedingungen für den Datenschutz einzelner dem „sicheren Hafen" angehöriger Organisationen gilt das US-Recht; es gilt nicht, wenn sich eine Organisation zur Zusammenarbeit mit europäischen Datenschutzbehörden verpflichtet hat. Sofern nicht anderweitig festgelegt, finden die Grundsätze des „sicheren Hafens" in sämtlichen Teilen, einschließlich der FAQ, in allen Fällen, in denen sie relevant sind, Anwendung.

Personenbezogene Daten sind in beliebiger Form aufgezeichnete Daten über eine identifizierte oder identifizierbare Person, die unter die Richtlinie fallen und aus der Europäischen Union an eine US-Organisation übermittelt werden.

Informationspflicht

Die Organisation muss Privatpersonen darüber informieren, zu welchem Zweck sie die Daten über sie erhebt und verwendet, wie sie die Organisation bei eventuellen Nachfragen oder Beschwerden kontaktieren können, an welche Kategorien von Dritten die Daten weitergegeben werden und welche Mittel und Wege sie den Privatpersonen zur Verfügung stellt, um die Verwendung und Weitergabe der Daten einzuschränken. Diese Angaben sind den Betroffenen unmissverständlich und deutlich erkennbar zu machen, wenn sie erstmalig gebeten werden, der Organisation personenbezogene Daten zu liefern, oder so bald wie möglich danach, auf jeden Fall aber bevor die Organisation die Daten zu anderen Zwecken verwendet als denen, für die sie von der übermittelnden Organisation ursprünglich erhoben oder verarbeitet wurden, oder bevor sie die Daten erstmalig an einen Dritten weitergibt.

Wahlmöglichkeit

Die Organisation muss Privatpersonen die Möglichkeit geben zu wählen („opt out"), ob ihre personenbezogenen Daten
a) an Dritte weitergegeben werden sollen oder
b) für einen Zweck verwendet werden sollen, der mit dem ursprünglichen oder dem nachträglich von der betreffenden Person genehmigten Erhebungszweck unvereinbar ist.

Der betroffenen Person muss die Ausübung ihres Wahlrechts durch leicht erkennbare und verständliche, leicht zugängliche und kostengünstige Verfahren ermöglicht werden.

Bei sensiblen Daten (wie z. B. Angaben über den Gesundheitszustand, über Rassen- oder ethnische Zugehörigkeit, über politische, religiöse oder philosophische Überzeugungen, über die Mitgliedschaft in einer Gewerkschaft oder über das Sexualleben) benötigen die Organisationen die ausdrückliche Zustimmung („opt in") der betroffenen Personen, wenn die Daten an Dritte weitergegeben oder für einen anderen als den ursprünglichen Erhebungszweck oder den Zweck verwendet werden sollen, dem die betroffene Person nachträglich durch Ausübung des Wahlrechts zugestimmt hat. In jedem Fall sollen die Organisationen alle ihnen von Dritten übermittelten Informationen als sensibel behandeln, die der Übermittler als sensibel einstuft und behandelt.

Weitergabe

Eine Organisation darf Daten nur dann an Dritte weitergeben, wenn sie die Grundsätze der Informationspflicht und der Wahlmöglichkeit anwendet. Möchte eine Organisation Daten an einen Dritten weitergeben, der in ihrem Auftrag und auf ihre Anweisung tätig ist, kann sie dies tun, sofern der Dritte entweder dem „sicheren Hafen" angehört oder der Richtlinie unterliegt, oder von

einer anderen Feststellung angemessenen Schutzniveaus erfasst wird oder sich schriftlich in einer Vereinbarung mit der Organisation dazu verpflichtet, zumindest das Maß an Schutz personenbezogener Daten zu gewährleisten, das in den entsprechenden Grundsätzen des „sicheren Hafens" gefordert wird. Eine Organisation, die diese Forderungen erfüllt, kann nicht haftbar gemacht werden (sofern sie nichts anderes vereinbart hat), wenn ein Dritter, an den sie Daten übermittelt hat, Beschränkungen der Verarbeitung dieser Daten missachtet oder sie in einer Weise verarbeitet, die seinen Erklärungen widerspricht, es sei denn, die Organisation wusste oder konnte wissen, dass der Dritte die Daten in unzulässiger Weise verarbeiten würde, und hat keine angemessenen Schritte unternommen, um das zu unterbinden.

Sicherheit

Organisationen, die personenbezogene Daten erstellen, verwalten, verwenden oder verbreiten, müssen angemessene Sicherheitsvorkehrungen treffen, um sie vor Verlust, Missbrauch und unbefugtem Zugriff, Weitergabe, Änderung und Zerstörung zu schützen.

Datenintegrität

In Übereinstimmung mit den Grundsätzen müssen personenbezogene Daten für den beabsichtigten Verwendungszweck erheblich sein. Eine Organisation darf personenbezogene Daten nicht in einer Weise verarbeiten, die mit dem ursprünglichen Erhebungszweck oder mit dem Zweck unvereinbar ist, dem der Betroffene nachträglich zugestimmt hat. In dem für diese Zwecke notwendigen Umfang muss die Organisation durch angemessene Maßnahmen gewährleisten, dass die Daten für den vorgesehenen Zweck hinreichend zuverlässig, genau, vollständig und aktuell sind.

Auskunftsrecht

Privatpersonen müssen Zugang zu den personenbezogenen Daten haben, die eine Organisation über sie besitzt, und sie müssen die Möglichkeit haben, diese zu korrigieren, zu ändern oder zu löschen, wenn sie falsch sind, es sei denn, die Belastung oder die Kosten für die Gewährung des Zugangs würden in dem jeweiligen Fall in einem Missverhältnis zu den Nachteilen für den Betroffenen stehen, oder Rechte anderer Personen als des Betroffenen würden verletzt.

Durchsetzung

Für einen effektiven Schutz der Privatsphäre müssen Mechanismen geschaffen werden, die die Einhaltung der Grundsätze des sicheren Hafens gewährleisten, Rechtsbehelfe für Betroffene vorsehen, bei deren Daten die Grundsätze nicht eingehalten wurden, sowie Sanktionen für die Organisation, die die Grundsätze nicht befolgt. Diese Mechanismen müssen mindestens Folgendes umfassen:

a) leicht zugängliche, erschwingliche und von unabhängigen Stellen durchgeführte Verfahren, nach denen Beschwerden, die betroffene Personen unter Berufung auf die Grundsätze erhoben haben, behandelt werden und nach denen Schadenersatz geleistet wird, wenn das geltende Recht oder private Regelungen dies vorsehen;

b) Kontrollmaßnahmen, um zu überprüfen, ob die Bescheinigungen und Behauptungen der Unternehmen über ihre Datenschutzmaßnahmen der Wahrheit entsprechen und ob diese Maßnahmen wie angegeben durchgeführt werden;

c) Verpflichtungen zur Lösung von Problemen, die daraus resultieren, dass Organisationen die Einhaltung der Grundsätze zwar erklärt, sich aber trotzdem nicht daran gehalten haben, sowie entsprechende Sanktionen für diese Organisationen. Die Sanktionen müssen hinreichend streng sein, um sicherzustellen, dass die Organisationen die Grundsätze einhalten.

Häufig gestellte Fragen

Sensible Daten

Muss eine Organisation für die Verarbeitung sensibler Daten stets die Zustimmung der betroffenen Person einholen?

Nein, die Zustimmung ist nicht erforderlich, wenn die Verarbeitung:

1. im lebenswichtigen Interesse der betroffenen Person oder einer anderen Person liegt;
2. zur Geltendmachung von Rechtsansprüchen oder für die Rechtsverteidigung notwendig ist;
3. für eine medizinische Behandlung oder Diagnose erforderlich ist;
4. durch eine politisch, philosophisch, religiös oder gewerkschaftlich ausgerichtete Stiftung, Vereinigung oder sonstige Körperschaft, die keinen Erwerbszweck verfolgt, im Rahmen rechtmäßiger Tätigkeiten und unter der Voraussetzung, dass sich die Verarbeitung ausschließlich auf die Mitglieder der Organisation oder Personen, die im Zusammenhang mit deren Tätigkeitszweck regelmäßige Kontakte mit ihr unterhalten, beziehen und die Daten nicht ohne Einwilligung der betroffenen Person an Dritte weitergegeben werden;
5. zur Erfüllung der arbeitsrechtlichen Pflichten der Organisation notwendig ist;
6. sich auf Daten bezieht, die von der Person nachweislich veröffentlicht worden sind (...).

Die Rolle der Datenschutzbehörden

Wie können Organisationen, die sich zur Zusammenarbeit mit Datenschutzbehörden in der Europäischen Union verpflichten, diese Verpflichtung eingehen und wie wird sie umgesetzt?

Nach den Grundsätzen des „sicheren Hafens" müssen in den USA ansässige Organisationen, die personenbezogene Daten aus der EU erhalten, mit geeigneten Mitteln dafür sorgen, dass diese Grundsätze gewahrt werden. Wie im Durchsetzungsgrundsatz beschrieben, gehören zu diesen Mitteln unter anderem

a) Rechtsbehelfe für Personen, über die die Organisationen Daten besitzen,

b) Verfahren, mit denen sie überprüfen, ob ihre Aussagen und Zusicherungen betreffend ihre Datenschutzpraxis den Tatsachen entsprechen,

c) die Pflicht der Organisationen, Abhilfe zu schaffen, falls es zu Problemen kommt, weil die Grundsätze des „sicheren Hafens" bei ihnen nicht gewahrt werden, sowie Sanktionen für Verstöße gegen diese Grundsätze. (...).

Anlassunabhängige Kontrolle

Nach welchen Verfahren prüfen Organisationen, dass der von ihnen zugesicherte Datenschutz tatsächlich besteht und dass ihre Datenschutzpolitik tatsächlich umgesetzt worden ist und den Grundsätzen des „sicheren Hafens" entspricht?

Die nach dem Durchsetzungsgrundsatz erforderliche anlassunabhängige Kontrolle kann eine Organisation entweder selbst durchführen oder von einer externen Stelle durchführen lassen.

Die Selbstkontrolle umfasst eine Erklärung darüber, dass die Organisation feststellt, dass ihre veröffentlichten Geschäftsbedingungen zum Datenschutz betreffend personenbezogene Daten aus der EU sachgerecht, umfassend, an auffälliger Stelle bekannt gemacht, vollständig umgesetzt und für jedermann zugänglich sind. Sie muss ferner feststellen, dass ihre Geschäftsbedingungen zum Datenschutz den Grundsätzen des „sicheren Hafens" entsprechen, dass betroffene Personen über interne Beschwerdeverfahren und Beschwerdeverfahren bei unabhängigen Schiedsstellen informiert werden, dass sie ihre Beschäftigten systematisch in der Praxis des Datenschutzes unterweist und Verstöße gegen die Datenschutzregeln sanktioniert und dass es bei ihr interne Verfahren gibt, nach denen die Einhaltung der Datenschutzvorschriften regelmäßig und objektiv überprüft wird. Die Selbstkontrolle sollte mindestens einmal jährlich stattfinden, eine Erklärung über ihre Durchführung ist von einem leitenden Angestellten oder einem bevollmächtigten Vertreter der Organisation zu unterzeichnen. Sie ist vorzulegen auf Verlangen von Einzelpersonen, im Rahmen einer Untersuchung oder bei einer Beschwerde wegen Nichteinhaltung von Datenschutzvorschriften.

Organisationen sollten die Umsetzung ihrer nach den Grundsätzen des „sicheren Hafens" konzipierten Geschäftsbedingungen zum Datenschutz dokumentieren und im Fall einer Untersuchung oder einer Beschwerde wegen Verletzung der Datenschutzvorschriften ihre Unterlagen der unabhängigen Schiedsstelle übergeben, die für die Prüfung von Beschwerden zuständig ist, oder der gesetzlichen Aufsichtsbehörde, die bei unlauterem und irreführendem Geschäftsgebaren entscheidungsbefugt ist.

Bei externer anlassunabhängiger Kontrolle ist nachzuweisen, dass die Geschäftsbedingungen zum Datenschutz der Organisation für den Schutz personenbezogener Daten aus der EU den Grundsätzen des „sicheren Hafens" entsprechen, dass diese Regeln eingehalten werden und dass betroffene Personen über die Beschwerdewege informiert werden, die ihnen offen stehen. Dazu können ohne Einschränkung Buchprüfungen und Zufallskontrollen durchgeführt sowie „Köder" und jede Art von technischen Hilfsmitteln eingesetzt werden. Die externe Kontrolle sollte mindestens einmal jährlich stattfinden, eine Erklärung über ihre Durchführung ist von einem leitenden Angestellten oder einem bevollmächtigten Vertreter der Organisation zu unterzeichnen. Sie ist vorzulegen auf Verlangen von Einzelpersonen, im Rahmen einer Untersuchung oder bei einer Beschwerde wegen Nichteinhaltung von Datenschutzvorschriften.

Auskunftsrecht

Gibt es ein absolutes Auskunftsrecht?

Nein. Nach den Grundsätzen des „sicheren Hafens" ist das Auskunftsrecht zwar grundlegend für den Schutz der Privatsphäre und ermöglicht es dem Einzelnen, die Richtigkeit von Daten zu überprüfen, die über ihn gespeichert sind. Die Pflicht einer Organisation, Personen Zugang zu den sie betreffenden personenbezogenen Daten zu gewähren, hat jedoch Grenzen, die sich nach dem Grundsatz der Verhältnismäßigkeit und der Zumutbarkeit bestimmen, und muss in bestimmten Fällen abgemildert werden. In der Begründung zu den Datenschutzleitlinien der OECD von 1980 wird schon klar gesagt, dass das Auskunftsrecht nicht absolut ist. Die Organisation ist nicht verpflichtet, so gründlich zu recherchieren, wie es etwa im Rahmen einer gerichtlichen Untersuchung erforderlich wäre, und muss auch nicht Zugang zu allen verschiedenen Speicherformen gewähren, in denen Daten über den Betroffenen gespeichert sind.

Verlangt jemand Zugang zu den über ihn gespeicherten Daten, sollte sich die angesprochene Organisation zunächst fragen, welche Gründe die Person dazu veranlassen. Ist beispielsweise eine Anfrage vage formuliert oder betrifft sie einen sehr weiten Bereich, so kann die Organisation mit der Person in Dialog treten, um die Gründe für die Anfrage besser zu verstehen und die gewünschten Daten zu ermitteln. Die Organisation kann sich danach erkundigen, mit welchen Teilen der Organisation die Person Kontakt hatte und/oder um welche Art von Daten (oder deren Nutzung) es geht. Wer Zugang zu den ihn betreffenden Daten verlangt, muss das allerdings nicht begründen.

Bei der Beurteilung der Zumutbarkeit sind die Kosten und die Arbeit zu berücksichtigen, die die Gewährung des Zugangs erfordert, sie sind aber nicht entscheidend. Bilden die Daten etwa die Grundlage für Entscheidungen, die für die Person von großer Tragweite sind (z. B. die Gewährung oder Versagung erheblicher Vorteile wie eine Versicherung, einen Kredit oder einen Arbeitsplatz), dann ist es der Organisation zumutbar, über diese Daten Auskunft zu geben, selbst wenn das einen relativ hohen Kosten- und Arbeitsaufwand erfordert.
Wenn die angeforderten Daten nicht sensibel sind oder nicht für Entscheidungen verwendet werden, die für die Person von großer Tragweite sind (z. B. nichtsensible Marketingdaten, nach denen entschieden wird, ob die Person einen Katalog zugesandt bekommt), aber leicht zugänglich sind und kostengünstig zur Verfügung gestellt werden können, muss die Organisation Zugang zu den Daten gewähren, die sie über die Person speichert. Diese Daten können von der Person selbst erhoben, im Verlauf eines Geschäftsvorgangs gesammelt oder von anderen erlangt worden sein.

Wegen seines grundlegenden Charakters sollen Organisationen das Auskunftsrecht nie ohne Not beschränken. Müssen z. B. bestimmte Daten geschützt werden und lassen sie sich leicht von den Daten trennen, zu denen Zugang verlangt wird, sollte die Organisation die geschützten Daten unkenntlich machen und die übrigen zur Verfügung stellen. Beschließt eine Organisation in einem bestimmten Fall, keinen Zugang zu gewähren, sollte sie der Person, die um Zugang ersucht hat, ihre Entscheidung begründen und ihr eine Kontaktstelle nennen, die weitere Auskünfte erteilt.

Kann eine Organisation, die personenbezogene Daten in ihren Datenbanken gespeichert hat, Personen lediglich mitteilen, welche Daten über sie gespeichert sind, oder muss sie ihnen Zugang zu den Datenbanken gewähren?

Es genügt eine Mitteilung über die gespeicherten Daten, der Person muss kein Zugang zu den Datenbanken der Organisation gewährt werden.

Muss eine Organisation ihre Datenbanken erforderlichenfalls umstrukturieren, um Auskunft gewähren zu können?

Die Organisation muss nur Auskunft über die von ihr gespeicherten personenbezogenen Daten geben. Das Auskunftsrecht begründet keine Pflicht, Dateien mit personenbezogenen Daten aufzubewahren, zu pflegen oder erforderlichenfalls umzustrukturieren.

In welchen weiteren Fällen kann der Zugang zu personenbezogenen Daten verwehrt werden?

Das ist nur in wenigen Fällen möglich und muss in jedem Fall konkret begründet werden. Eine Organisation kann den Zugang zu personenbezogenen Daten insoweit verwehren, als ihre Bekanntgabe wesentliche öffentliche Belange gefährden würde wie die nationale Sicherheit, die Verteidigung oder die öffentliche Sicherheit. Außerdem kann der Zugang verwehrt werden, wenn personenbezogene Daten ausschließlich für wissenschaftliche oder statistische Zwecke verarbeitet werden sollen. Weitere Gründe für die Verweigerung oder Beschränkung des Zugangs sind:

a) Beeinträchtigung von Rechtsvollzug oder Vollstreckung, einschließlich der Verhütung, Untersuchung oder Aufdeckung von Straftaten, oder des Rechts auf einen fairen Prozess;

b) Beeinträchtigung eines zivilrechtlichen Verfahrens, einschließlich der Abwehr, Untersuchung und Verfolgung von Rechtsansprüchen, oder des Rechts auf einen fairen Prozess;

c) die personenbezogenen Daten haben Bezüge zu anderen Personen, die nicht unkenntlich gemacht werden können;

d) gesetzliche oder andere berufliche Rechte und Pflichten werden verletzt;

e) es kommt zum Bruch der notwendigen Vertraulichkeit künftiger oder laufender Verhandlungen, z. B. über die Übernahme börsennotierter Organisationen;

f) die Sicherheitsprüfung von Arbeitnehmern oder ein Beschwerdeverfahren wird beeinträchtigt;

g) die Vertraulichkeit, die bei der Neubesetzung von Stellen oder bei der Umorganisation von Organisationen für eine gewisse Zeit gewahrt werden muss, wird gefährdet;

h) die Vertraulichkeit ist gefährdet, die bei der Überwachung, bei der Prüfung und bei sonstigen gesetzlich vorgeschriebenen Ordnungsfunktionen im Zusammenhang mit der ordnungsgemäßen Wirtschaftsführung erforderlich ist;

i) die Gewährung des Zugangs ist mit unverhältnismäßigen Kosten oder Arbeit verbunden, oder sie führt zur Beeinträchtigung der Rechte oder der berechtigten Interessen anderer.

Eine Organisation, die sich auf einen dieser Ausnahmefälle beruft, muss nachweisen, dass er tatsächlich vorliegt (was in der Regel der Fall ist). Wie bereits gesagt, sollen der anfragenden Person die Gründe für eine Zugangsverweigerung oder -beschränkung mitgeteilt werden, und es soll ihr eine Anlaufstelle für weitere Fragen genannt werden.

Kann eine Organisation eine Gebühr erheben, um die Kosten für die Auskunftserteilung zu decken?

Ja, die OECD-Leitlinien gestehen Organisationen das Recht zu, eine Gebühr zu erheben. Sie darf aber nicht überhöht sein. Organisationen dürfen also eine angemessene Gebühr in Rechnung stellen. Eine Gebühr kann sinnvoll sein, um wiederholten oder belästigenden Anfragen vorzubeugen (...).

Ist eine Organisation verpflichtet, Zugang zu personenbezogenen Daten zu gewähren, die sie aus öffentlichen Datenbeständen gewonnen hat?

Zunächst eine Begriffsklärung: Öffentliche Datenbestände sind Datenbestände, die von Ämtern aller Ebenen geführt werden und der Öffentlichkeit zur Einsichtnahme offen stehen. Das Auskunftsrecht gilt für solche Daten nur, wenn sie mit anderen personenbezogenen Daten kombiniert sind. Das Auskunftsrecht gilt nicht, wenn lediglich kleine Mengen von Daten aus nichtöffentlichen Qellen verwendet wurden, um die öffentlichen Daten zu indexieren oder zu ordnen. Die Bestimmungen der einschlägigen Rechtsvorschriften über die Einsichtnahme in Datenbestände sind einzuhalten. Sind Daten aus öffentlichen Beständen mit anderen als den genannten Datenmengen aus nichtöffentlichen Quellen kombiniert, muss die Organisation Zugang zu allen personenbezogenen Daten gewähren, sofern nicht einer der genannten Ausnahmefälle vorliegt.

Gilt das Auskunftsrecht für öffentlich verfügbare personenbezogene Daten?

Wie bei Daten, die aus öffentlichen Beständen gewonnen wurden, ist das Auskunftsrecht nicht auf Daten anzuwenden, die bereits der Öffentlichkeit zur Verfügung stehen, sofern sie mit nicht öffentlich verfügbaren Daten kombiniert sind.

Wie kann sich eine Organisation vor wiederholten oder belästigenden Auskunftsbegehren schützen?

Eine Organisation muss solchen Auskunftsbegehren nicht entsprechen. Deshalb kann sie für Auskünfte eine angemessene Gebühr erheben oder die Zahl der Anfragen einer Person innerhalb eines bestimmten Zeitraums angemessen begrenzen. Bei der Festlegung dieser Grenze sind Faktoren zu berücksichtigen wie die Häufigkeit, mit der Daten aktualisiert werden, der Zweck, für den die Daten verwendet werden, und die Art der Daten.

Wie kann sich eine Organisation vor Auskunftserschleichung schützen?

Eine Organisation muss nur Auskunft erteilen, wenn die anfragende Person ihre Identität zweifelsfrei nachweist.

Personaldaten

Gilt der Grundsatz des „sicheren Hafens", wenn personenbezogene Daten, die im Rahmen eines Beschäftigungsverhältnisses erhoben wurden, aus der EU in die Vereinigten Staaten übermittelt werden?

Ja. Übermittelt eine in der EU ansässige Organisation im Rahmen des Beschäftigungsverhältnisses erhobene personenbezogene Daten über ihre (früheren oder derzeitigen) Beschäftigten an eine Mutterorganisation, eine verbundene Organisation oder eine nicht verbundene Dienstleistungsorganisation in den USA, die sich auf die Grundsätze des „sicheren Hafens" verpflichtet hat, so fällt diese Übermittlung in den Anwendungsbereich der Grundsätze des „sicheren Hafens". In einem solchen Fall gelten für die Erhebung der Daten und ihre Verarbeitung vor der Übermittlung die Rechtsvorschriften des EU-Mitgliedstaats, aus dem sie stammen; sämtliche nach diesen Rechtsvorschriften geltenden Bedingungen und Beschränkungen der Übermittlung müssen beachtet werden. Die Grundsätze des „sicheren Hafens" gelten nur für die Übermittlung von und den Zugriff auf Daten über identifizierte Einzelpersonen. Statistische Informationen, die auf aggregierten, anonymisierten oder pseudonymisierten Beschäftigungsdaten beruhen, sind unter dem Datenschutzaspekt unbedenklich.

Datenverarbeitung im Auftrag (Artikel 17 der Datenschutzrichtlinie)

Wenn Daten aus der EU in den USA im Auftrag verarbeitet werden sollen, muss dafür ein Vertrag geschlossen werden unabhängig davon, ob der Auftragsverarbeiter der Vereinbarung zum sicheren Hafen beigetreten ist oder nicht?

Ja. Werden Daten lediglich zur Verarbeitung im Auftrag übermittelt, muss der in Europa für die Verarbeitung Verantwortliche darüber stets einen Vertrag schließen, gleich ob die Verarbeitung in oder außerhalb der EU stattfindet. Der Vertrag soll die Interessen des für die Verarbeitung Verantwortlichen schützen, also der natürlichen oder juristischen Person, die Mittel und Zweck der Verarbeitung bestimmt und die gegenüber der (den) betroffenen Person(en) voll verantwortlich bleibt. Im Vertrag wird festgehalten, welche Arbeiten genau auszuführen sind und mit welchen Vorkehrungen für die Sicherheit der Daten zu sorgen ist.

Eine amerikanische Organisation, die der Vereinbarung zum „sicheren Hafen“ beigetreten ist und personenbezogene Daten aus der EU zur Verarbeitung im Auftrag übermittelt bekommt, braucht bei diesen Daten die Grundsätze nicht anzuwenden, denn die Verantwortung dafür gegenüber der betroffenen Person liegt nach den geltenden EU-Rechtsvorschriften (die strenger sein können als die Grundsätze des „sicheren Hafens“) weiterhin bei dem für die Verarbeitung Verantwortlichen.

Da die dem „sicheren Hafen“ angehörenden Organisationen einen angemessenen Schutz gewähren, ist bei reinen Verarbeitungsverträgen mit dem „sicheren Hafen“ angehörenden Organisationen keine vorherige Genehmigung erforderlich (oder die Genehmigung wird von dem jeweiligen Mitgliedstaat automatisch erteilt), wie sie bei Verträgen mit Empfängern, die sich nicht auf die Grundsätze des sicheren Hafens verpflichtet haben bzw. nicht auf andere Weise einen angemessenen Schutz bieten, erforderlich wäre.

Arzneimittel und Medizinprodukte

Wenn in der EU erhobene personenbezogene Daten für Zwecke der pharmazeutischen Forschung oder für andere Zwecke in die USA übermittelt werden, gilt dann das Recht der Mitgliedstaaten oder gelten die Grundsätze des sicheren Hafens?

Das Recht der Mitgliedstaaten gilt für die Erhebung der personenbezogenen Daten und für ihre Verarbeitung vor der Übermittlung in die USA. Die Grundsätze des sicheren Hafens gelten, nachdem die Daten in die USA übermittelt worden sind. Daten, die für die pharmazeutische Forschung oder sonstige Zwecke benutzt werden, sollten gegebenenfalls anonymisiert werden.

In medizinischen und pharmazeutischen Studien gewonnene personenbezogene Daten sind oft sehr wertvoll für künftige Forschungsarbeiten. Darf eine dem „sicheren Hafen“ beigetretene US-Organisation, die personenbezogene Daten im Rahmen eines Forschungsvorhabens erhoben hat, diese Daten für ein anderes Forschungsvorhaben verwenden?

Ja, wenn das dem Betroffenen schon zu Anfang ordnungsgemäß mitgeteilt und wenn ihm eine Wahlmöglichkeit eingeräumt wurde. Eine Mitteilung muss Angaben über die künftige Verwendung der Daten enthalten wie Angaben über regelmäßige Folgeuntersuchungen, ähnliche Forschungsvorhaben, für die sie verwendet werden sollen, oder ihre kommerzielle Nutzung. Es versteht sich, dass dabei nicht jede künftige Verwendung der Daten angegeben werden kann. Die Verwendung für einen anderen Forschungszweck kann sich aus neuen Erkenntnissen über die ursprünglichen Daten, aus neuen medizinischen Entdeckungen und Fortschritten sowie aus Entwicklungen im Gesundheitswesen und in der Gesetzgebung ergeben. Gegebenenfalls ist in der Mitteilung darauf hinzuweisen, dass personenbezogene Daten für künftige medizinische und pharmazeutische Forschungsarbeiten verwendet werden können, die nicht vorauszusehen sind. Entspricht die neue Verwendung nicht dem allgemeinen Forschungszweck, für den die Daten ursprünglich erhoben wurden oder in den der Betroffene später eingewilligt hat, muss erneut seine Einwilligung eingeholt werden.

Was geschieht mit den Daten eines Teilnehmers, der sich auf eigenen Wunsch oder auf Wunsch der Trägerorganisation aus einem klinischen Versuch zurückzieht?

Ein Teilnehmer kann sich jederzeit aus einem klinischen Versuch zurückziehen oder dazu aufgefordert werden. Daten über ihn, die vor seinem Rückzug erhoben wurden, können jedoch weiterhin verarbeitet werden wie die übrigen im Rahmen des Versuchs erhobenen Daten, wenn er darauf hingewiesen wurde, als er seine Bereitschaft zur Teilnahme erklärte.

Daten aus öffentlichen Registern und öffentlich zugängliche Daten

Gelten die Grundsätze der Informationspflicht, der Wahlmöglichkeit und der Weiterübermittlung für Daten aus öffentlichen Registern bzw. öffentlich verfügbaren Daten?

Die Grundsätze der Informationspflicht, der Wahlmöglichkeit und der Weiterübermittlung sind nicht auf Daten in öffentlichen Registern anzuwenden, wenn diese nicht mit nichtöffentlichen Daten kombiniert sind und solange die von der zuständigen Behörde festgelegten Bedingungen für ihre Abfrage beachtet werden.

Im Allgemeinen gelten die Grundsätze der Informationspflicht, der Wahlmöglichkeit und der Weiterübermittlung auch nicht für öffentlich verfügbare Daten, es sei denn, der europäische Übermittler weist darauf hin, dass diese Daten Beschränkungen unterliegen, aufgrund deren die Organisation die genannten Grundsätze im Hinblick auf die von ihr geplante Verwendung anwenden muss.

Wird festgestellt, dass eine Organisation unter Missachtung der obigen Grundsätze absichtlich personenbezogene Daten offen gelegt hat, sodass diese Ausnahme von der Regel für die Organisation selbst oder aber für andere von Nutzen ist, verliert sie ihren Status als „sicherer Hafen“ und die damit verbundenen Vorteile.

(...)

Anlage 30

Orientierungshilfe des LfD vom 16. November 2000 „Zugriffsberechtigungen der kommunalen Behördenleitungen“

Infolge des zunehmenden Einsatzes moderner Informationstechnik bei den Kommunalverwaltungen stellt sich verstärkt die Frage, in welchem Umfang den Behördenleitungen Zugriffsberechtigungen bezüglich der behördlichen Datenbestände eingeräumt werden können. Sowohl bei den Kreisverwaltungen als auch auf der Ebene der Städte und Gemeinden ist diese Frage von besonderer Bedeutung. Denn direkte und unbeschränkte Einsichts- und Zugriffsrechte der Behördenleitungen haben datenschutzrechtlich relevante Auswirkungen: So können sie einerseits als Kontrollmöglichkeit gegenüber den eigenen Bediensteten eingesetzt werden; zugleich ist aber auch mit Hilfe umfassender Zugriffsberechtigungen ohne konkrete Rechtfertigung die Erstellung eines weitgehenden Datenprofils einzelner Bürger möglich, was aus der Sicht des Datenschutzes als unzulässig bewertet werden muss.

Der Landesbeauftragte für den Datenschutz Rheinland-Pfalz will mit den nachfolgenden Empfehlungen allen Kommunalverwaltungen des Landes zu diesem Thema eine praktikable Orientierungshilfe an die Hand geben.

Im Hinblick auf die Einräumung von Zugriffsberechtigungen zugunsten der bereichsübergreifend zuständigen Leiter kommunaler Gebietskörperschaften (z. B. Landräte, Oberbürgermeister, Bürgermeister) ist Folgendes zu beachten:

Keine fallunabhängige allgemeine Zugriffsberechtigung

Die Einräumung einer allgemeinen und unbeschränkten Zugriffsberechtigung zugunsten der Behördenleitung auf sämtliche in elektronischer Form vorgehaltenen Informationen der Behörde mit dem Ziel, in einem eventuellen künftigen Bedarfsfalle (beispielsweise Bürgersprechstunde) auf alle entsprechenden Dokumente zugreifen zu können, verstößt gegen § 13 Abs. 1 Landesdatenschutzgesetz (LDSG) und ist datenschutzrechtlich unzulässig.

Zugriffsberechtigungen i. d. R. nur zugunsten der funktional verantwortlichen Stelle

Die in § 13 Abs. 1 LDSG verankerten Grundsätze der Erforderlichkeit und Zweckgebundenheit der Datenverarbeitung, die in zahlreichen bereichsspezifischen datenschutzrechtlichen Regelungen ihre Wiederholung gefunden haben (z. B. §§ 67 ff. SGB X; 31 ff. MG), bedeuten, dass eine Verarbeitung der personenbezogenen Daten grundsätzlich nur bei der auch funktional dafür verantwortlichen Stelle der Behörde erfolgen soll. Zugriffsberechtigungen beschränken sich folglich regelmäßig auf einzelne Funktionsbereiche (Sozialamt, Meldeamt etc.) bzw. die insoweit fachlich zuständigen Mitarbeiter.

Aufsichts- und Kontrollbefugnisse sind keine Grundlage für generellen Zugriff

Die der Behördenleitung zustehenden Aufsichts- und Kontrollbefugnisse stellen keine ausreichende Grundlage für den generellen Zugriff auf die Mitarbeiter- und Bürgerdaten aus den verschiedenen Bereichen der Verwaltung im Sinne von § 13 Abs. 1 und 3 LDSG dar. Der jeweiligen Behördenleitung ist es folglich verwehrt, ihr Begehren auf Einräumung unbeschränkter Zugriffsbefugnisse mit ihren Zuständigkeiten im Rahmen der Dienstaufsicht zu rechtfertigen.

Direktzugriff der Behördenleitung ist mitbestimmungspflichtig

Ungeachtet der aus der Gesamtverantwortung eines Behördenleiters resultierenden Aufgaben und Befugnisse handelt es sich bei der Direktzugriffsberechtigung auf personenbezogene Daten um ein Verfahren, das geeignet ist, das Verhalten oder die Leistung der Beschäftigten zu überwachen. Einführung und Anwendung eines solchen Verfahrens sind gemäß § 80 Abs. 1 Nr. 3 Landespersonalvertretungsgesetz mitbestimmungspflichtig.

Einräumung einer Zugriffsbefugnis zugunsten der Behördenleitung ist im Einzelfall zulässig

Die Einräumung einer Zugriffsbefugnis auf die innerhalb der Behörde automatisiert gespeicherten personenbezogenen Daten zugunsten eines Landrates, (Ober-)Bürgermeisters oder sonstigen Behördenleiters darf, soweit diese an sich nicht funktional verantwortlich sind, nur im Einzelfall und beschränkt unter Berücksichtigung des Zwecks der Befugnis und der entsprechenden Kontroll- und Auswertungsmöglichkeiten erfolgen. Sie ist dann zulässig, wenn sie zur rechtmäßigen Erfüllung der in der Zuständigkeit der Behördenleitung liegenden Aufgaben erforderlich ist und keine Anhaltspunkte vorliegen, dass ihr überwiegende schutzwürdige Interessen der Betroffenen entgegenstehen. Der Umfang der im Einzelfall der Behördenleitung eingeräumten Zugriffsrechte ist zu dokumentieren; dessen Erforderlichkeit und Zweck sind darzulegen.

Kein allgemeiner Zugriff des Bürgermeisters auf Geschäftsbereiche der Beigeordneten

Auch dem Bürgermeister ist ein uneingeschränkter Zugriff auf alle in den Geschäftsbereich eines Beigeordneten fallenden Dokumente versagt. Dies folgt bereits aus § 50 Abs. 6 der Gemeindeordnung (GemO). Die aus § 55 Abs. 2 GemO hervorgehende eigene kommunalpolitische Verantwortung der Beigeordneten sowie der in § 50 Abs. 6 Satz 2 GemO verankerte Grundsatz des eingeschränkten Weisungsrechtes des Bürgermeisters bedeuten, dass die Einrichtung einer umfassenden Zugriffsmöglichkeit zugunsten der Bürgermeister auf alle Dokumente der Verwaltung schon kommunalverfassungsrechtlich unzulässig ist. Die Kontrolle der Beigeordneten bzw. deren Geschäftsbereiche in Routineangelegenheiten gehört nicht zu den Aufgaben eines Bürgermeisters; ihm steht lediglich in den Fällen des § 50 Abs. 6 Satz 2 GemO ein direktes Weisungsrecht gegenüber den Beigeordneten zu. Grundsätzlich obliegt es jedoch den Beigeordneten, ihren Geschäftsbereich selbständig und eigenverantwortlich zu leiten. Diesem Recht würde die Einräumung einer generellen Zugriffsberechtigung der Bürgermeister auf die jeweiligen Datenbestände widersprechen.

Anlage 31

LfD-Entwurf eines Musterantrags auf Einrichtung einer Übermittlungssperre

Tagesstempel

Antrag auf Einrichtung einer Übermittlungssperre

Familienname/Doktorgrad/Vornamen		Geburtsname	Geburtsdatum
Anschrift			
1	( ) An Adressbuchverlage dürfen mein Name und meine Anschrift nicht weitergelteitet werden (§ 35 Abs. 4 Meldegesetz)		
2	( ) Wenn ich ein Altersjubiläum (z. B. 80. Geburtstag) begehe, darf eine Mitteilung über dieses Jubiläum nicht weitergegeben werden (§ 35 Abs. 3 Meldegesetz)		
3	( ) Wenn wir ein Ehejubiläum (z. B. Goldene Hochzeit) begehen, darf eine Mitteilung über dieses Jubiläum nicht weitergegeben werden (§ 35 Abs. 3 Meldegesetz)		
4	( ) Ich beantrage eine Auskunftssperre hinsichtlich der Datenweitergabe an Parteien, Wählergruppen und andere Träger von Wahlvorschlägen (§ 35 Abs. 1 Meldegesetz)		
5	( ) Da ich nicht der Religionsgemeinschaft meines Ehegatten angehöre, beantrage ich gemäß § 32 Abs. 2 Meldegesetz, dass meine Daten nicht an die Religionsgemeinschaft meines Ehegatten übermittelt werden. Diese Erklärung gilt auch für meine minderjährigen Kinder: Familienname Vornamen Geburtsdatum		
6	( ) Ich beantrage eine Auskunftssperre, die sich auf eine erweiterte Melderegisterauskunft nach § 34 Abs. 2 Meldegesetz bezieht. Mein berechtigtes Interesse an dieser Auskunftssperre begründe ich unten.		
7	( ) Ich beantrage eine Auskunftssperre, die sich auf eine Gruppenauskunft nach § 34 Abs. 3 Meldegesetz bezieht. Mein berechtigtes Interesse an dieser Auskunftssperre begründe ich unten.		
8	( ) Ich beantrage eine Auskunftssperre wegen einer Gefahr für Leben, Gesundheit, persönliche Freiheit oder ähnlicher schutzwürdiger Belange (§ 34 Abs. 5 Meldegesetz). Die Anhaltspunkte für eine schwerwiegende Gefahr begründe ich unten.		
Begründung zu Nr. [6] Nr. [7] Nr. [8] (bitte ankreuzen)			
Amtliche Vermerke		_____ Datum, Unterschrift	

Anlage 32

Entschließung
des Sondertreffens der Datenschutzbeauftragten des Bundes und der Länder zur Terrorismusbekämpfung vom 1. Oktober 2001

Die Datenschutzbeauftragten des Bundes und der Länder unterstützen mit Nachdruck den Kampf des demokratischen Rechtsstaats gegen Terrorismus und organisierte Kriminalität. Sie sind heute zu einem Sondertreffen in Bonn zusammengekommen, um die aktuelle Situation nach den Terroranschlägen zu erörtern. Im politischen Raum werden zahlreiche Forderungen und Vorschläge zur Verbesserung der inneren Sicherheit diskutiert, die auch Auswirkungen auf den Datenschutz haben.

Die Datenschutzbeauftragten weisen darauf hin, dass die Sicherheits- und Strafverfolgungsbehörden zur Terrorismusbekämpfung bereits über weit reichende Befugnisse zur Datenverarbeitung verfügen. So ist. z. B. die Rasterfahndung zu Strafverfolgungszwecken generell möglich, in den meisten Ländern auch zur Gefahrenabwehr durch die Polizei. Das Bundesamt für die Anerkennung ausländischer Flüchtlinge kann bereits heute Erkenntnisse über terroristische Aktivitäten an den Verfassungsschutz und die Polizei übermitteln. Auch ist eine effektive Zusammenarbeit zwischen Polizei und Verfassungsschutz durch die geltende Rechtslage gewährleistet; Vollzugsdefizite sind kein Datenschutzproblem. Zu pauschalen Forderungen nach Einschränkung des Bürgerrechts auf Datenschutz besteht deshalb kein Anlass. Die Datenschutzbeauftragten betonen, dass Datenschutz nie Täterschutz war und auch in Zukunft nicht sein wird.

Die Datenschutzbeauftragten sind zu einem offenen und konstruktiven Dialog über etwa notwendige Anpassungen an die neue Bedrohungslage bereit. Sie erwarten, dass sie rechtzeitig beteiligt werden. Die Datenschutzbeauftragten warnen vor übereilten Maßnahmen, die keinen wirksamen Beitrag zur Terrorismusbekämpfung leisten, aber die Freiheitsrechte der Bürgerinnen und Bürger einschränken. Sie sprechen sich dafür aus, alle neu beschlossenen Eingriffsbefugnisse zu befristen und tief greifende Eingriffsbefugnisse, damit auch die laufende Rasterfahndung, einer ergebnisoffenen Erfolgskontrolle zu unterziehen.

Bei der künftigen Gesetzgebung sind die grundlegenden Rechtsstaatsprinzipien, das Grundrecht der freien Entfaltung der Persönlichkeit, das Verhältnismäßigkeitsprinzip, die Unschuldsvermutung und das Gebot besonderer gesetzlicher Verwendungsregeln für sensible Daten selbstverständlich zu beachten. Diese verfassungrechtlichen Garantien prägen den Rechtsstaat, den wir gemeinsam zu verteidigen haben.