Sächsischer Landtag
2. Wahlperiode

DRUCKSACHE 2/3300

Schutz des Persönlichkeitsrechts im öffentlichen Bereich

4. Tätigkeitsbericht

des

Sächsischen Datenschutzbeauftragten

Dem Sächsischen Landtag

vorgelegt zum 31. März 1996

gemäß § 27 des Sächsischen Datenschutzgesetzes

Eingegangen am: 11. Juni 1996 Ausgegeben am: 12. Juni 1996

Vorbemerkung zum Sprachgebrauch in diesem Bericht:
Logisch ist zu unterscheiden zwischen biologischem und grammatischem Geschlecht (sexus und genus). Es wäre ein Verlust, diese Unterscheidung aufzugeben; es wäre das Unterfangen, Sprache zu sexualisieren. Ich beteilige mich nicht an solchen Versuchen. Frauen bitte ich, sich auch von scheinbar männlichen, in Wahrheit nur generellen Be zeichnungen gemeint zu wissen: Bauherr, Lehrer, Beamter, Betroffener etc.

Beim Datenschutz wird der einzelne Mensch ganz groß geschrieben (im übertragenen Sinne). Dem soll die Rechtschreibung entsprechen: Mit dem Bundesverfassungsgericht - und gegen den Duden - schreibe ich den "Einzelnen" groß. Dies betont seine Individualität, nie den Individualismus.

Herausgeber: Der Sächsische Datenschutzbeauftragte
Dr. Thomas Giesen
Holländische Str. 2 Postfach 120905
01067 Dresden 01008 Dresden
Telefon: 0351/4935401
Fax : 0351/4935490

Vervielfältigung erwünscht.
Herstellung: OTTO Verlag und Druckerei pp.
Gedruckt auf chlorfreiem Papier.

Inhaltsverzeichnis

	Abkürzungsverzeichnis	13
1	**Datenschutz im Freistaat Sachsen**	24
1.1	Der Blick über den Tellerrand	24
1.2	Nochmals: Gegen den Zentralismus	24
1.3	Rückblick	27
2	**Parlament; Rechnungshof**	28
	Einschränkungen bei der Beantwortung einer Kleinen Anfrage	28
3	**Europäische Union / Europäische Gemeinschaft**	29
	EU-Datenschutzrichtlinie	29
4	Medien	31
5	**Inneres**	31
5.1	**Personalwesen**	31
5.1.1	Rechtliche Entwicklung des öffentlichen Dienstrechts	31
5.1.2	Führung und Verwaltung von Personalakten für Arbeiter und Angestellte im öffentlichen Dienst	32
5.1.3	Verwaltungsvorschrift des SMI zur Begründung und Beendigung des Beamtenverhältnisses: Frage nach anhängigen Strafverfahren	33
5.1.4	Belegverkehr im Bereich Besoldung zwischen Personalstellen und dem Landesamt für Finanzen (LfF	33
5.1.5	Nachweise für die Bezügeberechnung	34
5.1.6	Landeseinheitlicher Vordruck für den Bereich Reisekosten	34
5.1.7	Verwendung datenschutzgerechter Personalbögen	35
5.1.8	Frage nach nicht rechtswidriger Sterilisation und nicht rechtswidrigem Schwangerschaftsabbruch	35
5.1.9	Erklärung über ausgeübte Nebentätigkeiten	36
5.1.10	Einsichtnahme der Staatlichen Rechnungsprüfungsämter in Personalakten	37
5.1.11	Personalakteneinsicht durch einen beratenden Ausschuß des Kreistages	38
5.1.12	Einsicht in eine Personalakte für einen Privatdetektiv	39
5.1.13	Aushändigung der Personalakte nach Beendigung des Beschäftigungsverhältnisses	39

5.1.14	Regelbeurteilung von Angestellten	40
5.1.15	Inhalt von Dienstzeugnissen	40
5.1.16	Bekanntgabe der Prüfungsergebnisse der Laufbahnprüfung für den gehobenen Forstdienst	41
5.1.17	Behördliche Telefonverzeichnisse im Internet?.	41
5.1.18	Dezentralisierung des Personalwesens	42
5.1.19	Einführung automatisierter Verfahren der Arbeitszeiterfassung (elektronische Zeiterfassungsgeräte	42
5.1.20	Umsetzung der "Richtlinien zur Neuregelung der Eingruppierung der angestellten Lehrer	43
5.1.21	Umgang mit Beschäftigtendaten im SMWK	45
5.1.22	Behandlung von Personaldaten bei der Landesversicherungsanstalt (LVA) Sachsen	45
5.1.23	Kontrolle von Leistung und Verhalten kommunaler Vollzugsbediensteter – möglicherweise als Statistik?	46
5.1.24	Datenschutzrechtliche Kontrolle der Personalverwaltung einer Stadt	48
5.1.25	Unübersichtliche Personalaktenführung in einer Gemeindeverwaltung	49
5.1.26	Einbehalten privater Telefongebühren imGehaltsabzugsverfahren	50
5.1.27	Namentliche Nennung bei Verlust des Dienstausweises im Sächsischen Amtsblatt (oder in anderen amtlichen Bekanntmachungen)	51
5.2	**Personalvertretung**	51
5.2.1	Automatisierte Verarbeitung von Beschäftigtendaten beim Personalrat	51
5.2.2	Auswertung von Dienstgesprächen bei ISDN-Telefonanlagen	52
5.2.3	Inhalt von Wählerverzeichnissen bei Wahlen zum Personalrat	53
5.2.4	Aushändigung des Stellenplans oder Stellenbesetzungsplans an den Personalrat	53
5.2.5.	Diskrepanz zwischen § 77 Nr.4 und § 80 Abs. 3 Nr. 16 SächsPersVG	54
5.2.6	Beteiligung des Personalrats und der Frauenbeauftragten bei Beurlaubung aus persönlichen Gründen	55
5.3	**Einwohnermeldewesen; Paß- und Personalausweiswesen**	55
5.3.1	Rechtliche Entwicklung	55
5.3.1.1	Entwurf eines Gesetzes zur Änderung des Sächsischen Meldegesetzes	55
5.3.1.2	Entwurf einer Sächsischen Meldedatenübermittlungsverordnung	56
5.3.2	Meldedatenübermittlungen und Melderegisterauskünfte	57
5.3.2.1	Unzulässige Meldedatenübermittlungen an Mitgliedsgemeinden	57

5.3.2.2	Übermittlung von Meldedaten an die öffentlich-rechtlichen Rundfunkanstalten und an die GEZ	57
5.3.2.3	Adreßbuchdaten auf CD-ROM	58
5.3.3	Verbot der Datenverarbeitung bei "Beeinträchtigung schutzwürdiger Interessen	59
5.3.4	Teilnahme in Deutschland lebender türkischer Staatsbürger an den Wahlen in ihrem Heimatland	59
5.3.5	Aufenthaltsfeststellungsverfahren nach § 24 b WPflG	60
5.3.6	Abgrenzung der "automatisierten Führung" des Melderegisters gegenüber den "melderechtlichen Hilfstätigkeiten	61
5.3.7	Datenerhebung durch Vermieter über die bei ihnen gemeldeten Mieter	62
5.3.8	Beauftragung eines privaten Zustell- oder Kurierdienstes mit der Weiterleitung der Anträge auf Ausstellung eines Passes oder Personalausweises an die Bundesdruckerei	62
5.4	**Wahlrecht; Personenstandswesen**	
5.4.1	Hinterbliebenensuche des Volksbundes Deutsche Kriegsgräberfürsorge e. V. (Volksbund	63
5.4.2	Wahrung des Adoptionsgeheimnisses: Melderechtliche Behandlung eines zur Adoption freigegebenen Kindes nach der Geburt	64
5.5	**Kommunale Selbstverwaltung**	
5.5.1	Veröffentlichung personenbezogener Sachverhalte aus nichtöffentlicher Gemeinderatssitzung	64
5.5.2	Video- und Tonbandaufnahmen in öffentlichen Gemeinderatssitzungen durch die Presse	65
5.5.3	Einsetzung einer Untersuchungskommission durch den Oberbürgermeister der Stadt Leipzig	66
5.5.4	Verbandstätigkeit eines Datenverarbeitungs-Zweckverbandes	68
5.5.5	Übertragung der Vollstreckungsaufgaben auf Private	69
5.5.6	Fernmeldeerschließung durch die Deutsche Telekom AG (Telekom	69
5.5.7	Ausstellung eines "Familienpasses" zur Erlangung von Vergünstigungen	71
5.5.8	Inhalt des Auskunftsanspruchs	72
5.5.9	Personenbezogene Daten in einer Ortschronik	73
5.6	**Baurecht; Wohnungswesen**	73
	Anbieterdatei im Hochbauamt	73

5.7	**Statistikwesen**	74
5.7.1	VO über den Einsatz von Datenverarbeitungsanlagen in kommunalen Statistikstellen	74
5.7.2	VO über die Frauenförderungs-Statistik	75
5.7.3	Grundsatzfrage: Privatisierung der Durchführung amtlicher Statistiken, insbesondere kommunaler Statistiken	76
5.7.4	Grundsatzfrage: Von öffentlichen Stellen durchgeführte Meinungs-umfragen als amtliche Statistik	81
5.7.5	Gebäude- und Wohnungszählung 1995: Zwischenbilanz	82
5.7.6	Befragung von Jugendlichen zu einem Straßenbauvorhaben	83
5.7.7	Verkehrszählung mit und ohne Videoaufzeichnungen	85
5.7.8	Kommunale Gewerbestatistik	86
5.8	**Archivwesen**	87
5.8.1	DDR-Unterlagen über kirchliche Funktionsträger	87
5.8.2	Archivbenutzung zum Zwecke der Erbenermittlung	90
5.8.3	Einstellung freier Mitarbeiter im Stadtarchiv	91
5.9	**Polizei**	92
5.9.1	Kontrollbesuche bei der Polizei	92
5.9.2	Rücknahme sächsischer Daten aus Beständen des Bundeskriminalamts (BKA	93
5.9.3	Aufbewahrung von Blutentnahmeprotokollen bei den Untersuchungsstellen	93
5.9.4	Geplante Dienstanweisung für verdeckte Ermittler bei Gefahrenabwehr	94
5.9.5	Speicherung des Merkmals "homosexuell" bei der Datenerfassung durch Polizeibehörden	95
5.9.6	Aufzeichnung eingehender Anrufe	95
5.9.7	Speicherung von Wiederholungsfällen bei Verstößen im ruhenden Verkehr	96
5.9.8	Bildaufzeichnungen bei Demonstrationen	96
5.9.9	Polizeiliche Einsichtnahme in das Personalausweis- und Passregister	97
5.9.10	Lichtbilder bei Verkehrsüberwachung	98
5.9.11	Datenübermittlung der Polizei an Fußballvereine zur Erteilung von Stadionverboten	98
5.9.12	Praktikanten bei der Polizei	99
5.9.13	Eingaben	99

5.10	**Verfassungsschutz**	100
5.10.1	Internes Informationsystem	100
5.10.2	Eingaben	100
5.11	Landessystemkonzept / Landesnetz	101
5.12	**Sonstiges**	102
	Ehrung von Alters- und Ehejubilaren durch den Bundespräsidenten	102
6	**Finanzen**	102
6.1	Automatisierte Datenübermittlung der Vermessungsämter an die Finanzbehörden	102
6.2	Beauftragung des e-Postdienstes der Deutschen Post AG mit dem Druck, der Kuvertierung und dem Versand von Grund- und Gewerbesteuerbescheiden	103
7	**Kultus**	104
7.1	Schule	104
	Entwurf der "Verordnung des SMK über Förderschulen im Freistaat Sachsen (Schulordnung Förderschulen – SOFS	104
7.2	Datenschutz im kirchlichen Bereich	105
	Benutzung kirchlicher Archive	105
8	**Justiz**	
8.1	Verwaltungsvorschrift über das Justizpressewesen	105
8.2	**Justizvollzug**	109
8.2.1	Kontrolle der Justizvollzugsanstalt Waldheim	109
8.2.2	Lichtbilder von Gefangenen	110
8.2.3	Briefkontrolle von Behördenpost	111
8.2.4	Informations- und Verwaltungssystem (IVS	112
8.2.5	Kontrolle der Post des Sächsischen Datenschutzbeauftragten an Gefangene	112
8.3	**Staatsanwaltschaften**	113
8.3.1	Verwaltungsvorschrift zur Zusammenarbeit von Staatsanwaltschaft und Polizeivollzugsdienst bei der Bekämpfung der Organisierten Kriminalität	113
8.3.2	Geplantes staatsanwaltschaftliches Registrierungs- und Informations-system (STARIS) in Sachsen	114

8.3.3	Mitteilung der Staatsanwaltschaften und Gerichte über den Ausgang von Ermittlungsverfahren	115
8.3.4	Einstellung des Ermittlungsverfahrens wegen Schuldunfähigkeit	116
8.3.5	Staatsanwaltschaft ersucht Gesundheitsamt um Patientendaten	116
8.3.6	Einsicht in Ermittlungsakten der Staatsanwaltschaft durch Dritte	117
8.4	**Sozialer Dienst der Justiz**	118
	Bewährungshilfe (EDV-System RESO	118
8.5	**Rechtsanwaltskammer; Notarkammer**	120
8.5.1	Offenbarung von Mandantendaten gegenüber der Sächsischen Rechtsanwaltskammer im Rahmen der Erteilung der Befugnis zum Führen einer Fachanwaltsbezeichnung	120
8.5.2	Entwurf einer Verwaltungsvorschrift über gerichtliche Mitteilungen von Klagen, Vollstreckungsmaßnahmen u. ä. an öffentliche Stellen	121
9	**Wirtschaft und Arbeit**	121
9.1	**Straßenverkehrswesen**	121
9.1.1	Änderung von § 52 Abs. 2 BZRG	121
9.1.2	Vorlage des Gutachtens einer medizinisch-psychologischen Untersuchungsstelle für die Verlängerung der Fahrerlaubnis zur Fahrgastbeförderung ab dem fünfzigsten Lebensjahr	122
9.1.3	Kontrolle einer Führerscheinstelle / Kfz-Zulassungsstelle	123
9.1.4	Inhalt einer Fahrtenbuchauflage	123
9.1.5	Weitergabe von Beschäftigtendaten durch eine Polizeidienststelle an eine Fahrerlaubnisbehörde	124
9.1.6	Welche Daten dürfen Fahrerlaubnisbehörden im Rahmen der Eignungsprüfung bei Neuerteilung einer Fahrerlaubnis verarbeiten	124
9.2	**Gewerberecht**	125
9.2.1	Rechtliche Entwicklung	125
9.2.1.1	Gesetz zur Änderung der Gewerbeordnung und sonstiger gewerberechtlicher Vorschriften	125
9.2.1.2	Verwaltungsvorschrift zur Durchführung der §§ 14, 15 und 55 c GewO	125
9.2.2	Einholung unbeschränkter Auskünfte aus dem Bundeszentralregister über Beschäftigte von Bewachungsunternehmen	126
9.2.3	Gewerberegisterauskunft über ausländische Gewerbetreibende	127
9.2.4	Zum Begriff "Glaubhaftmachen	127

9.3	**Handwerkskammern; Industrie- und Handelskammern**	127
9.3.1	Einrichtung von "Warndateien" mit Angaben über säumige Schuldnerfirmen	127
9.3.2	Lebenslauferstellung bei Fortbildungsveranstaltungen	128
9.3.3	Bekanntgabe von Prüfungsergebnissen durch die Kammern an den Ausbildungsbetrieb	128
9.3.4	Verpflichtung zur Vorlage des Arbeitsvertrages zwischen Gewerbetreibendem und Betriebsleiter bei der Handwerkskammer	129
9.4	**Offene Vermögensfragen**	130
9.4.1	Bekanntgabe des Investitionsvorrangbescheides	130
9.4.2	Anspruch auf Auskunft über Verträge, mit denen Kommunen Immo - bilien aus Volkseigentum veräußert haben	132
9.4.3	Datenübermittlung von den Vermögensämtern an Notare für das Vermittlungsver- fahren nach dem Sachenrechtsbereinigungsgesetz	134
9.5	**Sonstiges**	136
	Planfeststellung: Auslegung von Planungsunterlagen	136
10	**Soziales und Gesundheit**	137
10.1	**Gesundheitswesen**	137
10.1.1	Sächsisches Ausführungsgesetz zum Krebsregistergesetz des Bundes	137
10.1.2	Meldeordnung der Sächsischen Landesapothekerkammer	138
10.1.3	Datenschutz bei der Sächsischen Landesärztekammer	140
10.1.4	Einführung eines automatisierten Datenübermittlungsverfahrens zwischen der Sächsischen Ärzteversorgung und dem Landesamt für Finanzen	141
10.1.5	Dienstanweisung für den Datenschutz in einem Krankenhaus	142
10.1.6	Öffnen und Weiterleiten von Post in einem Krankenhaus	145
10.1.7	Einsicht des Patienten in seine Krankenakte	146
10.1.8	Offene Lagerung von Patientenunterlagen	148
10.1.9	Einsichtnahme in Todesbescheinigungen durch Doktoranden	148
10.1.10	Datenschutz im Maßregelvollzug	149
10.1.11	Ärztliche Bescheinigung zur Haft- und Gewahrsamsfähigkeit	151
10.2	**Sozialwesen**	152
10.2.1	Verwaltungsvorschrift zur Durchführung des Wohngeldverfahrens	152

10.2.2	Führung eines Dateien- und Geräteverzeichnisses durch Sozialleistungsträger	153
10.2.3	Übermittlung von Sozialdaten aufgrund einer landesrechtlichen Regelung	154
10.2.4	Weitergabe des Prüfberichts durch das Landesprüfungsamt für Sozialversicherung	156
10.2.5	Wie wird der überwiegende Teil des gesamten Datenbestandes bei der Auftragsdatenverarbeitung von Sozialdaten bestimmt	158
10.2.6	Datenverarbeitung im Auftrag zur Wohngeldberechnung	160
10.2.7	Vorlage des Steuerbescheides bei Beantragung von Wohngeld	162
10.2.8	Antrag auf Eingliederungshilfe für ein körperbehindertes Kind	163
10.2.9	Antrag auf Eingliederungshilfe für seelisch behinderte Kinder und Jugendliche	164
10.2.10	Bescheinigung für Zwecke der Arbeitsbefreiung bei Erkrankung von Kindern	166
10.2.11	Angabe ausländischen Einkommens und Vermögens bei Anträgen auf Sozialhilfe	167
10.2.12	Befreiung von der Rundfunkgebührenpflicht	167
10.2.13	Durchführung des automatisierten BAföG-Hauptverfahrens	170
10.3	**Lebensmittelüberwachung und Veterinärwesen**	171
10.3.1	Lebensmittelüberwachung: Selbstvermarkter-Statistik des SMS	171
10.3.2	Datenverarbeitung im Bereich der Sächsischen Landestierärztekammer	172
10.4	**Rehabilitierungsgesetze**	174
10.4.1	Übermittlung von Antragsteller-Daten durch nach § 25 StrRehaG zuständige Stellen an Rehabilitierungsbehörden nach dem BerRehaG	174
10.4.2	Verlangen nach Einverständnis mit Einsichtnahme der Rehabilitierungsbehörde in die Unterlagen der Gauck-Behörde	175
11	**Landwirtschaft, Ernährung und Forsten**	177
11.1	Verdacht einer strafbaren Datenübermittlung aus dem SML an einen privaten Dritten: Zweiter Teil	177
11.2	Überwachung der Betriebe des ökologischen Landbaus	177
12	**Umwelt und Landesentwicklung**	178
12.1	Datenerhebung zur Vorbereitung der Einführung codierter Abfallbehälter	178
12.2	Datenerhebung durch ehrenamtliche Naturschutzhelfer	178

13	**Wissenschaft und Kunst**	180
13.1	Hochschulgesetzgebung	180
13.2	Evaluation der Lehre	180
13.3	Forschung	183
	Forschungsverbund "Public Health" Sachsen	183
14	**Technischer und organisatorischer Datenschutz**	185
14.1	Orientierungshilfe zu Datenschutzfragen des Anschlusses von Netzen der öffentlichen Verwaltung an das Internet	185
14.2	Digitale Telekommunikationsanlagen – ISDN	196
14.2.1	Kontrolle von Dienstgesprächen	196
14.2.2	Zur Gestaltung von Dienstvereinbarungen	197
14.3	Entwicklung von DV-Verfahren	200
14.4	Wartung / Fernwartung	202
14.5	Datenfernübertragung	203
14.6	Dienstliche Nutzung privater Hard- und Software	204
14.7	Löschung bzw. Vernichtung magnetischer Datenträger	206
14.8	Zugangskontrolle - Datenerfassung beim Pförtner	208
14.9	Gestaltung von Behördenpost	209
15	Vortrags- und Schulungstätigkeit	209
16	**Materialien**	210
16.1	**Entschließungen der 50. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 9./10. November 1995 in Bremen**	210
16.1.1	Zur Weiterentwicklung des Datenschutzes in der Europäischen Union	210
16.1.2	Zu Planungen für ein Korruptionsbekämpfungsgesetz	213
16.1.3	Zu Forderungen an den Gesetzgeber zur Regelung der Übermittlung personenbezogener Daten durch die Ermittlungsbehörden an die Medien (außerhalb der Öffentlichkeitsfahndung der Ermittlungsbehörden	215
16.1.4	Zu Datenschutzrechtlichen Anforderungen an den Einsatz von Chipkarten im Gesundheitswesen	216
16.1.5	Zum Datenschutz bei der Neuordnung der Telekommunikation (Postreform III	220

16.2 Entschließungen der 51. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14./15. März 1996 in Hamburg 222

16.2.1 Zur Modernisierung und europäischen Harmonisierung des Datenschutzrechts 222

16.2.2 Zum Transplantationsgesetz 224

16.3 Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 29. April 1996 zu Eckpunkten für die datenschutzrechtliche Regelung von Mediendiensten 224

Abkürzungsverzeichnis

Vorschriften

Nachstehend werden Gesetze und andere Vorschriften nach der alphabetischen Reihenfolge der *amtlichen, in Ausnahmefällen auch nicht-amtlichen Abkürzung*, ersatzweise der *amtlichen Kurzbezeichnung* aufgeführt.

Diese genaue Fundstellenangabe ist bei bekannteren Bundesgesetzen (die in den gängigen Gesetzessammlungen leicht zu finden sind) weggelassen.

AO	Abgabenordnung
ArbZG	Arbeitszeitgesetz vom 6. Juni 1994 (BGBl. I S. 1170)
BAföG	Bundesgesetz über individuelle Förderung der Ausbildung (Bundesausbildungsförderungsgesetz) in der Fassung der Bekanntmachung vom 6. Juni 1983 (BGBl. I S. 645), zuletzt geändert durch Art. 34 des Gesetzes vom 11. Oktober 1995 (BGBl. I S. 1250)
BAT(-O)	Erster Tarifvertrag zur Anpassung des Tarifrechts - Manteltarifliche Vorschriften (BAT-O) vom 10. Dezember 1990 (SächsABl. 1991 Nr. 10 S. 1), zuletzt geändert durch Änderungstarifvertrag Nr. 7 vom 15. Dezember 1995 (noch nicht veröffentlicht)
BBG	Bundesbeamtengesetz vom 27. Februar 1985, zuletzt geändert durch Art. 1 des Neunten Gesetzes zur Änderung dienstrechtlicher Vorschriften vom 11. Juni 1992 (BGBl. I S. 1030)
BBiG	Berufsbildungsgesetz
BDSG	Gesetz zur Fortentwicklung der Datenverarbeitung und des Datenschutzes (Bundesdatenschutzgesetz)
BerRehaG	Gesetz über den Ausgleich beruflicher Benachteiligungen für Opfer politischer Verfolgung im Beitrittsgebiet (Berufliches Rehabilitierungsgesetz) vom 23. Juni 1994 (BGBl. I S.1311, 1314), geändert durch das Gesetz zur Änderung des Strafrechtlichen Rehabilitierungsgesetzes, des Verwaltungsrechtlichen Rehabilitierungsgesetzes und des Beruflichen Rehabilitierungsgesetzes vom 15. Dezember 1995 (BGBl. I S. 1782)
Berufskrankheiten-VO	Berufskrankheiten-Verordnung vom 20. Juni 1968 (BGBl. I S. 721), zuletzt geändert durch die Zweite Änderungsverordnung vom 18. Dezember 1992 (BGBl. I S. 2343)
BewG	Bewertungsgesetz
BGB	Bürgerliches Gesetzbuch
BRAO	Bundesrechtsanwaltsordnung vom 1. August 1959 (BGBl. I S. 565), zuletzt geändert durch das Gesetz zur Neuordnung des Berufsrechts der Rechtsanwälte und der Patentanwälte vom 2. September 1994 (BGBl. I S. 2278)
BSeuchG	Gesetz zur Verhütung und Bekämpfung übertragbarer Krankheiten beim Menschen (Bundes-Seuchengesetz) in der Fassung der Bekanntmachung vom 18. Dezember 1979 (BGBl. I S. 2262, ber. 1980 I S. 151)
BSHG	Bundessozialhilfegesetz in der Fassung der Bekanntmachung vom 10. Januar 1991 (BGBl. I S. 94, ber. S. 808), zuletzt geändert durch das Gesetz zur sozialen Absicherung der Pflegebedürftigkeit (Pflege-Versicherungsgesetz - PflegeVG) vom 26. Mai 1994 (BGBl. I S. 1014)
BStatG	Gesetz über die Statistik für Bundeszwecke (Bundesstatistikgesetz) vom 22. Januar 1987 (BGBl. I S. 462, 565), zuletzt geändert durch Art. 2 des Mikrozensusgesetzes und Gesetzes zur Änderung des Bundesstatistikgesetzes vom 17. Januar 1996 (BGBl. I S. 34)

BVerfSchG	Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz vom 20. Dezember 1990 (BGBl. I S. 2954), zuletzt geändert durch § 38 Abs. 2 des Sicherheitsüberprüfungsgesetzes vom 20. April 1994 (BGBl. I S. 867)
BZRG	Gesetz über das Zentralregister und das Erziehungsregister (Bundeszentralregistergesetz)
DA	Dienstanweisung für die Standesbeamten und ihre Aufsichtsbehörden vom 23. November 1987 (BAnz. Nr. 227 a), zuletzt geändert durch Änderungsverwaltungsvorschrift vom 31. März 1994 (BAnz. S. 3881)
EStG	EinkommensteuergesetzGeschlKrG Gesetz zur Bekämpfung von Geschlechtskrankheiten vom 23. Juli 1953 (BGBl. I S. 700; BGBl. III 2126-4), zuletzt geändert durch Art. 7 des Gesetzes zur Reform des Rechts der Vormundschaft und Pflegschaft für Volljährige vom 12. September 1990 (BGBl. I S. 2002)
GeschoSReg	Geschäftsordnung der Sächsischen Staatsregierung vom 27. Juli 1992 (SächsABl. S. 1116), geändert gemäß Bekanntmachung vom 12. November 1993 (SächsABl. S. 1266)
GewO	Gewerbeordnung
GG	Grundgesetz für die Bundesrepublik Deutschland (Grundgesetz)

GVG	Gerichtsverfassungsgesetz
HandwO	Gesetz zur Ordnung des Handwerks (Handwerksordnung)
InVorG	Gesetz über den Vorrang für Investitionen bei Rückübertragungsansprüchen nach dem Vermögensgesetz (Investitionsvorranggesetz), als Art. 6 Bestandteil des 2. VermRÄndG vom 14. Juli 1992 (BGBl. I S. 1257, 1268), geändert durch die Verordnung zur Verlängerung des Investitionsvorranggesetzes vom 8. Dezember 1995 (BGBl. I S. 1609)
JGG	Jugendgerichtsgesetz in der Fassung der Bekanntmachung vom 11. Dezember 1974 (BGBl. I S. 3427), zuletzt geändert durch das Verbrechensbekämpfungsgesetz vom 28. Oktober 1994 (BGBl. I S. 3186)
KommStatVO	VO des Sächsischen Staatsministeriums des Innern zum Einsatz von Datenverarbeitungsanlagen in kommunalen Statistikstellen vom 9. Februar 1996 (GVBl. S. 81)
KpS-Richtlinien	Richtlinien des Sächsischen Staatsministeriums des Innern für die Führung Kriminalpolizeilicher personenbezogener Sammlungen in den Polizeidienststellen des Freistaates Sachsen vom 15. Juli 1993 (SächsABl. S. 1094)
KRG	Gesetz über Krebsregister (Krebsregistergesetz) vom 4. November 1994 (BGBl. I S. 3351)
MDR-Staatsvertrag	Staatsvertrag über den Mitteldeutschen Rundfunk (MDR) vom 30. Mai 1991 (GVBl. S. 169)
MiStra	Anordnungen über Mitteilungen in Strafsachen vom 15. März 1985 (BAnz. Nr. 60)
MiZi	Anordnungen über Mitteilungen in Zivilsachen vom 1. Oktober 1967 in der ab 1. März 1993 geltenden bundeseinheitlichen Fassung (BAnz. Nr. 28)
MRRG	Melderechtsrahmengesetz in der Fassung der Bekanntmachung vom 24. Juni 1994 (BGBl. I S. 1430)
OWiZuVO	Verordnung der Sächsischen Staatsregierung über Zuständigkeiten nach dem Gesetz über Ordnungswidrigkeiten vom 2. Juli 1993 (GVBl. S. 561), geändert durch VO vom 2. November 1994 (GVBl. S. 1629) und durch ÄndVO vom 7. Februar 1995 (GVBl. S. 100)
PaßVwV	Allgemeine Verwaltungsvorschriften zur Durchführung des Paßgesetzes (PaßG) vom 2. Januar 1988 (GMBl. S. 3; BAnz. Nr. 1 a)
PAuswG	Gesetz über Personalausweise in der Fassung der Bekanntmachung vom 21. April 1986 (BGBl. I S. 548)

Pflegebedürftigkeits-richtlinien	Richtlinien der Spitzenverbände der Pflegekassen über die Abgrenzung der Merkmale der Pflegebedürftigkeit und der Pflegestufen sowie zum Verfahren der Feststellung der Pflegebedürftigkeit (PflRi) einschließlich Gutachten-Vordruck vom 7. November 1994 (nicht verkündet)
PStG	Personenstandsgesetz
RHG	Gesetz über den Rechnungshof des Freistaates Sachsen vom 11. Dezember 1991 (GVBl. S. 409)
RiStBV	Richtlinien für das Strafverfahren und das Bußgeldverfahren vom 1. Januar 1977, zuletzt geändert am 16. Februar 1996 (SächsJMBl. S. 48)
RVO	Reichsversicherungsordnung
SachenRBerG	Gesetz zur Sachenrechtsbereinigung im Beitrittsgebiet (Sachenrechtsbereinigungsgesetz) vom 21. September 1994 (BGBl. I S. 2457)
SächsAGLMBG	Gesetz zur Ausführung des Lebensmittel- und Bedarfsgegenständegesetzes im Freistaat Sachsen vom 31. März 1994 (GVBl. S. 682)
SächsArchG	Archivgesetz für den Freistaat Sachsen vom 17. Mai 1993 (GVBl. S. 449)
SächsBestG	Sächsisches Gesetz über das Friedhofs-, Leichen- und Bestattungswesen (Sächsisches Bestattungsgesetz) vom 8. Juli 1994 (GVBl. S. 1321)
SächsBeurtVO	Verordnung der Sächsischen Staatsregierung über die dienstliche Beurteilung der Beamten vom 11. Januar 1994 (GVBl. S. 90)
SächsBG	Beamtengesetz für den Freistaat Sachsen in der Fassung der Bekanntmachung vom 16. Juni 1994 (GVBl. S. 1153) SächsDSG Gesetz zum Schutz der informationellen Selbstbestimmung im Freistaat Sachsen (Sächsisches Datenschutzgesetz) vom 11. Dezember 1991 (GVBl. S. 401)
SächsFFG	Gesetz zur Förderung und der Vereinbarkeit von Familie und Beruf im öffentlichen Dienst im Freistaat Sachsen (Sächsisches Frauenförderungsgesetz) vom 31. März 1994 (GVBl. S. 684)

SächsFFStatVO	Verordnung der Sächsischen Staatsministerin für Fragen der Gleichstellung von Frau und Mann über die statistischen Angaben für die Frauenförderung in Dienststellen im Freistaat Sachsen (Sächsische Frauenförderungsstatistikverordnung) vom 22. August 1995 (GVBl. S. 295)
SächsGDG	Gesetz über den öffentlichen Gesundheitsdienst im Freistaat Sachsen (Sächsisches Gesundheitsdienstgesetz) vom 11. Dezember 1991 (GVBl. S. 413)
SächsGemO	Gemeindeordnung für den Freistaat Sachsen vom 21. April 1993 (GVBl. S. 301), zuletzt geändert durch Gesetz vom 15. Juli 1994 (GVBl. S. 1432)
SächsHKaG	Gesetz über Berufsausübung, Berufsvertretungen und Berufsgerichtsbarkeit der Ärzte, Zahnärzte, Tierärzte und Apotheker im Freistaat Sachsen (Sächsisches Heilberufekammergesetz) vom 24. Mai 1994 (GVBl. S. 935)
SächsKHG	Gesetz zur Neuordnung des Krankenhauswesens (Sächsisches Krankenhausgesetz) vom 19. August 1993 (GVBl. S. 675)
SächsLErzGG	Gesetz über die Gewährung von Landeserziehungsgeld im Freistaat Sachsen vom 16. Oktober 1992 (GVBl. S. 467)
SächsLKrO	Landkreisordnung für den Freistaat Sachsen vom 19. Juli 1993 (GVBl. S. 577), zuletzt geändert durch Gesetz vom 19. April 1994 (GVBl. S. 773)
SächsMG	Sächsisches Meldegesetz vom 21. April 1993 (GVBl. S. 353), zuletzt geändert durch § 15 des Gesetzes über die Errichtung der Sächsischen Anstalt für kommunale Datenverarbeitung (SAKDG) vom 15. Juli 1994 (GVBl. S. 1432)
SächsNatSchG	Sächsisches Gesetz über Naturschutz und Landschaftspflege vom 11. Oktober 1994 (GVBl. S. 1601, ber. 1995 S. 106)
SächsNTVO	Verordnung der Sächsischen Staatsregierung über die Nebentätigkeit der Beamten und Richter im Freistaat Sachsen vom 21. Juni 1994 (GVBl. S. 1110)
SächsPersVG	Sächsisches Personalvertretungsgesetz vom 21. Januar 1993 (GVBl. S. 29)
SächsPolG	Polizeigesetz des Freistaates Sachsen in der Fassung der Bekanntmachung vom 15. August 1994 (GVBl. S. 1541)
SächsPresseG	Sächsisches Gesetz über die Presse vom 3. April 1992 (GVBl. S. 125)
SächsPsychKG	Sächsisches Gesetz über die Hilfen und die Unterbringung bei psychischen Krankheiten vom 16. Juni 1994 (GVBl. S. 1097)

SächsSchulG	Schulgesetz für den Freistaat Sachsen vom 3. Juli 1991 (GVBl. S. 213), zuletzt geändert durch Gesetz zur Änderung des Schulgesetzes für den Freistaat Sachsen vom 15. Juli 1994 (GVBl. S. 1434)
SächsStatG	Sächsisches Statistikgesetz vom 17. Mai 1993 (GVBl. S. 453)
SächsStudDatVO	Verordnung des Sächsischen Staatsministeriums für Wissenschaft und Kunst zur Verarbeitung personenbezogener Daten der Studienbewerber, Studenten und Prüfungskandidaten für statis tische und Verwaltungszwecke der Hochschulen (Sächsische Studentendatenverordnung) vom 9. Mai 1994 (GVBl. S. 916)
SächsVerf	Verfassung des Freistaates Sachsen vom 27. Mai 1992 (GVBl. S. 243)
SächsVSG	Gesetz über den Verfassungsschutz im Freistaat Sachsen (Sächsisches Verfassungsschutzgesetz) vom 16. Oktober 1992 (GVBl. S. 459)
SächsVwVG	Sächsisches Verwaltungs-Vollstreckungsgesetz vom 17. Juli 1992 (GVBl. S. 327)
SächsWahlG	Gesetz über die Wahlen zum Sächsischen Landtag vom 5. August 1993 (GVBl. S. 723), zuletzt geändert durch Art. 1 des Gesetzes zur Änderung des Sächsischen Wahlgesetzes und des Abgeordnetengesetzes vom 12. Januar 1995 (GVBl. S. 1)
SäHO	Vorläufige Haushaltsordnung des Freistaates Sachsen (Vorläufige Sächsische Haushaltsordnung) vom 19. Dezember 1990 (GVBl. S. 21)
2. SED-UnBerG	Zweites Gesetz zur Bereinigung von SED-Unrecht (2. SED-Unrechtsbereinigungsgesetz) vom 23. Juni 1994 (BGBl. I S. 1311)
SGB I	Sozialgesetzbuch - Allgemeiner Teil - vom 11. Dezember 1975 (BGBl. I S. 3015), zuletzt geändert durch Art. 2 des Agrarsozialreformgesetzes 1995 vom 29. Juli 1994 (BGBl. I S. 1890)
SGB IV	Sozialgesetzbuch - Gemeinsame Vorschriften für die Sozialversicherung - vom 23. Dezember 1976 (BGBl. I S. 3845), zuletzt geändert durch Art. 2 des Gesetzes zur Änderung des Sechsten Buches Sozialgesetzbuch und anderer Gesetze vom 15. Dezember 1995 (BGBl. I S. 1824)

SGB V	Sozialgesetzbuch - Gesetzliche Krankenversicherung - vom 20. Dezember 1988 (BGBl. I S. 2477), zuletzt geändert durch das Vierte Gesetz zur Änderung des Fünften Buches Sozialgesetzbuch vom 4. Dezember 1995 (BGBl. I S. 1558)
SGB VI	Sozialgesetzbuch - Gesetzliche Rentenversicherung - vom 18. Dezember 1989 (BGBl. I S. 2261, ber. BGBl. 1990 I S. 1337), zuletzt geändert durch Art. 1 des Gesetzes zur Änderung des Sechsten Buches Sozialgesetzbuch und anderer Gesetze vom 15. Dezember 1995 (BGBl. I S. 1824)
SGB VIII	Sozialgesetzbuch - Kinder- und Jugendhilfe - vom 26. Juni 1990 (BGBl. I S. 1163) in der Fassung der Bekanntmachung vom 3. Mai 1993 (BGBl. I S. 637), zuletzt geändert durch Art. 5 des Zweiten Gesetzes zur Änderung des Sozialgesetzbuches vom 13. Juni 1994 (BGBl. I S. 1229)
SGB X	Sozialgesetzbuch - Verwaltungsverfahren - vom 18. August 1980 (BGBl. I S. 1469) und 4. November 1982 (BGBl. I S. 1450), zuletzt geändert durch Art. 3 des Gesetzes zur Änderung des Sechsten Buches Sozialgesetzbuch und anderer Gesetze vom 15. Dezember 1995 (BGBl. I S. 1824)
SGB XI	Sozialgesetzbuch - Soziale Pflegeversicherung - vom 26. Mai 1994 (BGBl. I S. 1014), geändert durch Art. 4 des Gesetzes zur Änderung des Sechsten Buches Sozialgesetzbuch und anderer Gesetze vom 15. Dezember 1995 (BGBl. I S. 1824)
SHG	Gesetz über die Hochschulen im Freistaat Sachsen (Sächsisches Hochschulgesetz) vom 4. August 1993 (GVBl. S. 693)StGB Strafgesetzbuch
StPO	Strafprozeßordnung
StrRehaG	Gesetz über die Rehabilitierung und Entschädigung von Opfern rechtsstaatswidriger Strafverfolgungsmaßnahmen im Beitrittsgebiet (Strafrechtliches Rehabilitierungsgesetz) vom 29. Oktober 1992 (BGBl. I S. 814) zuletzt geändert durch Gesetz zur Änderung des Strafrechtlichen Rehabilitierungsgesetzes, des Verwaltungsrechtlichen Rehabilitierungsgesetzes und des Beruflichen Rehabilitierungsgesetzes vom 15. Dezember 1995 (BGBl. I S. 1782)
StUG	Gesetz über die Unterlagen des Staatssicherheitsdienstes der ehemaligen Deutschen Demokratischen Republik (Stasi-Unterlagen-Gesetz) vom 20. Dezember 1991 (BGBl. I S. 2272), zuletzt geändert durch Art. 12 des Gesetzes vom 14. September 1994 (BGBl. I S. 2325)

StVG	Straßenverkehrsgesetz
StVollZG	Gesetz über den Vollzug der Freiheitsstrafe und der freiheitsentziehenden Maßregeln der Besserung und Sicherung (Strafvollzugsgesetz) vom 16. März 1976 (BGBl. I S. 581, ber. S. 2088 und 1977 I S. 436), zuletzt geändert durch das Rechtspflege-Vereinfachungsgesetz vom 17. Dezember 1990 (BGBl. I S. 2847)
StVZO	Straßenverkehrs-Zulassungs-Ordnung
SVermG	Gesetz über die Landesvermessung und das Liegenschaftskataster im Freistaat Sachsen (Sächsisches Vermessungsgesetz) in der Fassung der Bekanntmachung vom 2. August 1994 (GVBl. S. 1457)
TKV 1995	Telekommunikations-Kundenschutzverordnung vom 19. Dezember 1995 (BGBl. I S. 2020)
UAusschG	Gesetz über Einsetzung und Verfahren von Untersuchungsausschüssen des Sächsischen Landtages (Untersuchungsausschußgesetz) vom 12. Februar 1991 (GVBl. S. 29)
VermG	Gesetz zur Regelung offener Vermögensfragen (Vermögensgesetz) vom 23. September 1990 (BGBl. II S. 885, 1159, in der Fassung der Bekanntmachung vom 3. August 1992, BGBl. I S. 446), zuletzt geändert durch Art. 1 des Vermögensrechtsanpassungsgesetzes vom 4. Juli 1995 (BGBl. I S. 895)
Verpflichtungs-gesetz	Gesetz über die förmliche Verpflichtung nichtbeamteter Personen vom 2. März 1974 (BGBl. I S. 469, 545; III 453-17), zuletzt geändert durch Änderungsgesetz vom 15. August 1974 (BGBl. I S. 1942)
VersammlG	Gesetz über Versammlungen und Aufzüge (Versammlungsgesetz) in der Fassung der Bekanntmachung vom 15. November 1978 (BGBl. I S. 1790), zuletzt geändert durch Art. 3 des Gesetzes zur Änderung des Strafgesetzbuches usw. vom 9. Juni 1989 (BGBl. I S. 1059)
VGO	Vollzugsgeschäftsordnung [bundeseinheitliche Länder-Verwaltungsvorschrift] vom Juli 1976 (veröffentlicht z. B. im Bayerischen Justizministerialblatt 1976 S. 339), zuletzt geändert 1986 (vgl. z. B. Bayerisches Justizministerialblatt 1987, S. 3)
VOB	Verdingungsordnung für Bauleistungen, Fassung 1979, Bundesanzeiger 1979, Nr. 206
VwRehaG	Gesetz über die Aufhebung rechtsstaatswidriger Verwaltungsentscheidungen im Beitrittsgebiet und die daran anknüpfenden Folgeansprüche (Verwaltungsrechtliches Rehabilitierungsgesetz) vom 23. Juni 1994 (BGBl. I S.1311), geändert durch das Gesetz zur Änderung des Strafrechtlichen Rehabilitierungsgesetzes, des Verwaltungsrechtlichen Rehabilitierungsgesetzes und des Beruflichen Rehabilitierungsgesetzes vom 15. Dezember 1995 (BGBl. I S. 1782)
VwVfG	Verwaltungsverfahrensgesetz
WoGSoG	Gesetz über Sondervorschriften für die vereinfachte Gewährung von Wohngeld in dem in Art. 3 des Einigungsvertrages genannten Gebiet in der Fassung der Bekanntmachung vom 16. Dezember 1992 (BGBl. I S. 2406), zuletzt geändert durch Art. 4 des Gesetzes zur Überleitung preisgebundenen Wohnraums im Beitrittsgebiet in das allgemeine Miethöherecht vom 6. Juni 1995 (BGBl. I S. 748)
WoStatG	Gesetz über gebäude- und wohnungsstatistische Erhebungen (Wohnungsstatistikgesetz) vom 18. März 1993 (BGBl. I S. 337)
WPflG	Wehrpflichtgesetz in der Fassung der Bekanntmachung vom 14. Juli 1994 (BGBl. I S. 1505)
WRV	Weimarer Reichsverfassung vom 11. August 1919 (RGBl. S. 1383)
ZDG	Gesetz über den zivilen Ersatzdienst vom 28. September 1994 (BGBl. I S. 2811), zuletzt geändert durch Art. 12 des Gesetzes vom 15. Dezember 1995 (BGBl. I S. 1726)

Sonstiges

ÄndVO	Änderungs-Verordnung
a. F.	alte Fassung
AROV	Amt zur Regelung offener VermögensfragenBAnz. Bundesanzeiger
BfD	Der Bundesbeauftragte für den Datenschutz
BGBl.	Bundesgesetzblatt
BGH	Bundesgerichtshof
BGHZ	Amtliche Sammlung der Entscheidungen des Bundesgerichtshofs in Zivilsachen

BMI	Bundesministerium des Innern
BMJ	Bundesministerium der Justiz
BMJFFG	Bundesministerium für Jugend, Familie, Frauen und Gesundheit [Organisationsstand 1986]
BSI	Bundesamt für Sicherheit in der Informationstechnik
BStU	Der Bundesbeauftragte für die Unterlagen des Staatssicherheitsdienstes der ehemaligen Deutschen Demokratischen Republik
BVerfG	Bundesverfassungsgericht
BVerfGE	Amtliche Sammlung der Entscheidungen des Bundesverfassungsgerichts
BVerwG	Bundesverwaltungsgericht
BVerwGE	Amtliche Sammlung der Entscheidungen des Bundesverwaltungsgerichts
CD-ROM	Compact disc-read only memory
CR	Computer und Recht [Zeitschrift; früher auch "CuR"]
EG	Europäische Gemeinschaften
EU	Europäische Union
EWG	Europäische Wirtschaftsgemeinschaft
FTP	File transfer protocol
Gauck-Behörde	Der Bundesbeauftragte für die Unterlagen des Staatssicherheitsdienstes der ehemaligen Deutschen Demokratischen Republik
GEZ	Gebühreneinzugszentrale der öffentlich-rechtlichen Rundfunkanstalten der Bundesrepublik Deutschland
GMBl.	Gemeinsames Ministerialblatt, hrsg. vom Bundesministerium des Innern
GSF	Forschungszentrum für Umwelt und Gesundheit GmbH (ehemals „Gesellschaft für Strahlenforschung“)
GVBl.	Sächsisches Gesetz- und Verordnungsblatt
GWZ 1995	Gebäude- und Wohnungszählung 1995
IKK	Innungskrankenkasse
ISDN	Integrated services digital network
JVA	Justizvollzugsanstalt
KGSt	Kommunale Gemeinschaftsstelle für Verwaltungsvereinfachung
LARoV	Landesamt zur Regelung offener Vermögensfragen

LfF	Landesamt für Finanzen des Freistaates Sachsen
LKA	Landeskriminalamt Sachsen
MDR	Mitteldeutscher Rundfunk
MedR	Medizinrecht [Zeitschrift]
MfS	Ministerium für Staatssicherheit
NJW	Neue Juristische Wochenschrift
NVwZ	Neue Zeitschrift für Verwaltungsrecht
PASS-System	Polizeiliches Auskunftssystem Sachsen
PersR	Zeitschrift Personalvertretungsrecht
PIN	Personal identification number (Persönliche Identifikationsnummer)
SächsABl.	Sächsisches Amtsblatt
SächsJMBl.	Sächsisches Justizministerialblatt
SK	Sächsische Staatskanzlei
SLT	Sächsischer Landkreistag e. V.
SMF	Sächsisches Staatsministerium der Finanzen
SMI	Sächsisches Staatsministerium des Innern
SMJus	Sächsisches Staatsministerium der Justiz
SMK	Sächsisches Staatsministerium für Kultus
SML	Sächsisches Staatsministerium für Landwirtschaft, Ernährung und Forsten
SMS	Sächsisches Staatsministerium für Soziales, Gesundheit und Familie
SMU	Sächsisches Staatsministerium für Umwelt und Landesentwicklung
SMWA	Sächsisches Staatsministerium für Wirtschaft und Arbeit
SMWK	Sächsisches Staatsministerium für Wissenschaft und Kunst
SSG	Sächsischer Städte- und Gemeindetag e. V.
TB	Tätigkeitsbericht
TCP/IP	Transmission control protocol/Internet protocol
TK-Anlage	Telekommunikationsanlage
TU	Technische Universität
VIZ	Zeitschrift für Vermögens- und Investitionsrecht
WWW	World wide Web

1 Datenschutz im Freistaat Sachsen

1.1 Der Blick über den Tellerrand

Das Bundesverfassungsgericht hat 1983 den Schutz unserer Privatsphäre vor ungesetzlicher Ausforschung durch öffentliche Stellen als Grundrecht entdeckt und definiert; die Sächsische Verfassung von 1992 hat dieses "Recht auf informationelle Selbstbestimmung" oder "auf Schutz personenbezogener Informationen" - kurz: "den Datenschutz" - in ihren Grundrechtskatalog aufgenommen (Art. 33).

In den ersten Jahren haben einige das Grundrecht geradezu euphorisch begrüßt, andere sind ihm mit Unverständnis, Ratlosigkeit und Ablehnung begegnet. Die Integration dieses Grundrechts in die Gesetzgebung, die Verwaltungspraxis und die Rechtswirklichkeit fiel und fällt schwer. Das hängt auch damit zusammen, daß der öffentliche Dienst dazu neigt, Rechtsfragen statisch, regelhaft und abgehoben von der bunten Lebenswirklichkeit zu betrachten und lösen zu wollen.

Ein vernünftiger, ausgeglichener, wirklich gerechter Umgang mit Verfassungsbestimmungen, sei es mit Staatsorganisationsnormen, sei es mit Grundrechtsbestimmungen, verlangt den Überblick, also eine nicht solitär fokussierende, sondern eine breit angelegte Abwägung im Zusammenhang aller in Betracht zu ziehenden Verfassungsregeln.

Deshalb ist es falsch, den Datenschutz als Regelung für sich allein zu betrachten. Deshalb ist es falsch, wenn ein Datenschutzbeauftragter seinen Blick nicht auch nach links und rechts neben das Grundrecht, für dessen Durchsetzung und Kontrolle er zuständig ist, richtet. Er muß danach fragen, was er mit der Betonung datenschutzrechtlicher Forderungen erreicht und bisweilen auch "anrichtet". Meine Behörde hat auch darüber nachzudenken, ob und wie das von ihr vertretene Grundrecht sich in die Gesamtordnung, die die Verfassung im Blick hat, einfügt.

Nur dann sind wir glaubwürdig.

Aus diesen Gründen müssen die Datenschützer darauf achten, ob ihre Interpretationen und Forderungen sich mit anderen Zielgrößen vertragen oder gar decken, ob der Datenschutz z. B. dem Urbedürfnis nach Sicherheit, der ersten und wichtigsten Begründung für einen Staat, zu einer breiten Akzeptanz auch bei kritischen und dem Gemeinwesen weniger zugewandten Personen verhilft oder ob der Datenschutz dazu beitragen kann, die Verwaltung zu vereinfachen und überschaubar zu machen, also Geld und Stellen einzusparen und dem Einzelnen das Gefühl zu geben, daß er als Subjekt nicht nur akzeptiert ist, sondern an seiner örtlichen Gemeinschaft aktiv teilnehmen kann.

1.2 Nochmals: Gegen den Zentralismus

In ihrer Stellungnahme vom 21. Februar 1996 teilt die Staatsregierung zu meinem 3.

Tätigkeitsbericht mit, die Entscheidung für eine zentrale oder dezentrale Datenverarbeitung "hängt also nicht von datenschutzrechtlichen Erwägungen ab".

Diese Auffassung ist nicht haltbar, es sei denn, man versteht unter "Datenschutz" lediglich Fragen der Datensicherheit, oder man richtet - wie es die Staatsregierung in ihrer Erwiderung tut - das Augenmerk ausschließlich darauf, ob personenbezogene Daten in großen Rechenzentren besser vor Mißbrauch geschützt werden können als in kleinen Einheiten. Datenschutz erschöpft sich jedoch nicht in Fragen der Datensicherheit.

Es kommt nicht darauf an, daß das landeseinheitliche Datenverarbeitungsverfahren für die Kommunen im Rechenzentrum der Stadt Leipzig keine "Zusammenführung der personenbezogenen Daten vorsieht", wie die Staatsregierung beteuert. Es kommt auch nicht darauf an, ob das "Migrationskonzept" ausschließt, daß eine Stelle Zugriff auf alle Daten der beteiligten Kommunen bekommt oder gar eine Vermischung oder ein Abgleich dieser Daten erfolgt.

Daß der Freistaat Sachsen kein Überwachungsstaat ist, daß er auf Freiheit und Bürgersinn angelegt ist, versteht sich allemal. Es muß uns darum gehen, daß der Einzelne dies auch verinnerlicht, daß er das Gefühl haben kann, nicht Objekt einer entfernten, unbeeinflußbaren Datenverarbeitung zu sein, sondern mitwirkendes Subjekt in seinem überschaubaren Lebenskreis.

Das Bundesverfassungsgericht sagt deshalb im Volkszählungsurteil: Im Mittelpunkt der grundgesetzlichen Ordnung stehen Wert und Würde der Person, die in freier Selbstbestimmung als Glied einer freien Gesellschaft wirkt. Ihrem Schutz dient das Persönlichkeitsrecht. Es umfaßt auch die aus dem Gedanken der Selbstbestimmung folgende Befugnis des Einzelnen, grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen seine persönlichen Sachverhalte offenbart werden. Diese Befugnis bedarf unter den heutigen und künftigen Bedingungen der automatisierten Datenverarbeitung in besonderem Maße des Schutzes. Sie ist vor allem deshalb gefährdet, weil bei Entscheidungsprozessen nicht mehr wie früher auf manuell zusammengetragene Karteien und Akten zurückgegriffen werden muß, vielmehr heute mit Hilfe der automatisierten Datenverarbeitung Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person (personenbezogene Daten) technisch gesehen unbegrenzt speicherbar und jederzeit ohne Rücksicht auf Entfernungen in Sekundenschnelle abrufbar sind. Sie können darüber hinaus - vor allem beim Aufbau integrierter Informationssysteme - mit anderen Datensammlungen zu einem teilweise oder weitgehend vollständigen Persönlichkeitsbild zusammengefügt werden, ohne daß der Betroffene dessen Richtigkeit und Verwendung zureichend kontrollieren kann. Damit haben sich in einer bisher unbekannten Weise die Möglichkeiten einer Einsicht- und Einflußnahme erweitert, welche auf das Verhalten des Einzelnen schon durch den psychischen Druck öffentlicher Anteilnahme einzuwirken vermögen.
Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffenden

Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden. Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß.
Das Grundgesetz hat, wie in der Rechtsprechung des Bundesverfassungsgerichts mehrfach hervorgehoben ist, die Spannung Individuum-Gemeinschaft im Sinne der Gemeinschaftsbezogenheit und Gemeinschaftsgebundenheit der Person entschieden. Grundsätzlich muß daher der Einzelne Einschränkungen seines Rechts auf informationelle Selbstbestimmung im überwiegenden Allgemeininteresse hinnehmen. Entscheidend dafür, daß der Bürger seinen Staat positiv empfindet, daß der Einzelne sich in seinem wehrhaften und ordentlichen Gemeinwesen geborgen fühlt, sind überschaubare Nutzung und zweckgebundene Verwendung der Daten. Dies hängt von den der Informationstechnologie eigenen Verarbeitungs- und Verknüpfungsmöglichkeiten ab. In diesem Zusammenhang sind die - sachlich häufig unbegründeten - Ängste der Bürger davor zu berücksichtigen, einer bürokratischen Maschinerie ausgeliefert zu sein.

Die Verwendung der Daten ist durch die Sächsische Verfassung auf den gesetzlich bestimmten Zweck begrenzt. Schon angesichts der Gefahren der automatischen Datenverarbeitung ist ein - amtshilfefester - Schutz gegen Zweckentfremdung durch Weitergabe und Verwertungsverbote gesichert. Als weitere verfahrensrechtliche Schutzvorkehrungen sind Aufklärungs-, Auskunfts- und Löschungspflichten gesetzlich festgeschrieben. Dies alles sind Errungenschaften, von denen man hier vor wenigen Jahren nur träumen konnte.

Zweifellos erhält das Rechenzentrum in Leipzig in einer kaum übersehbaren Fülle Daten sächsischer Bürger zu höchst unterschiedlichen Zwecken in seine Hand. Natürlich gehe ich davon aus, daß - und dies werde ich im einzelnen kontrollieren - im Rechenzentrum weder eine Zusammenführung von Daten noch deren Vermischung oder gar ein Datenabgleich erfolgt. Jedoch entsteht für den einzelnen Bürger eine Unüberschaubarkeit und Unbeeinflußbarkeit in bezug auf die Verarbeitung seiner Daten; dies wäre nicht der Fall, wenn die einzelne (größere und leistungsfähige) Gemeinde die Datenverarbeitung selbst vornähme. Die zentrale Datenverarbeitung führt - zumindest annäherungsweise - dazu, daß der Bürger eben nicht mehr wissen kann, wer was wann und bei welcher Gelegenheit über ihn weiß.

Unbegrenzte Speicherung, unbegrenzte Abruf-, Verknüpfungs- und insbesondere Zusammenfügungs*möglichkeiten* in einem einzigen zentralen Rechenzentrum stellen sich für den Einzelnen wesentlich bedrohlicher dar, als wenn die Datenverarbeitung in der örtlichen Gemeinschaft erfolgt.

Es geht bei diesem Befund sowohl um objektive Mißbrauchsgefahren als auch - und

noch mehr - um subjektive Unsicherheiten und Ängste, die den Einzelnen in den neuen Ländern noch immer viel mehr als im Westen Deutschlands dazu bringen, "besser nicht aufzufallen" und sich der Obrigkeit eher machtlos ausgeliefert zu fühlen.

Das zu vermeiden ist meine Aufgabe.

Im übrigen ist der Zentralismus in der Datenverarbeitung nicht nur mit einer wachsenden Unüberschaubarkeit und folglich mit einer rein subjektiven Bedrohung des Einzelnen verbunden, sondern - und darauf muß ich hinweisen, weil ich nach wie vor über meinen Tellerrand zu sehen beabsichtige - auch mit einer erheblichen Verteuerung der technischen Apparaturen verbunden. Die gesamte technische Welt der Datenverarbeitung ist auf Dezentralisierung und zunehmend kleinere Einheiten hin ausgerichtet. Offenbar hat die Technik - mancherorts früher als die Verwaltung - erkannt, daß der dezentralisierten Datenverarbeitung die Zukunft gehört.

1.3 Rückblick

Im Sommer 1995 sorgten persönliche Vorwürfe gegen einen sächsischen Minister, lange unaufgeklärt, für eine Pressemitteilung und sodann für Aufregung der Bevölkerung. Der Ministerpräsident ordnete daraufhin eine Untersuchung der Vorgänge durch einen pensionierten Bundesrichter an, der tagelang ingesamt 41 Personen befragte. Dabei erhob er personenbezogene Informationen zur Intimsphäre und Daten von öffentlich Bediensteten, die in Personalakten und Sicherheitsakten gehören, er erhob in vielen "Vernehmungen" Einzelheiten, die auch strafrechtlich von Belang sein konnten.

Als ich von den Ermittlungen erfuhr, habe ich sofort auf den Ministerpräsidenten und den Ermittler einzuwirken versucht: Ich habe fernmündlich, im persönlichen Gespräch und schriftlich darauf verwiesen, daß derartige Ermittlungen gesetzlich nicht vorgesehen oder gestattet, verfahrensrechtlich nicht gesichert und daher rechtswidrig sind. Nachdem darauf zwei Tage lang keine Reaktion erfolgte, habe ich den Vorgang beanstandet; dennoch wurden die Befragungen - wie erwartet ohne verwertbare Erkenntnisse - fortgesetzt. Die Behauptung, ich hätte dem Ministerpräsidenten vor der Beanstandung keine Möglichkeit zur Stellungnahme gegeben, konnte ich leicht anhand meiner Akten widerlegen. Dem Parlament habe ich berichtet; zu den Einzelheiten verweise ich auf diesen Bericht.

Im Herbst 1995 kam es in Sachsen zum ersten "Lauschangriff" zur Gefahrenabwehr; ob es ein "Großer" war, ist schon fraglich, wurde doch im Nebenzimmer und nicht in dem Hotelzimmer selbst gelauscht, das ein mutmaßlicher Planer der Entführung eines mittelsächsischen Landrates bewohnte.

Nach wie vor halte ich daran fest, daß die sächsische Polizeiführung die geltenden Vorschriften des Sächsischen Polizeigesetzes zum Einsatz besonderer Mittel der

Datenerhebung grundsätzlich korrekt angewandt hat. Nachgeordneten Beamten sind allerdings Fehler unterlaufen; die nicht vollständige Dokumentation der verdeckten Datenerhebung wurde vom Präsidenten des Landeskriminalamtes entdeckt und dienst(recht)lich korrigiert.

Zu den Einzelheiten habe ich dem Innenausschuß des Landtages zweimal schriftlich berichtet.

Nach der Entscheidung des Verfassungsgerichtshofes zur Vereinbarkeit der §§ 35 bis 51 des Sächsischen Polizeigesetzes mit der Sächsischen Verfassung, die Mitte Mai 1996 zu erwarten ist, werden wir klüger sein. Für den Fall, daß das Polizeigesetz geändert werden muß, biete ich dem Sächsischen Staatsministerium des Innern meine beratende Mitarbeit an.

Ich kann wiederum über ein grundsätzlich gutes Jahr für den Datenschutz in Sachsen berichten: Die Sensibilität der Staatsregierung und der anderen öffentlichen Stellen für das Grundrecht auf informationelle Selbstbestimmung ist gewachsen; die Zusammenarbeit läuft - von Ausnahmen abgesehen - zufriedenstellend, oftmals reibungslos.

Dem Präsidenten des Sächsischen Landtages und seiner Verwaltung habe ich für guten Rat und tagtägliche Unterstützung zu danken. Allen Bediensteten in meiner Behörde danke ich für ihre Unterstützung.

2 Parlament; Rechnungshof

Einschränkungen bei der Beantwortung einer Kleinen Anfrage

Eine Kleine Anfrage galt Konzentrationsvorgängen in einem Wirtschaftsbereich, der weitgehend von Verträgen mit entsorgungspflichtigen Gebietskörperschaften (Landkreise und kreisfreie Städte) 'lebt'.

Das zuständige Ministerium hatte Zweifel, ob es, wie verlangt, - und zwar bezogen auf die einzelnen Gebietskörperschaften - die Namen der Unternehmen, die Marktanteile sowie die Beteiligungsverhältnisse nennen dürfe. Diese Zweifel waren begründet:

Art. 51 Abs. 2 SächsVerf ist, wegen der Bindung aller öffentlichen Gewalt an Gesetz und Recht (Rechtsstaatsprinzip, vgl. Art. 20 Abs. 3 GG) und namentlich an die Grundrechte (vgl. Art. 1 Abs. 3 GG), so zu verstehen, daß die Staatsregierung eine Abgeordneten-Anfrage nicht nur nicht beantworten muß, sondern gar *nicht* beantworten *darf*, soweit der Beantwortung gesetzliche Regelungen oder Rechte Dritter entgegenstehen (vgl. Kunzmann u. a., Verfassung des Freistaates Sachsen, Rdnr. 4 zu Art. 51). Die Ausübung des mit Verfassungsrang gewährleisteten Kontrollrechts des

Parlaments ermächtigt nur unter Wahrung des Grundsatzes der Verhältnismäßigkeit zu Eingriffen in betroffene Grundrechte (Grundrecht auf informationelle Selbstbestimmung, die grundrechtliche Gewährleistung des Eigentums, vgl. BVerfGE 67, 100 [142, 144]).

Diese Grundrechte waren im vorliegenden Falle betroffen. Zwar war die Tatsache, daß namentlich zu benennende Unternehmen Vertragspartner der entsorgungspflichtigen Gebietskörperschaften sind oder daß sie bestimmte Entsorgungsanlagen betreiben, in den jeweiligen Entsorgungsgebieten ohnehin schon in der Öffentlichkeit bekannt. In der Gesamtübersicht für ganz Sachsen würde jedoch durch die verlangten Angaben ein 'Profil' für großräumiger bestehende Verhältnisse gezeichnet, das so gerade nicht bereits in der Öffentlichkeit bekannt war. Derartige Profile wären - gerade angesichts der Konzentrationstendenzen - für Marktanalytiker höchst interessant.

Für den eigentlichen Zweck der Anfrage, nämlich eine Unterrichtung über Art und Umfang der Konzentration in dem betreffenden Wirtschaftsbereich, war es ausreichend, wenn das Ministerium ein recht genaues Bild vermittelte, ohne Grundrechte zu berühren, indem es nämlich die Angaben anonymisierte. So konnten zweckmäßigerweise die entsorgungspflichtigen Gebietskörperschaften - nicht in alphabetischer Reihenfolge ihrer Namen - durch Kennbuchstaben, die Unternehmen durch Kennzahlen angegeben werden.

Auf diese Weise war es auch ohne weiteres möglich, anzugeben, daß z. B. das Unternehmen mit der Kennzahl 1 Geschäftsanteile an den Unternehmen mit den Kennzahlen 5 und 14 hält, daß am Unternehmen mit der Kennzahl 1 die zuständigen Gebietskörperschaften Geschäftsanteile in Höhe von 51 v. H. halten, während außerdem noch Geschäftsanteile Privater in Höhe von 23 % und von 26 % daran bestehen.

Meine dahingehenden Ratschläge haben dem Staatsministerium und dem fragenden Abgeordneten eingeleuchtet.

In aller Regel dürfte dem Zweck der parlamentarischen Kontrolle, sofern diese wie im vorliegenden Fall nicht das Verhalten der Exekutive oder auch Privater in einem auffällig gewordenen Einzelvorgang von öffentlichem Interesse überprüfen will, ohnehin mehr durch die Zusammenstellung eines übersichtlichen Gesamtbildes gedient sein als mit einer Fülle nichtanonymisierter Einzelangaben.

3 Europäische Union

EU-Datenschutzrichtlinie

Nach langjährigen Verhandlungen hat der Ministerrat am 24. Juli 1995 die EU-

Richtlinie zum Datenschutz verabschiedet. Die im Oktober 1995 in Kraft getretene Richtlinie schafft ein einheitliches Datenschutzniveau innerhalb der EU und beseitigt damit die Hindernisse für einen freien EU-internen Datenverkehr. Zugleich wurde damit der erste bedeutende Schritt getan, Menschenrechte in Gemeinschaftsrecht auszuformulieren.

Indem sie die bestehenden nationalen Datenschutzsysteme lediglich harmonisiert - nicht vereinheitlicht -, läßt die Richtlinie den Mitgliedsstaaten die Kompetenz, aus dem Angebot der Regelungsvarianten geeignete Modelle in das nationale Recht zu übernehmen. Dabei ist es den Mitgliedsstaaten freigestellt, auch Datenschutzregelungen zu schaffen, die über das Schutzniveau der Richtlinie hinausgehen.

Mit der Annahme durch den Ministerrat im Juli 1995 läuft die für die Mitgliedsstaaten verbindliche dreijährige Frist, in der die Bestimmungen der Richtlinie in nationales Datenschutzrecht umzusetzen sind. Sowohl das Bundesdatenschutzgesetz als auch das Sächsische Datenschutzgesetz sind in weitem Umfang zu novellieren. Dabei werden insbesondere die folgenden Vorgaben der Richtlinie von Bedeutung sein:

- Die EU-Richtlinie unterscheidet nicht zwischen der Datenverarbeitung durch öffentliche Stellen und durch Private. Im privaten Bereich werden für die Zweckbindung der Daten und die Erforderlichkeit der Datenverarbeitung strengere Voraussetzungen gelten.
- Sensitive Daten, etwa über religiöse oder philosophische Überzeugungen, über rassische oder ethnische Herkunft, politische Meinungen, Gesundheit oder Sexualleben genießen nach der Richtlinie einen besonderen, über das deutsche Datenschutzrecht hinausgehenden Schutz vor Nutzung und Weitergabe.
- Mit der Richtlinie, die die Verarbeitungsprivilegien der Medien stark einschränkt, ist die derzeitige generelle Freistellung der Medien durch das Medienprivileg des Bundesdatenschutzgesetzes sowie die Privilegierung öffentlicher Rundfunkanstalten durch die Einrichtung von Rundfunkbeauftragten, auch für den kommerziellen Bereich, nicht mehr zu vereinbaren.
- Bewertende Einzelentscheidungen zu einer Person (wie etwa zur beruflichen Leistungsfähigkeit, Kreditwürdigkeit, etc.), die allein auf Grundlage einer automatisierten Datenverarbeitung ergehen, sind nach der Richtlinie verboten.
- Neben dem Auskunftsrecht wird dem Betroffenen nunmehr auch das Recht gegeben, einer Datenverarbeitung grundsätzlich (allerdings mit Einschränkungen) zu widersprechen.
- Die Mitgliedsstaaten können von umfassenden Pflichten zur Meldung an zentrale Register absehen, wenn sie die Einrichtung eines betrieblichen/behördlichen Datenschutzbeauftragten gewährleisten. Damit soll ermöglicht werden, bürokratische Meldeprozeduren durch konkrete Datenschutzleistungen zu ersetzen. Das Sächsische Datenschutzgesetz, das zur Bestellung eines internen behördlichen Datenschutzbeauftragten keine Aussage enthält, wird entsprechend zu ergänzen sein.
- Nach der Richtlinie müssen die Datenschutzkontrollinstanzen ihre Aufgaben in "völliger Unabhängigkeit" und auch im privaten Bereich anlaßunabhängig

wahrnehmen. Es besteht kein Zweifel, daß die völlige Unabhängigkeit die Einbindung in ministerielle Weisungsstränge ausschließt. In einigen Bundesländern (darunter dem Freistaat Sachsen) wirft die organisatorische, dienstrechtliche und rechtsaufsichtliche Einbindung von Aufsichtsbehörden die Frage auf, wie weit das Kriterium der völligen Unabhängigkeit erfüllt ist. Zweifelsfrei gemeinschaftskonform kann demnach die Schaffung einer Obersten Bundes- sowie Oberster Landesbehörden für die (einheitliche) Datenschutzkontrolle öffentlicher und privater Stellen sein. Das Berliner Modell könnte hier als Vorbild dienen.
Den Datenschutzkontrollinstanzen müssen nach der Richtlinie über die bloße Empfehlungskompetenz hinausgehende wirksame Einwirkungsbefugnisse verliehen werden, so z. B. unmittelbare Anordnungsbefugnisse, Klagerecht und Anzeigebefugnisse bei datenschutzrechtlichen Verstößen.

Zur Anpassung des Bundesdatenschutzgesetzes an die EU-Datenschutzrichtlinie wurde von der Konferenz der Datenschutzbeauftragten des Bundes und der Länder eine Arbeitsgruppe "Neues Datenschutzrecht" eingerichtet, an der ich teilnehme. Die Ergebnisse dieser Beratungen werden einfließen in den - hoffentlich intensiven und fruchtbringenden - Diskussionsprozeß zwischen den Regierungen und den Datenschutzbeauftragten zur Novellierung der Datenschutzgesetze.

4 Medien

Siehe Abschnitt 10.2.12 und Abschnitt 14.1.

5 Inneres

5.1 Personalwesen

5.1.1 Rechtliche Entwicklung des öffentlichen Dienstrechts

Zu einem Referentenentwurf eines Gesetzes zur Änderung dienstrechtlicher Vorschriften habe ich mich insbesondere zu den Bestimmungen über die Personaldatenverarbeitung (§§ 117 ff. SächsBG) geäußert.

Die bisherige Fassung des § 121 SächsBG (Vorlage von Personalakten und Auskünfte aus Personalakten) führt nach meinem Dafürhalten immer wieder zu Auslegungsproblemen.

So ist z. B. nicht eindeutig geregelt, unter welchen Voraussetzungen einem (künftigen) nichtstaatlichen und/oder außersächsischen Dienstherrn die Personalakte eines Beamten übersandt werden darf. Ebenso ist nicht eindeutig geregelt, unter welchen Voraussetzungen die in Absatz 1 aufgeführten Dritten Auskünfte aus der Personalakte für andere als in Absatz 1 genannte Zwecke erhalten können. Schließlich ist es bisher nicht deutlich, daß andere gesetzliche Bestimmungen über Auskunfts- und Vorlagepflichten (z. B. § 14 UAusschG) unberührt bleiben.
Ich habe deshalb vorgeschlagen, Absatz 2 wie folgt zu fassen:
"(2) [1]Die *Vorlage* von Personalakten an andere als in Absatz 1 genannte Dritte ist nur *mit Einwilligung* des Beamten zulässig und nur soweit es zur Vorbereitung oder Durchführung einer Personalentscheidung erforderlich ist. [2]*Auskünfte* an andere als in Absatz 1 genannte Dritte oder zu anderen als in Absatz 1 genannten Zwecken dürfen nur mit Einwilligung des Beamten erteilt werden, es sei denn, daß die Abwehr einer erheblichen Beeinträchtigung des Gemeinwohls oder der Schutz berechtigter, höherrangiger Interessen des Dritten die Auskunftserteilung zwingend erfordert. [3]Inhalt und Empfänger der Auskunft sind dem Beamten schriftlich mitzuteilen. [4]Absatz 1 Satz 5 gilt entsprechend. [5]Andere gesetzliche Bestimmungen über Auskunfts- und Vorlagepflichten bleiben unberührt."

Zu § 124 Abs. 1 SächsBG habe ich zur Klarstellung des bisher mißverständlichen Textes vorgeschlagen, daß Personalaktendaten entweder nur in "automatisierten" oder "sowohl in manuellen als auch in automatisierten Dateien" für die dort genannten Zwecke verarbeitet und genutzt werden dürfen.

Es bleibt abzuwarten, ob meine Vorschläge berücksichtigt werden.

5.1.2 Führung und Verwaltung von Personalakten für Arbeiter und Angestellte im öffentlichen Dienst

Bislang existieren in Sachsen keine Vorschriften zur Führung von Personalakten für die im öffentlichen Dienst beschäftigten Angestellten und Arbeiter. Bei Anfragen und Kontrollen habe ich oft empfohlen, die für die Personalaktenführung der Beamten geltende Verwaltungsvorschrift des SMI vom 4. November 1993 auf den Arbeitnehmerbereich entsprechend anzuwenden.

Erfreulicherweise beabsichtigt das für den Tarifbereich zuständige SMF nunmehr den Erlaß einer Verwaltungsvorschrift zum Umgang mit Personalakten der Arbeitnehmer in enger Anlehnung an die o. g. Verwaltungsvorschrift des SMI. Ein konsensfähiger Entwurf liegt mir allerdings noch nicht vor.

Bei einer Novellierung des Sächsischen Datenschutzgesetzes werde ich mich dafür einsetzen, daß die für die Beamten geltenden Bestimmungen zur Personalaktenführung (§§ 117 ff. SächsBG) in § 31 SächsDSG für den Arbeitnehmerbereich für anwendbar erklärt werden.

5.1.3 Verwaltungsungsvorschrift des SMI zur Begründung und Beendigung des Beamtenverhältnisses: Frage nach anhängigen Strafverfahren

Im 3. Tätigkeitsbericht (5.1.3) habe ich den Entwurf einer Verwaltungsvorschrift des SMI zur Begründung und Beendigung eines Beamtenverhältnisses insofern nachdrücklich kritisiert, als sämtliche Bewerber um eine Beamtenstelle eine schriftliche Erklärung über etwa anhängige strafrechtliche Ermittlungsverfahren oder anhängige Strafverfahren abzugeben haben sollen.

Intensiver Schriftwechsel und Gespräche mit dem SMI führten zu dem Ergebnis, daß nach dem überarbeiteten Entwurf der o. g. Verwaltungsvorschrift diese Erklärung nur noch bei Bewerbern vorgesehen ist, deren Einstellung *konkret* beabsichtigt ist (Bewerber der engeren Wahl).

Dies halte ich im Hinblick auf die für Beamte verbindliche Gesetzestreue aus datenschutzrechtlicher Sicht für hinnehmbar, weise aber nochmals darauf hin, daß der Beschuldigte meist nicht weiß, daß gegen ihn ermittelt wird.

5.1.4 Belegverkehr im Bereich Besoldung zwischen Personalstellen und dem Landesamt für Finanzen (LfF)

Das SMF hat mich gemäß § 31 Abs. 7 SächsDSG am Verfahren zum Daten- und Belegverkehr zwischen personalverwaltenden Stellen und den Bezügestellen des LfF für die *Beamten- und Richterbesoldung* beteiligt (zum Verfahren für den *Tarifbereich* siehe Nr. 5.1.7 meines 2. Tätigkeitsberichtes). Meinen Anregungen und Hinweisen ist es weitgehend gefolgt:
Anstelle des Abdrucks der jeweiligen Verfügungen werden dem LfF nur noch die *Gründe des Wegfalls der Bezüge, z. B. der Tenor der Disziplinarentscheidung* formblattmäßig mitgeteilt. Ebenfalls mit Vordruck werden dem LfF Änderungen in den persönlichen Verhältnissen mitgeteilt. Auf die Angaben *Geburtsdatum und -ort des Ehegatten, Gericht und Aktenzeichen des Scheidungsurteils* sowie auf alle weiteren *Angaben zum Wohnsitz* (bisheriger Wohnsitz wird beibehalten - nicht beibehalten; 2. Wohnsitz) wird verzichtet.

Damit besteht jetzt im staatlichen Bereich ein einheitliches und datenschutzgerechtes Verfahren für die Festsetzung, Abrechnung und Zahlbarmachung der Vergütungen und Bezüge für Arbeiter, Angestellte, Beamte, Richter und Staatsanwälte. Das mit mir hergestellte Benehmen schließt nicht aus, daß künftig festgestellte datenschutzrechtliche Mängel im Belegverkehr erneut einer Prüfung unterzogen werden.

5.1.5 Nachweise für die Bezügeberechnung

Eine Bezügestelle im Landesamt für Finanzen forderte stets den Arbeitsamtsbescheid an, wenn ein Beschäftigter in der Erklärung über den Ortszuschlag angegeben hatte, der Ehegatte sei arbeitslos, werde umgeschult oder erhalte Altersübergangsgeld. Diese Praxis erschien einer Petentin fragwürdig, weil der vom SMF vorgeschriebene Erklärungsvordruck derartige Angaben über den Ehegatten nicht verlangte.

Wie sich herausstellte, hatte die betreffende Bezügestelle ohne Weisung gehandelt. Wie das SMF bestätigte, waren die angeforderten Unterlagen nicht erforderlich, denn über die Höhe des Ehegattenanteils im Ortszuschlag hätte allein aufgrund der Angaben in der Erklärung entschieden werden können.

Das SMF hat diese Praxis umgehend unterbunden. Als besonders erfreulich habe ich es gewertet, daß den Betroffenen mit der folgenden Bezügemitteilung ein Entschuldigungsschreiben übersandt wurde und die Aktenbereinigung eine Selbstverständlichkeit war.

Eine andere Petentin hatte Bedenken, die Geburtsurkunden der Kinder als Nachweise für die Angaben in der Erklärung über den Ortszuschlag vorzulegen. Sie fragte, ob die Daten nicht der bereits vorliegenden Lohnsteuerkarte entnommen werden könnten.

Ich habe der Petentin mitgeteilt, daß die Lohnsteuerkarte für diese Zwecke ungeeignet sei, da sie die *Freibeträge* für Kinder ausweise. Nach den Steuergesetzen seien die Voraussetzungen für die Eintragung von Kinderfreibeträgen - dies könnten auch *halbe* Kinderfreibeträge sein - andere als nach § 29 BAT-O für die Berücksichtigung von Kindern bei der Bemessung des Ortszuschlags. Wegen der unterschiedlichen Voraussetzungen sei die Anzahl der eingetragenen Kinderfreibeträge nicht identisch mit der Anzahl der im Ortszuschlag zu berücksichtigenden Kinder.

5.1.6 Landeseinheitlicher Vordruck für den Bereich Reisekosten

Das SMF hat mich an der Überarbeitung der Vordrucke beteiligt. Ich habe angeregt, bei Durchführung einer Dienstreise mit dem eigenen Pkw auf die Angabe des amtlichen Kennzeichens sowie der genauen Hubraumgröße zu verzichten, da sie reisekostenrechtlich nicht erforderlich sind. Das amtliche Kennzeichen ist künftig nicht mehr anzugeben und die Hubraumgröße nur noch in den nach Reisekostenrecht relevanten Kategorien von "bis 600 cm^3" (z. B. Fiat Cinquecento) und "von mehr als 600 cm^3".

5.1.7 Verwendung datenschutzgerechter Personalbögen

Mehrere Anfragen sächsischer Behörden und eigene Kontrollen von Personalstellen veranlassen mich, erneut auf die Verwendung des datenschutzgerechten und mit mir abgestimmten Personalbogens zu dringen.
Gemäß § 31 Abs. 1 SächsDSG dürfen öffentliche Stellen Daten von Bewerbern oder Beschäftigten nur verarbeiten, soweit dies zur Eingehung, Durchführung oder Beendigung des Dienst- oder Arbeitsverhältnisses erforderlich ist oder ein Gesetz, ein Tarifvertrag oder eine Dienstvereinbarung dies vorsieht. Dies gilt auch für Daten Dritter, denen Rechte aus dem Dienst- und Arbeitsverhältnis zustehen.
Ich habe festgestellt, daß mit Personalbögen, die wohl aus den alten Bundesländern stammen, nicht erforderliche Daten des Bewerbers/Bediensteten und dessen Familienangehöriger erhoben werden. Zum Beispiel gehen die Fragen nach dem Tag der Eheschließung und Ehescheidung, nach Ehegattendaten, Namen und Geburtsdaten der Kinder (Geburtsjahr ist zulässig, soweit für Ortszuschlag oder Kindergeld erforderlich), Vor- und Familiennamen des Vaters sowie Vor- und Geburtsnamen der Mutter über das erforderliche Maß hinaus. Nicht erforderliche Daten dürfen nicht erhoben und erst recht nicht gespeichert oder sonst verarbeitet werden. In den beanstandeten Fällen habe ich darum gebeten, die zuviel erhobenen Daten zuverlässig zu löschen (z. B. durch Schwärzen), den beanstandeten Personalbogen nicht mehr zu verwenden und das erforderliche Löschungsprotokoll mir nach Vollzug der Maßnahme zu übersenden.
Ich hielte es für hilfreich, wenn das SMI den datenschutzgerechten Personalbogen in geeigneter Weise (z. B. als Verwaltungsvorschrift) publik machen würde.

5.1.8 Frage nach nicht rechtswidriger Sterilisation und nicht rechtswidrigem Schwangerschaftsabbruch

Die staatlichen Dienststellen sind verpflichtet, die Bezügestelle u. a. über Beginn, Ende und Grund der Arbeitsunfähigkeit zu unterrichten. Hierzu dient eine vom SMF vorgeschriebene "Mitteilung der Arbeitsunfähigkeit von BAT-O-Angestellten" (§ 37 Abs. 1 BAT-O). Bei dem Grund der Arbeitsunfähigkeit sind zwei Kästchen vorgesehen, die entweder bei Krankheit oder bei Unfall anzukreuzen sind. Im Falle von Krankheit wird auf folgende Fußnote verwiesen:

"*Einschließlich nicht rechtswidriger Sterilisation und nicht rechtswidrigem Abbruch der Schwangerschaft bei einer Dauer der Arbeitsunfähigkeit bis zu 6 Wochen*".

Aufgrund dieser Fußnote ist es vorgekommen, daß öffentlich-rechtliche Arbeitgeber bei Krankmeldungen die Arbeitnehmerinnen befragten, ob der Grund des Fernbleibens vom Dienst eine Sterilisation oder ein Schwangerschaftsabbruch war. Eine solche Frage, die ggf. sogar in eine Selbstbezichtigung münden kann, halte ich für nicht hinnehmbar.

Hierauf habe ich das SMF hingewiesen und um Vorschläge gebeten, wie dem Recht auf informationelle Selbstbestimmung der Betroffenen Rechnung getragen werden kann (etwa durch Umgestaltung des Mitteilungsblatts).

Das SMF hat angeboten, künftig in der Fußnote lediglich auf § 37 Abs. 1 BAT-O hinzuweisen, wogegen ich keine Einwände hätte.

5.1.9 Erklärung über ausgeübte Nebentätigkeiten

Ein Beschäftigter des öffentlichen Dienstes bat mich um Auskunft über die Rechtmäßigkeit der von ihm verlangten Anzeige und Abrechnung *aller* Nebentätigkeiten. Sein Persönlichkeitsrecht sah er insbesondere durch die verlangte detaillierte Darlegung seiner Gewerkschaftsarbeit sowie der genehmigungsfreien Verwaltung des Privatvermögens beeinträchtigt.
Die abzugebenden Erklärungen hatten ihre Rechtsgrundlage in der SächsNTVO und waren insoweit nicht zu beanstanden. Gleichwohl war die Eingabe für mich Anlaß zu Kritik an der SächsNTVO, weil mit ihr in einem nicht mehr zu akzeptierenden Umfang in die Privatsphäre der Betroffenen eingegriffen wird.
Ich habe kritisiert, daß *alle* genehmigungs*freien* Nebentätigkeiten vor ihrer Aufnahme anzuzeigen sind, selbst wenn sie außerhalb der Dienstzeit ausgeübt werden, die Vergütungen nicht abzuliefern sind und Einrichtungen, Personal und Material des Dienstherren nicht in Anspruch genommen werden. Die Angabe von zeitlicher Beanspruchung, Auftraggeber und Höhe der Vergütung erlauben dem Dienstherren eine weitgehende Kontrolle der Privatsphäre der Bediensteten. Ob dies beabsichtigt war? Jedenfalls sah der Entwurf einer Verwaltungsvorschrift zu der SächsNTVO vor, daß es sich bei der Angabe der voraussichtlichen Vergütungshöhe "nicht lediglich um grobe Schätzungen handeln" dürfe und der Dienstvorgesetzte stichprobenweise zu prüfen habe, "ob die von den Bediensteten abgegebenen Anzeigen und Erklärungen den Tatsachen entsprechen ...".
Welchen Eingriff dies bedeutet, läßt sich am Beispiel der Verwaltung eigenen Vermögens zeigen (abgesehen vom gelegentlichen Gang zur Bank wegen kleiner Geldanlagen). Denn zu der nach § 83 Abs. 1 Nr. 2 SächsBG genehmigungsfreien Verwaltung des eigenen und des Familienvermögens gehören seine Erhaltung, Bewirtschaftung und Nutzung, z. B. die Vermietung und Verpachtung von Grundstücken und Räumen, die Nutzung der eigenen Eigentumswohnung oder des eigenen Einfamilienhauses, Verpachtung landwirtschaftlicher Flächen, Verwaltung von Aktien, Wertpapieren, Sparguthaben usw. (vgl. Keymer/Kolbe/Braun, Das Nebentätigkeitsrecht in Bund und Ländern, 1. Aufl. 1988, § 66 BBG Rdnr. 8). Damit würden Erträge oder geldwerte Vorteile in den genannten Beispielen der Vermögensverwaltung unter den weit auszulegenden Begriff "Vergütung" fallen und müßten vorab mit geschätzten Werten angezeigt und nach Ablauf des Kalenderjahrs sogar abgerechnet werden, wenn sie insgesamt 3.000,- DM überschreiten. Diese Grenze dürfte jede Vermietung von Wohnraum erreichen.

Da mit derart weitgehenden Anzeige-, Kontroll- und Abrechnungspflichten Datensammlungen ohne Bezug zum Dienst- oder Arbeitsverhältnis entstehen, habe ich folgende Änderungen der SächsNTVO gefordert:

1. Verzicht auf die Anzeige und Abrechnung von *genehmigungsfreien*, außerhalb der Dienstzeit ausgeübten Nebentätigkeiten, für deren Vergütungen keine Ablieferungspflicht besteht und bei deren Ausübung weder Einrichtungen noch Personal oder Material des Dienstherrn in Anspruch genommen werden.

2. Abrechnung und/oder Auskunft nur in bezug auf Vergütungen, die abzuliefern sind, weil sie die Höchstbeträge nach § 6 Abs. 3 SächsNTVO übersteigen oder weil das Nutzungsentgelt gemäß § 12 SächsNTVO nach der Bruttovergütung zu bemessen ist. Werden die Höchstbeträge für ablieferungspflichtige Vergütungen nicht überschritten, muß die einfache Erklärung des Beschäftigten darüber ausreichen.

3. Keine detaillierten Angaben über allgemein genehmigte Nebentätigkeiten von geringem Umfang. Auch hier dürfte eine einfache Mitteilung über die Art einer Nebentätigkeit von geringem Umfang ausreichen.

Das SMI hat meine Forderungen aufgegriffen und die SächsNTVO entsprechend geändert.

5.1.10 Einsichtnahme der Staatlichen Rechnungsprüfungsämter in Personalakten

Ein Landratsamt fragte, ob ein Staatliches Rechnungsprüfungsamt die Personalakten einsehen dürfe, wenn der Prüfauftrag "Prüfung der Jahresrechnungen 1990 bis 1993" laute. Die Zulässigkeit habe ich wie folgt beurteilt:

Die Staatlichen Rechnungsprüfungsämter führen als nachgeordnete Behörden des Sächsischen Rechnungshofs (§ 14 Abs. 1 Rechnungshofgesetz) ihre Prüfung nach Weisung des Rechnungshofs und nach Maßgabe der SäHO durch. Gemäß § 95 Abs. 1 SäHO sind ihnen auf Verlangen alle Unterlagen vorzulegen, die sie zur Aufgabenerfüllung *für erforderlich halten*. Nicht erforderliche Unterlagen dürfen demnach nicht verlangt werden.

Aufgabe und damit Prüfumfang ergeben sich aus dem Auftrag des Rechnungshofs (hier: Prüfung der Jahresrechnungen 1990 bis 1993). Zu diesem umfassenden Auftrag gehört auch die Prüfung der Personalverwaltung, wobei die Personalakten Aufschluß über die Rechtmäßigkeit von Eingruppierungen, Ernennungen usw. geben. Die Einsichtnahme der Prüfer in Personalakten ist daher *ohne* Zustimmung der betreffenden Beschäftigten zulässig.

5.1.11 Personalakteneinsicht durch einen beratenden Ausschuß des Kreistages

Immer wieder werde ich gefragt, unter welchen Voraussetzungen Ausschüssen Einsicht in Personalakten gewährt werden darf.

Gemäß § 24 Abs. 4 SächsLkrO kann ein Viertel der Kreisräte in *allen* Angelegenheiten des Landkreises u. a. verlangen, daß der Landrat dem Ausschuß *Akteneinsicht* gewährt. Insoweit ist die Landkreisordnung eine bereichsspezifische Vorschrift, die dem Sächsischen Datenschutzgesetz gemäß § 2 Abs. 4 SächsDSG *vorgeht.*

Das Akteneinsichtsrecht gilt im Rahmen des § 24 Abs. 3 SächsLkrO auch für Personalakten, und zwar, wie ich meine, uneingeschränkt.

Allerdings - und das sollte in der Geschäftsordnung geregelt werden - ist zu gewährleisten, daß die Akteneinsicht ausschließlich im Fachamt (hier Personalamt) zu erfolgen hat. Eine Herausgabe an die einzelnen Kreisräte - insbesondere z. B. der Versand der Akten oder von Kopien zur Sitzungsvorbereitung an die Privatanschriften - hat zu unterbleiben.

Empfehlenswert wäre auch eine Regelung in der Geschäftsordnung, daß die Akteneinsichtnahme möglichst auf einen kleinen Personenkreis zu begrenzen ist (z. B. je ein Verantwortlicher pro Fraktion), es sei denn, daß gewichtige Gründe eine Ausdehnung der Akteneinsichtsbefugnis erfordern.

Weiter muß gewährleistet sein, daß die Ausschuß-/Kreistagssitzungen in Personalangelegenheiten nichtöffentlich und die Kreisräte neben ihrer Verschwiegenheitspflicht (§ 33 Abs. 2 SächsLkrO) auch auf das Datengeheimnis (§ 6 SächsDSG) verpflichtet sind.

In den Sitzungsunterlagen selbst sollte grundsätzlich auf personenbezogene Daten verzichtet werden (z. B. durch Numerierung). Nach Sitzungsende sollten die Unterlagen eingesammelt und zuverlässig vernichtet werden.

Soweit vorstehende Voraussetzungen erfüllt sind, darf die Akteneinsicht datenschutzrechtlich gesehen gewährt werden. Sie darf sogar nicht verweigert werden, weil sonst die rechtlich gewährte Entscheidungskompetenz und Verantwortung der Ausschüsse beschnitten würde.

5.1.12 Einsichtgewährung in eine Personalakte durch einen Privatdetektiv

Der Presse war zu entnehmen, daß der Präsident einer Handwerkskammer einen Privatdetektiv mit der Bespitzelung einer unliebsamen Mitarbeiterin beauftragt habe. Die Zeitungsmeldungen ließen vermuten, daß dem Detektiv Einsicht in die Personalakte der Beobachteten gewährt worden war.

Meine Ermittlungen bei der Handwerkskammer bestätigten den Verdacht. Der Handwerkskammerpräsident hatte veranlaßt, daß dem Detektiv entgegen § 31 Abs. 2 SächsDSG Einsicht in die Personalakte gewährt wurde. Eine solche Datenübermittlung an einen Privaten wäre nur auf gesetzlicher Gundlage oder mit Einwilligung der Betroffenen zulässig gewesen. Keine dieser Voraussetzungen war gegeben, so daß von einer Ordnungswidrigkeit durch den Präsidenten ausgegangen werden mußte (§ 32 Abs. 1 Buchst. a SächsDSG).

Ich habe die zuständige Bußgeldbehörde unterrichtet und die Vorgehensweise des Handwerkskammerpräsidenten beanstandet.

5.1.13 Aushändigung der Personalakte nach Beendigung des Beschäftigungsverhältnisses?

Ein Petent hatte nach seinem Ausscheiden aus dem öffentlichen Dienst die *Aushändigung* seiner Personalakte verlangt. Da ihm dies verweigert worden war, bat er mich um Unterstützung. Ich habe ihm dazu folgendes mitgeteilt:

Arbeitnehmer und Beamte haben keinen Rechtsanspruch auf Herausgabe ihrer Personalakten bei Beendigung des Beschäftigungs- bzw. Beamtenverhältnisses. Der Grund liegt zum einen darin, daß der Arbeitgeber bzw. Dienstherr Eigentümer der Personalakten ist. Zum anderen sind Personalakten für den Dienstgebrauch bestimmt und unterliegen nach ihrem Abschluß einer fünfjährigen Aufbewahrungsfrist.

Die Personalakte eines Arbeiters oder Angestellten wird mit Ablauf des Jahres als abgeschlossen angesehen, in dem der Arbeitnehmer das 65. Lebensjahr vollendet hat - selbst, wenn er schon vorher ausgeschieden ist. Bei Beamten ist sie erst mit Wegfall der letzten Versorgungsverpflichtung abgeschlossen oder - beim Ausscheiden *ohne* Versorgungsbezüge - mit Ablauf des Jahres, in dem das 65. Lebensjahr vollendet wird (§ 123 SächsBG).

Auch nach Ablauf der Aufbewahrungsfrist können die öffentlichen Stellen nicht frei über die Personalakten verfügen. Vielmehr verpflichtet sie das SächsArchG, die Akten dem Hauptstaatsarchiv anzubieten. Lehnt dieses die Übernahme ab, sind die Personalakten zu vernichten, wobei die Aushändigung der Personalakte an den Betroffenen nicht als Alternative vorgesehen ist.

(Zum *Einsichtsrecht* in Personalakten nach Beendigung des Beschäftigungsverhältnisses s. 2. Tätigkeitsbericht Nr. 5.1.5 und 3. Tätigkeitsbericht Nr. 5.1.17)

5.1.14Regelbeurteilung von Angestellten

Eine Stadt bat mich um Stellungnahme zu dem Entwurf einer Beurteilungsrichtlinie für die Angestellten.

Ich habe es als problematisch angesehen, daß außer den Beamten auch die Arbeitnehmer (Angestellte und Arbeiter) beurteilt werden sollten. Denn gemäß § 31 Abs. 1 SächsDSG dürfen öffentliche Stellen Daten von Beschäftigten nur verarbeiten, soweit dies zur Eingehung, Durchführung oder Beendigung des Dienst- oder Arbeitsverhältnisses erforderlich ist oder ein Gesetz, ein Tarifvertrag oder eine Dienstvereinbarung dies vorsieht, wobei das geltende Recht den Rahmen für jede Dienstvereinbarung vorgibt.

Die dienstliche Beurteilung der Beamten hat ihre Rechtsgrundlage in § 115 SächsBG und der dazu ergangenen SächsBeurtVO. Dazu findet sich keine Entsprechung in den Tarifverträgen für die Angestellten. Auch wenn die Tarifverträge Beurteilungen nicht entgegenstehen, habe ich erhebliche Zweifel an der Erforderlichkeit von *Regelbeurteilungen* für Angestellte geäußert, weil das Beurteilungsergebnis keinen Einfluß auf das vertragliche Arbeitsverhältnis hat. Ein- oder Höhergruppierung, Fallgruppen- oder Bewährungsaufstieg usw. sind an völlig andere Voraussetzungen geknüpft als an ein bestimmtes Beurteilungsergebnis. Eine Erforderlichkeit könnte sich allenfalls im Zusammenhang mit einem Personalentwicklungskonzept ergeben. Solange ein solches nicht vorliegt, sind Regelbeurteilungen bei Nichtbeamten bedeutungslos und damit nicht erforderlich.

Der Wunsch, bei hausinternen Bewerbungen um höherwertige Dienstposten auch bei Angestellten auf Beurteilungen zurückgreifen zu können, um die Chancengleichheit gegenüber konkurrierenden Beamten zu wahren, ist kein Argument. In diesem Fall könnten *Anlaßbeurteilungen* erstellt werden.

5.1.15 Inhalt von Dienstzeugnissen

Ein im öffentlichen Dienst beschäftigter Arbeitnehmer fragte, welche Beschäftigtendaten das bei Beendigung seines Dienstverhältnisses zu erteilende Dienstzeugnis enthalten darf.

Aus dem Zeugnis dürfen nur diejenigen Daten ersichtlich sein, die zur Beurteilung seiner dienstlichen Leistungen erforderlich sind (vgl. § 31 Abs. 1 SächsDSG). Hierbei ist wie folgt zu differenzieren (vgl. § 630 BGB):

Fordert der Arbeitnehmer ein sogenanntes "einfaches Zeugnis", darf dieses folgende Angaben enthalten:
- Name des Arbeitnehmers (Anschrift und Geburtsdatum nur mit seinem Einverständnis)
- Art, Anfang und Ende der Beschäftigung
- Ausstellungsdatum.

Verlangt der ausscheidende Arbeitnehmer hingegen ein sogenanntes "qualifiziertes Zeugnis", muß zusätzlich eine Bewertung der Leistung des Arbeitnehmers erfolgen. Welche Eigenschaft der Dienstherr im einzelnen (positiv oder negativ) hervorheben will, steht in seinem (pflichtgemäßen) Ermessen. Daher ist es nicht möglich, abschließend festzulegen, welche Daten er in das Zeugnis aufnehmen darf. Zu beachten ist aber stets die Wahrheitspflicht, die Vollständigkeit und der Grundsatz der Erforderlichkeit.

5.1.16 Bekanntgabe der Prüfungsergebnisse der Laufbahnprüfung für den gehobenen Forstdienst

Durch das SML wird gegenwärtig eine Ausbildungs- und Prüfungsordnung für den gehobenen Forstdienst erarbeitet. Eine Regelung zur Veröffentlichung der Namen der Prüflinge, die die Laufbahnprüfung für den gehobenen Forstdienst bestanden haben, *ist nicht vorgesehen.*
Dafür soll in einem internen Informationsblatt (Mitarbeiterzeitung) die *Zahl* derer, die die Prüfung bestanden haben, veröffentlicht werden. Dagegen hätte ich keine Bedenken.
Ich habe aber festgestellt, daß in der genannten Mitarbeiterzeitung unter "Personalnachrichten" die Assessoren namentlich genannt werden, die künftig in der Sächsischen Landesforstverwaltung eingesetzt werden sollen. Das ist nach § 31 Abs. 1 und 2 SächsDSG ohne gesetzliche Grundlage und ohne Einwilligung der Betroffenen unzulässig. Ich habe das SML gebeten, künftig keine derartigen personenbezogenen Daten mehr zu veröffentlichen; es sei denn, die Betroffenen haben gem. § 4 Abs. 1 Nr. 2, Abs. 2 und 3 SächsDSG eingewilligt. Ich gehe davon aus, daß mir im Frühjahr 1996 der Entwurf der Ausbildungs- und Prüfungsordnung für den gehobenen Forstdienst zur Stellungnahme zugeleitet wird.

5.1.17 Behördliche Telefonverzeichnisse im Internet?

Eine Hochschule fragte an, ob sie ihr Telefonverzeichnis ins Internet (World-Wide-Web-Seiten) einstellen dürfe. Ich teilte der Hochschule mit, daß nach § 31 Abs. 1 Satz 1 SächsDSG sächsische öffentliche Stellen Beschäftigtendaten nur verarbeiten dürfen, soweit dies zur Eingehung, Durchführung oder Beendigung des Dienst- oder Arbeitsverhältnisses *erforderlich* ist oder ein Gesetz, ein Tarifvertrag oder eine Dienstvereinbarung dies vorsieht. Die Übermittlung von Beschäftigtendaten an

Personen oder Stellen *außerhalb* des öffentlichen Bereichs ist nur auf *gesetzlicher Grundlage oder mit Einwilligung* der Betroffenen zulässig (§ 31 Abs. 2 Satz 1 SächsDSG).

Behördliche Telefonverzeichnisse sind "nur für den Dienstgebrauch" vorgesehen. Ohne Einwilligung aller Betroffenen (vgl. § 4 Abs. 1 Nr. 2, Abs. 2 und 3 SächsDSG) wäre die Veröffentlichung auf World-Wide-Web-Seiten *unzulässig*.

5.1.18 Dezentralisierung des Personalwesens

In meinem 2. Tätigkeitsbericht (Nr. 5.1.15) habe ich bereits kritisch darauf hingewiesen, daß es in den sächsischen Großstädten üblich sei, das Personalwesen einschließlich der Personalaktenführung zumindest in den größeren Ämtern in Eigenregie bearbeiten zu lassen. Der jeweilige Amtsleiter ist (gleichzeitig) Fachvorgesetzter der Bediensteten des Amtes sowie der Personalsachbearbeiter und befugt, in gewissem Umfang Personalentscheidungen zu treffen, ohne daß das eigentliche Personalreferat beteiligt wird.

Meinen Vorschlag, die Personalsachbearbeitung in den einzelnen Fachämtern organisatorisch dem Personalreferat zuzuordnen und damit der Kompetenz des jeweiligen Amtsleiters zu entziehen (z. B. um Interessenkollisionen zu vermeiden), wurde nicht bzw. nur zögerlich gefolgt.

Das Festhalten an dieser (wohl DDR-historisch bedingten) Verfahrensweise wird heute pauschal damit gerechtfertigt, daß die beabsichtigte Einführung des von der KGSt proklamierten "neuen Steuerungsmodells" Kompetenzverschiebungen und Dezentralisierungen erforderlich mache und deshalb von einem zentralen Personalwesen im eigentlichen Personalreferat künftig abgesehen werden solle. Das ist so nicht einmal ansatzweise überzeugend.

Dennoch werde ich diese Problematik mit den Datenschutzbeauftragten des Bundes und der Länder erörtern.

5.1.19 Einführung automatisierter Verfahren der Arbeitszeiterfassung (elektronische Zeiterfassungsgeräte)

In den Verwaltungen wird die Arbeitszeit mehr und mehr durch elektronische Zeiterfassungssysteme aufgezeichnet. Im Berichtszeitraum wurde ich gemäß § 31 Abs. 7 SächsDSG an der Einführung einer Vielzahl von automatisierten Verfahren der Arbeitszeiterfassung beteiligt, zu denen ich meine Stellungnahme abgegeben habe.
Weil in den mir vorgelegten Verfahrenskonzepten vielfach die von mir im 1. Tätigkeitsbericht (5.1.12) gegebenen umfassenden Hinweise nicht ausreichend beachtet worden waren, sei im folgenden auf einige Schwerpunkte noch einmal hingewiesen:

Durch die Verwendung leistungsfähiger Hard- und Software und der Speicherung personenbezogener Daten ist eine verhaltenskontrollierende Auswertung der Zeitwertdaten, bezogen auf den einzelnen Mitarbeiter oder eine Mitarbeitergruppe, möglich (tägliches Zeitkonto, Verletzung von Kernzeiten, Überziehen von Pausen, unentschuldigtes Fehlen, Fehlzeiten nach Abwesenheitsgründen wie Urlaub und Krankheit). Die Gewohnheiten der Mitarbeiter können danach exakt nachvollzogen werden. Ich habe in meinen Stellungnahmen deshalb besonderen Wert darauf gelegt, daß für solche Verfahren die *zulässigen Nutzungszwecke* der Daten und die Personen, die diese Nutzung vornehmen dürfen, in den Dienstvereinbarungen abschließend und genau festgelegt werden.

Datenschutzrechtliche Bedenken gegen Auswertungen, die der Durchführung der *Dienstaufsicht* dienen oder zu Kontrollzwecken (z. B. der Datensicherheit) angefertigt werden, gibt es nach meinem Dafürhalten dann nicht, wenn sie zweckgebunden und mit dem Grundsatz der Erforderlichkeit des § 31 Abs. 1 SächsDSG zu vereinbaren sind. Dies ist bei Auswertungen über Beschäftigte, die unbegründet die Kernzeit verletzen oder die zulässige Zeitschuld überschreiten, stets der Fall. Bewegt sich der Beschäftigte innerhalb des zulässigen Zeitrahmens, ist eine Verhaltenskontrolle durch Vorgesetzte nicht erforderlich und daher unzulässig. Ich habe deshalb in meinen Stellungnahmen immer darauf hingewiesen, daß die Auswertungen für Zwecke der Dienstaufsicht durch Vorgesetzte auf die Kernzeitverletzer und Überschreitungen der zulässigen Minuszeit zu begrenzen sind.

In einigen Fällen haben sich sächsische Behörden im Zusammenhang mit der Einführung von automatisierten Arbeitszeiterfassungsverfahren auf die *zweijährige* Aufbewahrungspflicht der aufzeichnungspflichtigen Arbeitszeit nach § 16 Abs. 2 ArbZG - das für die Arbeitnehmer gilt - berufen. Das SMF, in dessen Zuständigkeit die Arbeitszeitregelung für Arbeitnehmer im öffentlichen Bereich liegt, hat angekündigt, daß im Interesse einer einheitlichen Aufbewahrung und Löschung von Arbeitszeitdaten die für die Beamten geltende Sächsische Arbeitszeitverordnung (SächsAZVO) gemäß § 19 ArbZG auf den Arbeitnehmerbereich übertragen werde. Damit wird für Arbeitszeitdaten einheitlich die maximale *Aufbewahrungsdauer* von *sechs Monaten* gelten, die ich in meinen Stellungnahmen zu den mir angezeigten Verfahren fordere.

5.1.20 Umsetzung der "Richtlinien zur Neuregelung der Eingruppierung der angestellten Lehrer"

Zwei Bezirkspersonalräte für Grund-, Mittel- und Förderschulen trugen mir ihre datenschutzrechtlichen Bedenken gegen eine im Herbst 1995 durch das SMK gestartete umfangreiche Datenerhebungsaktion im Zusammenhang mit einer rückwirkenden Höhergruppierung der Lehrer unterer Klassen (LuK) im gesamten Grundschulbereich vor.

Insbesondere bemängelten sie, daß sich die Datenerhebungen durch die Oberschulämter auch auf Lehrer erstreckten, bei denen zum damaligen Zeitpunkt keine Veränderung der Eingruppierung erfolgen konnte. Ebenso seien die verlangten Erklärungen bezüglich ggf. bei den Arbeitsgerichten anhängiger Klagen auf rückwirkende Höhergruppierung mit dem Erforderlichkeitsgrundsatz nicht zu vereinbaren (in der Tat machte das SMK die rückwirkende Höhergruppierung der Grundschullehrer zum 1. Januar 1995 von der Rücknahme einer ggf. eingereichten arbeitsgerichtlichen Klage bzw. von der Erklärung, daß keine Klage erhoben worden sei, abhängig).

In einer umfangreichen Stellungnahme versuchte das SMK die Aktion als erforderlich zu rechtfertigen. Dieser Stellungnahme entnahm ich im wesentlichen folgendes:

1. Sämtliche LuK - mit Ausnahme derer, die ihre Klage nicht zurückgenommen haben - wurden rückwirkend zum *1. Januar 1995* in die Vergütungsgruppe IV a BAT-O eingruppiert.
2. Die LuK, die ihre Klage nicht zurückgenommen haben, wurden rückwirkend zum *1. Juli 1995* in die Vergütungsgruppe IV a BAT-O eingruppiert, also augenscheinlich benachteiligt.

Dem SMK habe ich daher mitgeteilt: "Der enorme Verwaltungsaufwand, der nach Ansicht des SMK bei der Umsetzung des BAG-Urteils vom 20. April 1994 erforderlich war, um den unter 2. genannten Personenkreis von der rückwirkenden Eingruppierung zum 1. Januar 1995 auszugrenzen, war unverhältnismäßig. Vielmehr hätte man (ohne die umfangreichen Datenerhebungen usw.) die Nachzahlung der Bezüge rückwirkend ab 1. Januar 1995 *sämtlichen* LuK (unabhängig davon, ob geklagt wurde oder nicht; unabhängig davon, ob die Klage zurückgenommen wurde oder nicht) unter dem *Vorbehalt der Rückforderung* gewähren können (müssen).
Die Eingruppierung erfolgt nämlich ausschließlich nach den Tätigkeitsmerkmalen des BAT-O und bleibt unbeeinflußt von Vereinbarungen mit Berufsverbänden u. ä. Sie ist vor allem nicht vom Wohlverhalten (Klage, Nicht-Klage, Klagerücknahme) der Betroffenen abhängig.
Die Anwendung von Kriterien außerhalb des BAT-O, die zur Ungleichbehandlung der Betroffenen geführt hat, war ebenso rechtswidrig wie die damit zusammenhängenden Datenerhebungen, bei denen der Erforderlichkeitsgrundsatz des § 31 Abs. 1 SächsDSG nicht beachtet wurde."

Außerdem habe ich das SMK aufgefordert, die anläßlich der Aktion entstandenen Listen zu vernichten.

5.1.21Umgang mit Beschäftigtendaten im SMWK

Mehrere Beschäftigte aus dem Zuständigkeitsbereich des SMWK haben sich im Berichtszeitraum über angebliche Verstöße im Umgang mit Beschäftigtendaten beschwert.

Beispielsweise wurden durch einen SMWK-Bediensteten in amtlicher Eigenschaft in einem Leserbrief Einzelheiten einer einem Hochschullehrer gegenüber ausgesprochenen Kündigung veröffentlicht, ohne daß dafür die Befugnis gemäß § 80 SächsBG bestanden hätte. In einem anderen Fall wurde durch den Leiter einer dem SMWK nachgeordneten Einrichtung das Personal durch eine "Hausmitteilung" über die angebliche Stasi-Belastung einer gekündigten Mitarbeiterin unterrichtet. Außerdem hatte das SMWK die vor einer solchen Kündigung erforderliche Anhörung unterlassen. Ein weiterer Petent beschwerte sich, daß das SMWK eine ihm gegenüber nicht eröffnete Beurteilung in ein Verwaltungsgerichtsverfahren, das der Freistaat Sachsen gegen einen Dritten führt, eingebracht habe. Dieser Dritte wiederum machte geltend, daß das SMWK letztendlich dafür verantwortlich sei, daß Informationen über ihn betreffende Personalmaßnahmen an die Presse sowie andere unbeteiligte Privatpersonen gelangt seien.

Unabhängig davon, welcher Unrechtsgehalt sich in den einzelnen Fällen herausstellen wird, die ich noch aufzuklären habe, kann schon jetzt festgestellt werden, daß an die Stelle der anfänglichen dilatorischen Sachbehandlung eine erfreulich kooperative Haltung des SMWK getreten ist. Ich führe dies u. a. auf ein Gespräch mit dem zuständigen Staatsminister zurück.

5.1.22 Behandlung von Personaldaten bei der Landesversicherungsanstalt (LVA) Sachsen

Ein Petent teilte mir mit, daß bei der LVA Sachsen ein Dossier über ihn existiere, obwohl er kein Mitarbeiter dieser Behörde sei. Des weiteren unterrichtete er mich über die Existenz von "Rotbüchern", in denen Persönlichkeitsprofile von LVA-Mitarbeitern enthalten seien. Diese Unterlagen seien von einem im Ausland (Schweiz) ansässigen Unternehmensberater im Auftrag des inzwischen amtsenthobenen Geschäftsführers erstellt worden.

Meine Überprüfung ergab, daß in der Tat in der geschilderten eklatanten Weise gegen §§ 117 ff. SächsBG, §§ 11, 31 SächsDSG und die SächsBeurtVO verstoßen worden war.

Insbesondere wurde ohne Rechtsgrundlage eine Eignungsanalyse des Petenten durch den Schweizer Unternehmensberater erstellt und zu den Akten genommen. Das gleiche gilt für die Eignungsanalysen der anderen LVA-Mitarbeiter, deren Persönlichkeitsprofile sich in den "Rotbüchern" wiederfinden.

Bedauerlich ist, daß nicht mehr festgestellt werden konnte, wieviele Exemplare der "Rotbücher" erstellt wurden und wer die Empfänger gewesen sind. Auch kann im nachhinein nicht mehr festgestellt werden, ob der Unternehmensberater Personaldaten der LVA in seinem Unternehmen in der Schweiz aufbewahrt.

Der Geschäftsführer der LVA wurde aus diesem und anderen Gründen abgelöst.

5.1.23 Kontrolle von Leistung und Verhalten kommunaler Vollzugsbediensteter - möglicherweise als Statistik?

Der behördliche Datenschutzbeauftragte einer Stadt bat mich um Stellungnahme zu der Frage, ob es zulässig sei, daß der Leiter der Bußgeldstelle eine bisher manuell geführte personenbezogene "Monatsabrechnung" pro Mitarbeiter nunmehr auf PC führen dürfe: Die Bediensteten sollten unter Namensnennung Angaben über geleistete Arbeitszeiten, Fehlzeiten und die Anzahl der von ihnen eingeleiteten Abschleppmaßnahmen, unterschieden nach Fällen von Falschparken, Sicherstellungen oder anderem mehr, machen.

In meiner Stellungnahme habe ich klargestellt, daß nach § 31 Abs. 1 SächsDSG öffentliche Stellen Beschäftigtendaten nur verarbeiten dürfen, soweit dies zur Eingehung, Durchführung oder Beendigung des Dienst- oder Arbeitsverhältnisses *erforderlich* ist oder ein Gesetz, ein Tarifvertrag oder eine Dienstvereinbarung dies vorsieht. Traditionsgemäß erfolgt die Verarbeitung von Beschäftigtendaten in der personalverwaltenden Stelle (und nicht in der Bußgeldstelle).

Für die Datenerhebung, die mit der "Monatsabrechnung" erfolgt, vermochte ich weder für das bisherige manuelle noch für das beabsichtigte automatisierte Verfahren zu erkennen, daß die Voraussetzungen des § 31 Abs. 1 SächsDSG erfüllt sind. Ich hielt die "Monatsabrechnung" für ein Instrument zur (sogar lückenlosen!) Leistungs- und Verhaltenskontrolle durch den Leiter der Bußgeldstelle, das geeignet ist, ständigen Überwachungsdruck auf die Vollzugsbediensteten auszuüben und das deshalb unter Mißachtung des Übermaßverbots in unverhältnismäßiger Weise in deren Persönlichkeitsrecht eingreift. Dieser dauernde Leistungsdruck bleibt nicht ohne (negative) Folgen auf das dienstliche Verhalten der Politessen und ihrer Kollegen.

Ich lehnte die beabsichtigte *automatisiert* zu führende "Monatsabrechnung" im Vollzug des § 31 Abs. 7 SächsDSG ab (daran könnte auch eine eventuelle Zustimmung des Personalrates im Rahmen eines Mitbestimmungsverfahrens nach § 80 Abs. 3 Nr. 16 SächsPersVG nichts ändern).

Außerdem zog ich in Erwägung, die Bußgeldstelle wegen der unter Mißachtung von §§ 11 Abs. 2, 31 Abs. 1 SächsDSG erstellten *manuellen* "Monatsabrechnungen" zu beanstanden, falls das Verfahren nicht unverzüglich eingestellt würde und die erforderliche sofortige Löschung (Vernichtung) der bisher entstandenen Vorgänge unterbleiben sollte.

Dem Leiter der Bußgeldstelle leuchteten meine Argumente nur bedingt ein, und er wollte nunmehr die geplante Datensammlung in etwas geänderter Form, nämlich ohne Auswertung der persönlichen Leistungsdaten der einzelnen Beschäftigten, durchführen, zu rein statistischen Zwecken.

Ihm war dabei offensichtlich nicht bewußt, daß er damit in den Anwendungsbereich des Sächsischen Statistikgesetzes geriet (vgl. § 2 Abs. 1 Nr. 4 SächsStatG), also eines datenschutzrechtlichen Spezialgesetzes: Gemäß § 8 Abs. 1 Satz 2 i. V. m. § 6 Abs. 6 SächsStatG bedarf eine Gemeinde (oder eine andere kommunale Körperschaft, vgl. § 8 Abs. 4 SächsStatG) für statistische Erhebungen einer Satzung als Ermächtigungsgrundlage, und außerdem darf eine kommunale Statistik gemäß § 9 Abs. 1 Satz 1 SächsStatG nur von einer die besonderen gesetzlichen Voraussetzungen erfüllenden kommunalen Statistikstelle durchgeführt werden.

Von diesen im vorliegenden Falle offensichtlich nicht erfüllten Voraussetzungen befreit wäre die geplante statistische Erhebung nur, wenn sie als sog. *Statistik im Verwaltungsvollzug* gemäß § 2 Abs. 1 Nr. 5, § 7 Abs. 1 SächsStatG durchgeführt würde. Das aber setzt voraus:

- Erhoben (gesammelt) werden dürfen die Daten nur aus Unterlagen, die zu nicht-statistischen Zwecken ohnehin angefallen sind; also aus Unterlagen, die ausschließlich zu dem Zweck der Durchführung von Verwaltungsverfahren und ähnlichen Vorgängen angefertigt worden sind, an der die betreffenden Bediensteten beteiligt gewesen sind, und außerdem noch aus denjenigen Unterlagen, die zum Zwecke der erlaubten Leistungskontrolle angefallen sind, also aus Stechkarten oder dergleichen.
- Die Daten dürfen gerade nicht bei denjenigen Personen erhoben werden, auf die sie sich beziehen, also bei den gemeindlichen Vollzugsbediensteten. Von diesen dürfen keinerlei für die Zwecke der in Frage stehenden - eben statistischen - Datensammlung zu machende Angaben verlangt werden.
- Die Daten sind von derjenigen Stelle zu sammeln (und aufzubereiten), welche die Unterlagen, aus denen sie gewonnen werden, rechtmäßig - nämlich zum Zwecke der Erfüllung ihrer nicht-statistischen Aufgaben - hat, d. h. zumindest vorübergehend aufbewahrt.

Bei allem gilt das statistikrechtliche Gebot der frühestmöglichen Anonymisierung, d. h. einer den Personenbezug ausschließenden Zusammenführung der Daten, die so früh erfolgt, wie dies ohne Beeinträchtigung des statistischen Erkenntniszweckes (hier: Gesamtübersicht über Arbeitszeit und über Anzahl von Verwaltungsvorgängen bestimmter Art) möglich ist.

Konkret bedeutet dies insbesondere, daß bei der Datenerhebung aus den für die Durchführung der Verwaltungsvorgänge angelegten Unterlagen Namen der durchführenden Bediensteten von vornherein nicht erfaßt werden dürfen.

Ich werde den Fortgang der Angelegenheit weiter verfolgen.

5.1.24 Datenschutzrechtliche Kontrolle der Personalverwaltung einer Stadt

Bei der Kontrolle habe ich neben einer Reihe datenschutzgerechter Maßnahmen auch folgende Mängel festgestellt:

Aktenführung und Aktenverwaltung
Vermerke über Personalgespräche wurden in gesonderten Ordnern gesammelt, obwohl alle Unterlagen, die in einem unmittelbaren inneren Zusammenhang mit dem Dienst- oder Arbeitsverhältnis eines Beschäftigten stehen, materieller Bestandteil der Personalakte sind. Die betreffenden Vermerke wurden daraufhin zu den Personalakten genommen.

Verpflichtung auf das Datengeheimnis
Nicht alle Beschäftigten waren auf das Datengeheimnis verpflichtet worden. Ein Grund lag in der Weigerung von Mitarbeitern, sich auf das Datengeheimnis verpflichten zu lassen, ein anderer in der ungeklärten Frage, ob auch Beschäftigte, die ausschließlich mit "Firmendaten" in Berührung kommen, personenbezogene Daten verarbeiten. Zivildienstleistende wurden nicht verpflichtet, weil die Verwaltungsanweisungen des Bundesamtes für den Zivildienst dies nicht ausdrücklich vorsehen würden.

Ich habe deutlich gemacht, daß sämtliche Personen mit Zugang zu personenbezogenen Daten auf das Datengeheimnis zu verpflichten sind. Dies ist mit wenigen Ausnahmen (z. B. Stadtgärtner, Stadtreinigungspersonal) in der Regel das gesamte Personal. Auch Beschäftigte, die nur mit Firmen zu tun haben (z. B. Hochbauamt), haben insoweit Zugang zu personenbezogenen Daten, denn Ausschreibungsangebote, mangelhaft erbrachte Leistungen, Preisnachlässe enthalten letztlich personenbezogene Daten der Firmeninhaber. Zivildienstleistende bilden keine Ausnahme im Kreis der zu Verpflichtenden, weil die Verschwiegenheitspflicht nach § 28 ZDG die unbefugte Datenverarbeitung nach § 6 SächsDSG nicht abdeckt. Ich habe in allen Fällen gefordert, unterbliebene Verpflichtungen nachzuholen.

Abfindungslisten für die Kämmerei
Für Zwecke der Haushaltsführung war der Kämmerei vom Personalamt eine *namentliche* Aufstellung über die an ausgeschiedene Mitarbeiter gezahlten Abfindungen zugeleitet worden. Für finanzwirtschaftliche Zwecke hätte die Mitteilung der Abfindungs*summe* gereicht. Die in der Kämmerei vorhandenen namentlichen Aufstellungen wurden vernichtet und durch geeignete Unterlagen ohne Personenbezug ersetzt.

Automatisierte Verarbeitung von Beschäftigtendaten
Die Beschäftigtendaten werden in einem Personalinformationssystem, im Rahmen der Arbeitszeiterfassung sowie der Lohn- und Gehaltsabrechnung automatisiert verarbeitet. Obwohl dies nach § 31 Abs. 7 SächsDSG nur im Benehmen mit dem Sächsischen Datenschutzbeauftragten zulässig ist, bin ich nicht rechtzeitig unterrichtet worden. Aufgrund unvollständiger Unterlagen konnte das Benehmen noch nicht für alle

Verfahren hergestellt werden.

Altdaten
§ 35 Abs. 2 SächsDSG verpflichtet öffentliche Stellen, dem Sächsischen Datenschutzbeauftragten bis zum 31. März 1992 ein Verzeichnis über vorhandene Datenbestände aus DDR-Zeiten (Altdaten) vorzulegen. Dies hatte die Stadt versäumt, obwohl zumindest Kaderakten und Personalkarteien vorhanden waren. Das Verzeichnis wurde nachgereicht.

Datensicherheit
Doppel von Lohn- und Gehaltsabrechnungen wurden in offenen Regalen und ausgemusterten Schlafzimmerschränken einfachster Ausführung gelagert. Die Zimmertüren mit ihren Glasfüllungen und den von außen abschraubbaren Sicherheitsschlössern gewährleisteten keine Datensicherheit. Sobald es die Haushaltslage zuläßt, soll Abhilfe geschaffen werden.

Für Schreiben in Personalangelegenheiten und die Arbeit mit dem Personalinformationssystem steht der Personalstelle ein Einzelplatz-PC zur Verfügung, auf den die Bearbeiter unter ein und demselben Paßwort zugreifen können. Dies ist bei der hohen Schutzstufe von Personaldaten keine ausreichende Sicherheitsmaßnahme, so daß ich die Installation von Sicherheits-Software empfohlen habe. Für die sofortige Vernichtung von Schriftstücken (z. B. überarbeitete Entwürfe oder fehlerhafte Ausdrucke) habe ich angeregt, einen Reißwolf anzuschaffen, der von jedem Bediensteten unmittelbar bedient wird.

Personalkarte
Für jeden Beschäftigten wird außerhalb des automatisierten Personalinformationssystems eine Personalkarte geführt, die u. a. nicht erforderliche Angaben enthält wie z. B. lohnsteuerrechtlich unerhebliche Konfessionen, Geburtsnamen und Geburtstag der *Ehefrau* (entsprechende Angaben zum *Ehemann* werden von weiblichen Beschäftigten nicht verlangt) sowie Ort der Eheschließung, Art einer Erkrankung, Ehrungen. Ich habe gefordert, die Eintragungen zu allen nicht erforderlichen Merkmalen zu löschen. Dies ist geschehen. Generell sollte eine Personalkartei nicht geführt werden, wenn ein automatisiertes Personalinformationssystem zur Verfügung steht.

5.1.25 Unübersichtliche Personalaktenführung in einer Gemeindeverwaltung

Bei der datenschutzrechtlichen Kontrolle einer Gemeindeverwaltung mußte ich feststellen, daß die im Personalamt geführten Personalakten weder durchnumeriert noch nach sachlichen Gesichtspunkten gegliedert waren.

Ich habe die Gemeindeverwaltung darauf hingewiesen, daß die unübersichtliche Personalaktenführung geeignet ist, das Recht der Beschäftigten auf *gezielte*

Einsichtnahme in ihre Personalakten (vgl. § 13 BAT-O) zu erschweren, und angeregt, die Personalakten entsprechend der Verwaltungsvorschrift des SMI über die Führung und Verwaltung von Personalakten der Beamten zu führen.

Mir wurde zugesichert, die Personalakten an die Vorgaben der Verwaltungsvorschrift anzupassen.

5.1.26 Einbehalten privater Telefongebühren im Gehaltsabzugsverfahren

Verschiedene Behörden beabsichtigen, die Gebühren für Privatgespräche im Gehaltsabzugsverfahren einzubehalten.

Um Privatgespräche vom Dienstapparat aus führen zu können, müssen die Bediensteten eine persönliche Identifikationsnummer (PIN) beantragen und sich gleichzeitig schriftlich mit dem Gehaltsabzugsverfahren einverstanden erklären. Wer sein Einverständnis nicht erteilt, erhält keine PIN, kann somit auch keine Privatgespräche führen.

Abgesehen davon, daß Nr. 21 der Sächsischen Dienstanschlußvorschriften des SMF vom 13. Juli 1993 und die Allgemeine Verwaltungsvorschrift des Bundes über die Einrichtung und Benutzung dienstlicher Telekommunikationsanlagen ausdrücklich das o. a. Gehaltsabzugsverfahren verbieten, widerspricht diese Verfahrensweise nicht unerheblich den Grundsätzen einer *freiwilligen* Einwilligung.

Eine Einwilligung in das Gehaltsabzugsverfahren muß nämlich völlig frei von jedwedem Zwang erteilt werden können (Art. 2 Buchstabe h der EU-Datenschutzrichtlinie lautet: "Im Sinne dieser Richtlinie bezeichnet der Ausdruck 'Einwilligung der betroffenen Person' jede Willensbekundung, die *ohne Zwang*, für den konkreten Fall und in Kenntnis der Sachlage erfolgt und mit der die betroffene Person akzeptiert, daß personenbezogene Daten, die sie betreffen, verarbeitet werden"). Die Alternative "*entweder Sie geben uns die Einwilligung oder Sie erhalten keine PIN, dürfen also keine Privatgespräch führen*" stellt die Betroffenen vor eine Zwangssituation, die mit "*Freiwilligkeit*" nichts mehr zu tun hat.

Sofern Behörden den Bediensteten, die nicht einzuwilligen bereit sind oder die ihre Einwilligung widerrufen, keine andere Möglichkeit zur Führung von Privatgesprächen anbieten (z. B. als Selbstzahler), liegt eine echte "Freiwilligkeit" nicht vor, ist das Gehaltsabzugsverfahren somit unzulässig.

Im übrigen gebe ich zu bedenken, daß im Fall eines fehlerhaften Abzugs vom Gehalt der Betroffene seinem Geld "nachrennen" muß, d. h. er muß beweisen, daß die Abbuchung zu unrecht erfolgt ist, während der Selbstzahler nach Erhalt der Rechnung *vor* der Begleichung eine Klärung herbeiführen kann.

5.1.27 Namentliche Nennung bei Verlust des Dienstausweises im Sächsischen Amtsblatt (oder in anderen amtlichen Bekanntmachungen)

Mir wurden Bedenken gegen die namentliche Veröffentlichung bei Verlust des Dienstausweises im Sächsischen Amtsblatt unter Hinweis auf eine gewisse "Prangerwirkung" vorgetragen.

In der Tat verfahren die sächsischen Behörden in solchen Fällen nach Nr. 9 der Verwaltungsvorschrift des SMI über Dienstausweise für Beschäftigte im Staatsdienst vom 15. Januar 1991 (SächsABl. S. 4) in der Fassung der Änderungsbekanntmachung vom 11. Mai 1992 (SächsABl. S. 573). Danach hat die Ausstellungsbehörde in Verlust geratene Dienstausweise nach erfolglosen Ermittlungen im Sächsischen Amtsblatt für ungültig zu erklären. Dies geschieht in der Praxis u. a. durch namentliche Nennung des bisherigen Ausweisinhabers.

Ich habe dem SMI meine Ansicht mitgeteilt, daß es genügen würde, die Ausweisnummer, die Ausstellungsbehörde und das Ausstellungsdatum, nicht aber die Namen, zu veröffentlichen. Eine gesetzliche Grundlage zur Namensnennung, wie sie Art. 33 SächsVerf und § 31 Abs. 2 SächsDSG fordern, war mir nicht ersichtlich.

Das SMI hat mir nach Überprüfung geantwortet, daß die Veröffentlichungen keinen praktischen Nutzen hätten und der damit verbundene Verwaltungsaufwand unvertretbar sei. Durch Änderung der Verwaltungsvorschrift solle im Freistaat Sachsen deshalb künftig auf eine Veröffentlichung der Ungültigkeitserklärung bei Verlust von Dienstausweisen verzichtet werden.

Dies ist mit der Änderungsverwaltungsvorschrift des SMI vom 17. November 1995 (SächsABl. S. 1387) geschehen.

Zur Frauenförderungs-Statistik siehe Abschnitt 5.7.2

5.2 Personalvertretung

5.2.1 Automatisierte Verarbeitung von Beschäftigtendaten beim Personalrat

Mehrere Behördenleitungen und Personalräte fragten, ob und welche Beschäftigtendaten beim Personalrat automatisiert verarbeitet werden dürfen. Die Rechtslage stellt sich wie folgt dar:

Nach § 31 Abs. 1 SächsDSG darf eine öffentliche Stelle Beschäftigtendaten nur verarbeiten, soweit dies zur Eingehung, Durchführung oder Beendigung des Dienst- oder Arbeitsverhältnisses *erforderlich* ist oder ein Gesetz, ein Tarifvertrag oder eine

Dienstvereinbarung dies vorsieht. Soll die Datenverarbeitung automatisiert erfolgen, ist gemäß § 31 Abs. 7 SächsDSG das Benehmen mit mir herzustellen.
Der Personalrat darf ohne datenschutz- bzw. personalvertretungsrechtliche Bedenken lediglich folgende Grunddaten automatisiert speichern:
Name, Vorname, Sachgebiet, Besoldungs-/Vergütungsgruppe des Bediensteten.

Hierfür sind folgende Gründe maßgebend:

Aus § 73 SächsPersVG folgt, daß dem Personalrat kein uneingeschränktes Informationsrecht zusteht. Sein Informationsrecht beschränkt sich auf die zur Behandlung des konkreten Falles *erforderlichen* Informationen. Auch ein Recht auf Einsicht in Personalakten besteht nur für bestimmte Personalratsmitglieder und auch nur dann, wenn der betreffende Bedienstete sein Einverständnis dazu erklärt hat. Daraus ist abzuleiten, daß dem Personalrat ein dateimäßiges Vorhalten von Daten (die über den o. a. Rahmen hinausgehen) untersagt ist, wenn ihm Unterlagen *nur zur Beurteilung des Einzelfalles* (z. B. Höhergruppierung, Beförderung, Versetzung) überlassen werden oder wenn sie lediglich zur Einsichtnahme zur Verfügung stehen.

Grundsätzlich unzulässig wäre es demnach, wenn über den o. g. Rahmen hinaus aus einzelnen Beteiligungsfällen (z.B. Versetzungen, Abordnungen, Umsetzungen, Aus- und Fortbildung, Höhergruppierungen) personenbezogene Daten (auf Dauer) *auf Vorrat automatisiert gespeichert* würden, um ggf. später darauf zurückgreifen zu können. Insbesondere darf der Personalrat nicht auf diese Weise eine zweite (automatisierte) Personalakte - auch nicht in verkürzter Form - aufbauen.

Für die Speicherung von Daten im Rahmen der Erfüllung der öffentlich-rechtlichen Aufgaben der Personalvertretung, die durch das SächsPersVG zugewiesen sind, ist der Personalrat datenschutzrechtlich verantwortlich (insbesondere §§ 9, 10, 31 SächsDSG). Er unterliegt insoweit meiner Kontrollkompetenz.

5.2.2 Auswertung von Dienstgesprächen bei ISDN-Telefonanlagen

Im Zusammenhang mit dem Abschluß einer Dienstvereinbarung über die Einführung und Anwendung einer ISDN-Telefonanlage war der Umfang der Auswertung von Dienstgesprächen strittig. Die Dienststellenleitung bestand auf einem vollständigen Ausdruck *aller* Dienstgespräche mit Nebenstelle, Zeit und Kosten (Vollauswertung). Sie versprach sich davon eine Kostensenkung durch Verhaltensänderung der Beschäftigten und argumentierte, dem einzelnen werde so vor Augen geführt, welche monatlichen Telefonkosten und welche Zeit für Telefongespräche anfielen. Dies hätte vermöge der psychologischen Wirkung weniger und kürzere Gespräche und mehr Briefe (besonders ins Ausland) zur Folge.

Der Personalrat bestand dagegen auf einer lediglich *stichprobeweisen* Auswertung in Anlehnung an die "Verwaltungsvorschrift über den Betrieb und Nutzung der

Telekommunikationsanlage der Sächsischen Staatsregierung" vom 5. Dezember 1993 (SächsABl. S. 1354). Er befürchtete von der Vollauswertung und der vorgesehenen Überprüfung durch die Vorgesetzten eine Verhaltens- und Leistungskontrolle der Beschäftigten selbst dann, wenn die Dienstvereinbarung dies ausdrücklich verbietet.

Ich habe dazu folgende Position vertreten:

Eine Vollauswertung ist datenschutzrechtlich nicht per se unzulässig. Sie stellt allerdings den größtmöglichen Umfang dar, der ggf. unter dem Gesichtspunkt der Erforderlichkeit zu verringern wäre. Dabei müßte gefragt werden, ob nicht das Ziel "Kostensenkung durch Verhaltensänderung" auch ohne Vollauswertung erreicht werden könnte, z. B. durch eine Auflistung nur der kostenintensiven Gespräche (Auslandsgespräche und Gespräche, die eine bestimmte Zeit- oder Gebührengrenze überschreiten). Ein solches Verfahren wäre für die Beschäftigten und die Dienststelle von Vorteil: Die Beschäftigten wären in tatsächlicher Hinsicht vor der zwar unzulässigen, aber möglichen Verhaltenskontrolle geschützt; die Vorgesetzten hätten nicht Hunderte von Gesprächsdaten durchzusehen, da automationsgestützt eine "Vorauswertung" erfolgt wäre.

5.2.3 Inhalt von Wählerverzeichnissen bei Wahlen zum Personalrat

Zur Durchführung der Wahl des Personalrats erstellt der Wahlvorstand ein Verzeichnis der Wahlberechtigten (Wählerverzeichnis). Anders als die Kommunalwahlordnung enthält die Wahlordnung zum Sächsischen Personalvertretungsgesetz jedoch keine Bestimmungen über den Inhalt dieser Wählerverzeichnisse.
Eine Stadtverwaltung fragte daher, welche personenbezogenen Daten in die Wählerverzeichnisse aufgenommen werden dürfen (insbesondere, ob der Tag der Geburt erscheinen darf).

Das SMI, das ich um Stellungnahme hierzu gebeten habe, hat mir mitgeteilt, daß aus dortiger Sicht lediglich Name und Vornamen der Wahlberechtigten zum *erforderlichen* Inhalt der Verzeichnisse gehören.

Dieser Ansicht habe ich mich angeschlossen, und ich habe die Stadtverwaltung entsprechend informiert.

5.2.4 Aushändigung des Stellenplans oder Stellenbesetzungsplans an den Personalrat

Eine Dienststelle verweigerte dem Personalrat die Aushändigung des erbetenen Stellenplans (alternativ: Stellenbesetzungsplan) aus "datenschutzrechtlichen Gründen". Der Personalrat holte dazu meine Stellungnahme ein. Ich habe mich wie folgt geäußert:

Gemäß § 73 Abs. 2 SächsPersVG hat der Dienststellenleiter die Personalvertretung zur Durchführung ihrer Aufgaben umfassend zu unterrichten und ihr die hierfür erforderlichen Unterlagen vorzulegen. Zu den Aufgaben der Personalvertretung gehört nicht nur die Wahrnehmung der Mitwirkungs- und Mitbestimmungsrechte in konkreten Fällen (§§ 78, 80, 81 SächsPersVG). Vielmehr gehören dazu auch die allgemeinen Aufgaben nach §§ 72 und 73 SächsPersVG, insbesondere, auf die Gleichbehandlung der Beschäftigten zu achten und darüber zu wachen, daß die zugunsten der Beschäftigten geltenden Gesetze, Tarifverträge, Dienstvereinbarungen usw. eingehalten werden.

Diese Aufgaben erfordern einen breiten, über den Einzelfall hinausgehenden Kenntnisstand. Nur anhand einer allgemeinen Übersicht (z. B. Stellenplan, Stellenbesetzungsplan, Liste mit den Grunddaten der Beschäftigten) kann der Personalrat nachprüfen, ob entsprechend der tarifvertraglichen Vereinbarung und den beamtenrechtlichen Vorschriften verfahren wird und eine willkürliche Handhabung unterbleibt. Dies sichert nicht zuletzt den Betriebsfrieden (§ 71 Abs. 2 SächsPersVG). Da solche zunächst nicht personenbezogenen Übersichten folglich zur Aufgabenerfüllung der Personalvertretung erforderlich sind, steht ihrer Aushändigung datenschutzrechtlich nichts entgegen. Selbstverständlich sind diese Unterlagen auch beim Personalrat besonders gesichert aufzubewahren, zumal sie personenbeziehbar sind.

5.2.5 Diskrepanz zwischen §§ 77 Nr. 4 und 80 Abs. 3 Nr. 16 SächsPersVG

Nach § 77 Nr. 4 SächsPersVG *wirkt* der Personalrat *mit* bei der Einführung, Änderung, Ausweitung betrieblicher Informations- und Kommunikationsanlagen, der Art und Weise, wie Daten und Signale aufgenommen, erfaßt, übertragen und ausgegeben werden, soweit die Arbeitsweise der Beschäftigten betroffen ist.

Andererseits hat der Personalrat nach § 80 Abs. 3 Nr. 16 SächsPersVG das stärkere Instrument der *Mitbestimmung* bei der Einführung und Anwendung technischer Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Beschäftigten zu überwachen (nach ständiger Rechtsprechung genügt es, wenn die Einrichtung zur Leistungs- und Verhaltenskontrolle lediglich *geeignet* ist).

Wiederholt habe ich gegenüber dem SMI deutlich gemacht, daß die Diskrepanz zwischen diesen beiden Bestimmungen zu einer gewissen Verunsicherung der Behördenleitungen und der Personalvertretungen führt. Insbesondere wird das Recht der Beschäftigten auf informationelle Selbstbestimmung durch Beibehaltung des § 77 Nr. 4 SächsPersVG geschwächt.

Gleichwohl sieht Art. 3 des Entwurfs eines Gesetzes zur Änderung dienstrechtlicher Vorschriften keine Streichung dieser Mitwirkungsbestimmung vor. In meiner Stellungnahme zu diesem Gesetzentwurf habe ich nochmals nachdrücklich die

ersatzlose Streichung des § 77 Nr. 4 SächsPersVG gefordert. Eine Reaktion des SMI steht noch aus.

5.2.6 Beteiligung des Personalrats und der Frauenbeauftragten bei Beurlaubung aus persönlichen Gründen

Eine Petentin, die sich zur Pflege ihres behinderten Kindes hin und wieder beurlauben läßt, fühlte sich dadurch in ihren schutzwürdigen Belangen beeinträchtigt, daß die Behördenleitung den Personalrat und die Frauenbeauftragte von dem Grund der Beurlaubung in Kenntnis gesetzt hatte.

Ich habe ihr mitgeteilt, daß es nach § 73 Abs. 1 Nr. 2 SächsPersVG zu den Aufgaben des Personalrats gehört, darüber zu wachen, daß die zugunsten der Beschäftigten geltenden Gesetze, Verordnungen, Tarifverträge, Dienstvereinbarungen und Verwaltungsanordnungen (richtig) angewendet werden. Hierzu hat der Dienststellenleiter den Personalrat *rechtzeitig und umfassend* zu unterrichten und alle erforderlichen Unterlagen vorzulegen (§ 73 Abs. 2 SächsPersVG). Ähnliches gilt für die Frauenbeauftragte.

Eine Beurlaubung aus persönlichen Gründen (hier Pflege des Kindes) ist nach den einschlägigen tarifrechtlichen und beamtenrechtlichen Bestimmungen unter Wegfall der Bezüge grundsätzlich zulässig, wenn dienstliche Interessen nicht entgegenstehen. Falls die Dienststelle die Vorlage ärztlicher/amtlicher Bescheinigungen zum Nachweis, daß der Antrag auf unbezahlten Urlaub begründet ist, verlangt, sind sogar diese Unterlagen dem Personalrat (der Frauenbeauftragten) vorzulegen. Diese sind allerdings zur Verschwiegenheit verpflichtet.

5.3 Einwohnermeldewesen; Paß- und Personalausweiswese

5.3.1 Rechtliche Entwicklung

5.3.1.1 Entwurf eines Gesetzes zur Änderung des Sächsischen Meldegesetzes

Im 3. Tätigkeitsbericht (5.3.1.2) habe ich dargestellt, welche Änderungen des Sächsischen Meldegesetzes ich aufgrund der Novellierung des Melderechtsrahmengesetzes für erforderlich halte. Außerdem habe ich praxisbedingte

Änderungsvorschläge für das Sächsische Meldegesetz gemacht (unter 5.3.1.3). Bedauerlicherweise sind nicht alle meine Anregungen und Vorschläge in dem mir vom SMI vorgelegten Entwurf zur Änderung des Sächsischen Meldegesetzes berücksichtigt worden. Daher habe ich in meiner Stellungnahme zu dem Entwurf meine Auffassung im wesentlichen wiederholt und nochmals eingehend begründet.

Schwerpunktmäßig habe ich zu § 29 Abs. 1 Satz 3 des Entwurfs Stellung genommen, wonach automatisierte Abrufverfahren zugelassen werden sollen, wenn diese Verfahren unter Berücksichtigung der schutzwürdigen Interessen der Betroffenen und der Aufgaben der öffentlichen Stelle angemessen sind und mindestens eine stichprobenweise Abrufkontrolle gewährleistet ist. Ich habe u. a. darauf hingewiesen, daß ich eine explizite Benennung der am automatisierten Abrufverfahren beteiligten Stellen für erforderlich halte, wie sie z. B. § 36 StVG enthält. Nur wenn der Kreis der in Frage kommenden Stellen vom Gesetz umrissen ist, wird dem Regelungszweck des § 8 Abs. 1 SächsDSG Genüge getan: Danach muß ein Gesetz *das konkret anzuwendende Verfahren* ausdrücklich zulassen. Die lapidare Formulierung, automatisierte Abrufverfahren würden (unter den o. g. allgemeinen Voraussetzungen) zugelassen, beachtet gerade nicht den vom Gesetzgeber erteilten Vorbehalt, die Einrichtung *bestimmter* Online-Verbindungen von einer bereichsspezifischen gesetzlichen Befugnisnorm abhängig zu machen.

Erfreulich ist hingegen, daß - meinen langjährigen Forderungen entsprechend - der Entwurf für die Eintragung einer melderechtlichen Auskunftssperre bei Gefahr für Leben, Gesundheit, persönliche Freiheit oder ähnliche schutzwürdige Belange keine Kostenerhebung mehr vorsieht. Damit ist nicht mehr zu befürchten, daß Betroffene, denen durch eine Melderegisterauskunft eine Gefahr für o. g. Rechtsgüter droht, durch die Gebührenpflicht von der Geltendmachung dieses Schutzrechts abgehalten werden.

5.3.1.2 Entwurf einer Sächsischen Meldedatenübermittlungsverordnung

Im Berichtszeitraum wurde mir der überarbeitete Entwurf einer Sächsischen Meldedatenübermittlungsverordnung übersandt. Leider sind trotz meiner gegenüber dem ersten Entwurf angemeldeten Bedenken weiterhin regelmäßige Datenübermittlungen aus dem Melderegister an die Finanzämter vorgesehen. *Sämtliche* Polizeidienststellen sollen zudem Online-Zugriffe auf alle sächsischen Melderegister erhalten. Dies habe ich nochmals nachdrücklich kritisiert (vgl. Nr. 5.3.2.1.2 und 5.3.2.1.3 des 3. Tätigkeitsberichts).

5.3.2 Meldedatenübermittlungen und Melderegisterauskünfte

5.3.2.1 Unzulässige Meldedatenübermittlungen an Mitgliedsgemeinden

Drei Gemeinden übertrugen durch Zweckvereinbarung nach dem SächsKomZG die Aufgaben nach dem SächsMG auf eine Mitgliedsgemeinde. Diese war nun Meldebehörde auch für die beiden anderen Gemeinden.

Vertraglich war vereinbart worden, daß die Meldebehörde den anderen beiden Gemeinden aus Aktualisierungsgründen vierteljährlich jeweils eine aktuelle Einwohnerliste übersendet. Tatsächlich wurden Gesamteinwohnerlisten aller drei Gemeinden an die beiden Mitgliedsgemeinden geschickt. Die Listenempfänger erhielten somit Meldedaten der jeweils anderen Gemeinden.

Diese Verfahrensweise war mit dem *Erforderlichkeits*grundsatz (vgl. § 29 Abs. 1 Satz 1 SächsMG) nicht zu vereinbaren. Die Meldebehörde hat dies akzeptiert; die Listenübersendung unterbleibt; bereits übersandte Listen wurden vernichtet.

5.3.2.2 Übermittlung von Meldedaten an die öffentlich-rechtlichen Rundfunkanstalten und an die GEZ

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat sich in einer Entschließung zu den kritisierten regelmäßigen Meldedatenübermittlungen an die öffentlich-rechtlichen Rundfunkanstalten und an die GEZ am 26./27. Oktober 1993 u. a. wie folgt geäußert: "Die Datenschutzbeauftragten des Bundes und der Länder sind bereit, an geeigneten und verfassungskonformen Lösungen der Landesregierungen zur Sicherung des Gebührenaufkommens der Rundfunkanstalten mitzuwirken."

Mein unter Nr. 5.3.11 des 2. Tätigkeitsberichts dargestellter Vorschlag, nämlich den GEZ-Datenbestand mit den gemeindlichen Melderegistern abzugleichen und zu aktualisieren (Sterbefälle, Wegzüge), fand bisher keine große Resonanz, weil damit unbekannte Gebührenschuldner (Schwarzseher, Schwarzhörer) nicht zu ermitteln sind.

Auf Bitte der SK, an die sich der MDR gewandt hatte, ergänzte ich meinen o. a. Vorschlag wie folgt: "Nachdem der GEZ-Datenbestand (MDR-Datenbestand) vorschlagsgemäß bereinigt ist, ermittelt die Meldebehörde durch nochmaligen Abgleich alle Haushaltsvorstände, die sich noch nicht im Datenbestand der GEZ/des MDR befinden." Bei den so ermittelten Haushaltsvorständen kann der MDR/die GEZ gezielt auf eine denkbare Gebührenpflicht aufmerksam machen. Eine solche Vorgehensweise, die selbstverständlich mit allen beteiligten Stellen (SK, SMI, MDR/GEZ) erörtert werden muß, hätte den Vorteil gegenüber den in einigen Ländern existierenden Meldedatenübermittlungsverordnungen, daß die Übermittlung von Daten der Familienangehörigen, die vermutlich nicht selbst gebührenpflichtig sind, unterbliebe.

Erste Gepräche haben bereits im Frühjahr 1996 stattgefunden.

5.3.2.3 Adreßbuchdaten auf CD-ROM

Fortschreitende Technik bereitet neue Probleme. So hatte ich mich mit der Frage zu befassen, ob Adreßbuchangaben auch auf CD-ROM gespeichert und weitergegeben werden dürfen.

Nach § 33 Abs. 3 SächsMG darf die Meldebehörde Vor- und Familiennamen, Doktorgrad und Anschriften der volljährigen Einwohner in *alphabetischer* Reihenfolge der Familiennamen (nicht also straßenweise) in Adreß*büchern* und ähnlichen *Nachschlagewerken* veröffentlichen und anderen zum Zwecke der Herausgabe solcher Werke übermitteln.

Speicherung und Weitergabe von Adressen auf CD-ROM widersprechen in zweierlei Hinsicht dem Wortlaut des Gesetzes. Zum einen ist eine CD-ROM weder ein *Buch* noch ein sonstiges *Nachschlagewerk*. Zum anderen würde der Gesetzesbefehl, Einwohnerdaten nur in *alphabetischer* Reihenfolge zu veröffentlichen oder an Adreßbuchverlage weiterzugeben, durch die neue Technik unterlaufen. Die Daten wären jederzeit umsortier- und nach anderen Kriterien auswertbar, und das ist nicht gewollt. Die Weitergabe von Melderegisterdaten an Adreßbuchverlage sollte daher davon abhängig gemacht werden, daß keine Speicherung auf CD-ROM erfolgt.

Das schließt natürlich nicht aus, daß gewerbliche Unternehmen Adreßbücher, Telefonbücher u. ä. durch "Einscannen" digitalisieren, um diesen Datenbestand (der einem bundesweiten Melderegister gleichkommen kann) kommerziell zu nutzen. Die damit einhergehende datenschutzrechtliche Problematik wird derzeit bundesweit durch einen Erfahrungsaustausch der Datenschutzbeauftragten des Bundes und der Länder, aber auch zwischen den Datenschutzbehörden für den nicht-öffentlichen Bereich ("Düsseldorfer Kreis"), erörtert.

Um das Risiko, in solchen Dateien gespeichert zu werden, zu verringern, sei jedem Betroffenen geraten, bei seiner Meldebehörde von seinem Widerspruchsrecht gemäß § 33 Abs. 4 SächsMG Gebrauch zu machen. Die Meldebehörden sind aufgerufen, ihre Einwohner regelmäßig auf die Widerspruchsmöglichkeiten, die das SächsMG bietet, hinzuweisen (z. B. durch Hinweis im Gemeindeblatt).

5.3.3 Verbot der Datenverarbeitung bei "Beeinträchtigung schutzwürdiger Interessen"

Mehrere Einwohnermeldeämter fragten, nach welchen Kriterien sie prüfen sollen, ob schutzwürdige Interessen des Betroffenen durch die Verarbeitung seiner Meldedaten beeinträchtigt werden (vgl. § 22 SächsMG). Ich habe hierzu folgendes mitgeteilt:

Schutzwürdige Interessen sind alle von der Rechtsordnung geschützten Interessen, also die Persönlichkeitssphäre und andere durch Grundrechte geschützte Interessen, aber auch die durch sonstige Rechtsvorschriften geschützten Belange des Einzelnen. Nicht schutzwürdig ist zum Beispiel das Bestreben des Betroffenen, sich seinen Unterhaltspflichten oder sonstigen Zahlungspflichten zu entziehen.

Ob eine Beeinträchtigung schutzwürdiger Interessen des Betroffenen vorliegt, bedarf einer Interessenabwägung im Einzelfall. Dabei sind zunächst die schutzwürdigen Belange des Einzelnen festzustellen, sowie die entgegenstehenden öffentlichen oder privaten Interessen zu ermitteln. Eine Beeinträchtigung liegt nicht vor, wenn die öffentlichen oder privaten Belange die schutzwürdigen Interessen des Betroffenen überwiegen. Bei der gebotenen Interessenabwägung ist insbesondere der verfassungsrechtliche Grundsatz der Verhältnismäßigkeit zu beachten (vgl. § 22 Satz 2 SächsMG). Dieser verlangt, daß die beabsichtigte Maßnahme geeignet, erforderlich und angemessen sein muß.

Diese Voraussetzungen haben die Meldebehörden stets zu prüfen, bevor sie Meldedaten verarbeiten, falls die Meldedatenverarbeitung nicht durch Rechtsvorschrift vorgeschrieben ist (§ 22 Satz 3 SächsMG).

5.3.4 Teilnahme in Deutschland lebender türkischer Staatsbürger an den Wahlen in ihrem Heimatland

Das BMI bat die Innenministerien der Länder unter Hinweis auf eine Verbalnote des Auswärtigen Amtes an die türkische Botschaft, nach der Hilfestellung seitens deutscher Behörden bei ausländischen Wahlen grundsätzlich nicht geleistet wird, u. a. um Stellungnahme zu folgendem Vorschlag der türkischen Seite:

In Deutschland lebende, in der Türkei wahlberechtigte türkische Staatsbürger besorgen sich an ihrem Wohnort in Deutschland eine Meldebescheinigung, welche von der Meldebehörde mit Einwilligung der Betroffenen unmittelbar an die türkische Botschaft bzw. an das jeweilige Generalkonsulat geschickt wird. Dort sollen daraufhin die Wählerverzeichnisse erstellt werden.
Dem SMI, das um Stellungnahme bat, teilte ich folgendes mit:
Es ist zutreffend, daß sich türkische Staatsbürger (wie jeder Einwohner) bei der Meldebehörde eine Meldebescheinigung ausstellen lassen dürfen. Was die Betroffenen danach mit dieser Meldebescheinigung tun, bleibt ihnen selbst überlassen.

Die vom BMI erwähnte "Einwilligung" ist jedenfalls untauglich, da sie ein aktives Tätigwerden der Meldebehörde voraussetzen würde. Die Meldebehörde müßte die Betroffenen (von sich aus) fragen, ob sie mit der Weiterleitung der Meldebescheinigung an die Botschaft usw. einverstanden sind, wofür kein Anlaß besteht. Außerdem müßten die Anforderungen an eine Einwilligung gemäß § 4 Abs. 2 und 3 SächsDSG erfüllt sein. Den Meldebehörden kann die Aufklärung der Betroffenen schon im Hinblick auf Verständigungsschwierigkeiten und auf fehlende Kenntnisse darüber, was bei den Empfängern (Botschaft und Generalkonsulate) tatsächlich mit den Daten geschieht (denkbare Zweckänderung), nicht übertragen werden. Im Hinblick auf die Intention des § 1 SächsDSG und des § 22 SächsMG wäre die Weiterleitung der Meldebescheinigungen an die Botschaft und die Generalkonsulate schon deshalb rechtswidrig, weil den Meldebehörden eine Prüfung, ob tatsächlich keine schutzwürdigen Interessen beeinträchtigt werden (z. B. durch Zweckänderung der Daten), auf ausländischem Staatsgebiet versagt ist. Dies gilt insbesondere dann, wenn im Empfängerstaat kein dem deutschen Niveau entsprechendes Datenschutzrecht gilt. Daran würde auch ein *Auftrag* (Wunsch) der Betroffenen zur Weiterleitung der Meldescheine an die Botschaften nichts ändern. Zum einen gehört eine solche Dienstleistung nicht zu den gesetzlichen Aufgaben der Meldebehörden. Zum anderen können die Betroffenen die Weiterleitung schon deshalb nicht erzwingen, weil die Meldebehörden über Datenübermittlungen nach pflichtgemäßem Ermessen zu entscheiden haben. Dabei haben sie - gebunden an gesetzmäßiges Verwaltungshandeln - stets auch die allgemeinen Grundsätze wie Verhältnismäßigkeit, Erforderlichkeit der Datenverarbeitung, Zweckbindung der Daten sowie die schutzwürdigen Interessen der Betroffenen zu beachten. Das bedeutet, daß trotz ausdrücklichen Wunsches der Betroffenen eine Datenübermittlung an die Botschaft keineswegs erlaubt ist.

Schließlich stellt ein - jedoch weniger datenschutzrechtliches - Argument die Geeignetheit des Verfahrens als solches in Frage: Die Meldebehörden (Gemeinden) können aufsichtsrechtlich nicht angewiesen werden, diese sich außerhalb der melderechtlichen Aufgaben bewegende Aktion durchzuführen.

Letztendlich liefe das in Frage stehende Verfahren, entgegen der türkischen Ansicht, doch auf eine "organisatorische Unterstützung" der türkischen Wahl hinaus und ist schon deshalb - folgt man der Verbalnote des Auswärtigen Amtes - unzulässig.
Schließlich ist nicht ersichtlich, warum die Betroffenen ihre Meldebescheinigungen nicht selbst den türkischen Stellen zuleiten könnten.

5.3.5 Aufenthaltsfeststellungsverfahren nach § 24 b WPflG

Das SMI bat mich um Stellungnahme zur Zulässigkeit der Übertragung des in § 24 b WPflG vorgeschriebenen Aufenthaltsfeststellungsverfahren auf die Datenverarbeitungszweckverbände.

Nach § 24 b Abs. 2 WPflG darf das Bundesverwaltungsamt zur Feststellung des

Aufenthalts von nicht erreichbaren Wehrpflichtigen die entsprechenden Dateien in regelmäßigen Abständen u. a. den Meldebehörden *oder den von ihnen beauftragten Stellen* übermitteln.

Soweit die Meldebehörden die Zweckverbände mit der Wahrnehmung der sich aus § 24 b WPflG ergebenden Aufgaben beauftragen, bestehen keine Bedenken gegen das beabsichtigte Verfahren, sofern die Löschung der vom Bundesverwaltungsamt übermittelten Datei vom Empfänger vorschriftsmäßig dann erfolgt, wenn die nächste aktuelle Datei übermittelt wird (§ 24 b Abs. 3 WPflG).

Das SMI wurde gebeten, die Zweckverbände auf diese Löschungsverpflichtung hinzuweisen.

5.3.6 Abgrenzung der "automatisierten Führung" des Melderegisters gegenüber den "melderechtlichen Hilfstätigkeiten"

Nach § 3 SächsMG dürfen mit der *automatisierten Führung* des Melderegisters nur *sächsische öffentliche Stellen* beauftragt werden (Auftragsdatenverarbeitung). Die Frage war, ob die Vergabe anderer Arbeiten als der *automatisierten Führung* des Melderegisters an *Private* zulässig sei. Ich habe mich wie folgt geäußert:

"Automatisierte Führung" des Melderegisters ist die Bearbeitung melderechtlicher Vorgänge, wie
- Zuzug/Wegzug,
- Geburt,
- Eheschließung,
- Sterbefall,
- Namensänderung,
- Auskunfts- und Übermittlungssperren,
- Berichtigungen,

sowie die Erstellung von Datensätzen für die Lohnsteuerkarten, Wahlbenachrichtigungen und die regelmäßigen Datenübermittlungen nach den Meldedatenübermittlungsverordnungen des Bundes und des Landes mittels Datenverarbeitungsanlage.

Nicht davon erfaßt sind nach meinem Dafürhalten die aus dem automatisierten Melderegister herausgelösten "melderechtlichen Hilfstätigkeiten", als da sind
- Druck, Kuvertierung und Versand der Lohnsteuerkarten und Wahlbenachrichtigungen (Ausdruck erfolgt aus den automatisiert erstellten Dateien, z. B. Diskettenausdruck),
- Ausdruck und Versand von Listen der automatisiert erstellten Dateien bzw. Versand der entsprechenden Datenträger an die Empfänger regelmäßiger Datenübermittlungen z. B. mittels Kurierdienst.

Soweit diese "melderechtlichen Hilfstätigkeiten" nicht durch die Meldebehörde selbst bewerkstelligt werden können (z. B. mangels Druckkapazität), steht nach meinem Dafürhalten § 3 SächsMG nicht dagegen, auch ein zuverlässiges Privatunternehmen mit der Erledigung zu beauftragen, soweit dort die nach §§ 7 und 9 SächsDSG zu treffenden personellen, technischen und organisatorischen Maßnahmen - wozu auch die Verpflichtung des Firmenpersonals nach dem Verpflichtungsgesetz gehört - gegeben sind.

5.3.7 Datenerhebung durch Vermieter über die bei ihnen gemeldeten Mieter

In Sachsen werden Abfallgebühren vorwiegend nach dem "Personenmaßstab" erhoben, d. h. die Höhe der Gebühren richtet sich nach der Anzahl der in einem Haushalt wohnenden Personen. Die Gebührensatzung eines Landkreises sah daher vor, daß die Eigentümer von Miethäusern die Zahl der *gemeldeten* Bewohner dem Landkreis zur Gebührenberechnung mitteilen sollten.

Ich habe das Regierungspräsidium (Kommunalaufsicht) darüber informiert, daß ich die Satzung für rechtswidrig halte, soweit von den Eigentümern die Mitteilung des Datums "gemeldet" verlangt wird. Die Tatsache, ob ein Mieter seiner Meldepflicht nachgekommen ist, ist nämlich gebührenrechtlich ohne Bedeutung. Das Erheben dieses Datums ist daher nicht erforderlich. Die Datenerhebungsvorschrift der Abfallgebührensatzung verstieß mithin gegen den verfassungsrechtlichen Grundsatz der Verhältnismäßigkeit. Abgesehen davon sieht das Sächsische Meldegesetz eine Mitwirkung des Wohnungsgebers (z. B. Vermieter) bei der Anmeldung des Meldepflichtigen nicht vor, so daß er gar nicht mit Sicherheit wissen kann, ob und welche seiner Mieter tatsächlich gemeldet sind.

Das Regierungspräsidium hat meine Auffassung geteilt und auf eine datenschutzgerechte Änderung der Satzung hingewirkt.

5.3.8 Beauftragung eines privaten Zustell- oder Kurierdienstes mit der Weiterleitung der Anträge auf Ausstellung eines Passes oder Personalausweises an die Bundesdruckerei

Nach Nr. 6.6.1 PaßVwV sind die ausgefüllten und geprüften Anträge der Bundesdruckerei auf dem *Postwege* zu übersenden. Dieser Formulierung kommt jedoch keine Bindungswirkung dergestalt zu, daß andere Zustell- oder Kurierdienste mit dem Transport nicht beauftragt werden dürften.

Nach meinem Dafürhalten ist beim Transport der Paß- und Personalausweisanträge jedoch nach wie vor zu unterscheiden, ob er durch die Deutsche Post AG, die dem Postgeheimnis unterliegt, oder durch einen anderen (privaten) Kurierdienst, für den Art. 10 Abs. 1 GG nicht gilt, erfolgt.

Im letzteren Fall gelten für sächsische Paß- und Personalausweisbehörden die aus § 7 SächsDSG ersichtlichen Voraussetzungen. Danach obliegt es dem Auftraggeber, den Auftragnehmer unter besonderer Berücksichtigung der Eignung der von ihm getroffenen personellen, technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. Eine solche Maßnahme wäre der vom BMI und dem Bundesbeauftragten für den Datenschutz gemeinsam unterstützte Vorschlag, die Zustellung der Papiere durch Kurierdienst von einem Nachweis- und Quittungssystem mit Einzelnachweis abhängig zu machen. Sowohl der Transportweg als auch der Erhalt jeder einzelnen Sendung müssen dabei nachgewiesen und in der Posteingangsstelle der Bundesdruckerei kontrolliert und dokumentiert werden.

Ich habe das SMI gebeten, die sächsischen Paß- und Personalausweisstellen auf diese Erfordernisse hinzuweisen.

5.4 Wahlrecht; Personenstandswesen

5.4.1 Hinterbliebenensuche des Volksbundes Deutsche Kriegsgräberfürsorge e. V. (Volksbund)

Der Volksbund führt im Auftrag der Bundesregierung die Zentrale Gräberdatei der deutschen Kriegstoten. Noch immer informiert er auch Angehörige der Kriegstoten über die Lage der Grabstätten.

Zur Ermittlung der Hinterbliebenen wendet sich der Volksbund an Einwohnermelde- und Standesämter.

Während eine Melderegisterauskunft über die aktuelle Wohnanschrift der vom Volksbund namentlich genannten Hinterbliebenen unproblematisch ist, stoßen Auskünfte aus Standesamtsbüchern an die rechtlichen Grenzen des § 61 Abs. 1 PStG. Entscheidend für die Zulässigkeit von Auskünften aus den Standesamtsunterlagen ist die datenschutzrechtliche Einordnung des Volksbundes, der entweder wie eine Behörde oder - weil e. V. - als Privater zu behandeln ist.
Um Klarheit zu erhalten, habe ich mich an das Auswärtige Amt mit der Bitte um Information über Wesen und Aufgaben des Volksbundes gewandt. Erst dann werde ich abschließend beurteilen können, nach welchen Kriterien das Standesamt zu Auskünften an den Volksbund berechtigt ist.
Im Ergebnis darf die humanitäre Arbeit des Volksbundes nicht behindert werden. Dafür werde ich mich einsetzen.

5.4.2 Wahrung des Adoptionsgeheimnisses: Melderechtliche Behandlung eines zur Adoption freigegebenen Kindes nach der Geburt

Auf meine Anregung hin hat das SMI zur Wahrung des Adoptionsgeheimnisses die nachgeordneten Behörden wie folgt unterrichtet:

Soll ein Kind nach seiner Geburt nicht in die Wohnung der Mutter bzw. der Eltern aufgenommen werden, weil eine Inpflegenahme im Zusammenhang mit einer Adoption beabsichtigt ist, so unterrichtet die Adoptionsvermittlungsstelle hiervon unverzüglich den Standesbeamten am Geburtsort.

Liegt dem Standesbeamten zum Zeitpunkt der Geburtsbeurkundung eine solche Information vor, so unterbleibt seine Mitteilung an die für die Wohnung der Mutter bzw. der Eltern zuständige Meldebehörde nach § 98 Abs. 1 Nr. 2 in Verbindung mit § 277 DA.

In die Geburtenzählkarte (§ 398 Abs. 2 DA) nimmt der Standesbeamte statt der Angabe über die Hauptwohnung der Eltern bzw. der Mutter einen Hinweis über die beabsichtigte Annahme des Kindes auf. Die Mitteilung gemäß § 300 Abs. 3 Nr. 3 DA macht er nur an die Meldebehörde der Hauptwohnung der Adoptiveltern.

Die Adoptionsvermittlungsstelle informiert umgehend die für den beabsichtigten Aufenthalt zuständige Meldebehörde über die Aufnahme des Kindes in der Wohnung der Adoptiveltern und weist sie auf die bevorstehende Annahme des Kindes sowie auf die Beachtung des § 1758 Abs. 2 BGB hin. Wechselt das Kind die Wohnung, so teilt die Adoptionsvermittlungsstelle dies der zuständigen Meldebehörde der neuen Wohnung mit.

Die Mitteilung einer Adoptionsvermittlungsstelle bleibt für den Standesbeamten ohne Bedeutung und ist zu vernichten, wenn zwei Monate nach dem angegebenen Geburtstermin keine Angabe über die Geburt des Kindes vorliegt.

5.5 Kommunale Selbstverwaltung

5.5.1 Veröffentlichung personenbezogener Sachverhalte aus nichtöffentlicherGemeinderatssitzung

Wie in den vergangenen Jahren mußte ich wiederholt feststellen, daß über personenbezogene Sachverhalte, insbesondere in Personalangelegenheiten, unzulässigerweise in *öffentlicher* Sitzung verhandelt wird.

In einem besonders krassen Fall wurde zwar in nichtöffentlicher Sitzung beraten, die Ergebnisse wurden jedoch anschließend im gemeindlichen Amtsblatt veröffentlicht. So

war u. a. nachzulesen, welchen Gemeindebediensteten gekündigt worden ist und daß ein namentlich benanntes Kind "im Interesse der Entwicklung" in den Behindertenkindergarten aufgenommen werden soll.

Die von mir beanstandeten Veröffentlichungen widersprachen § 37 Abs. 1 Satz 3 und Abs. 2 SächsGemO in eklatanter Weise. Bereits in meinem 1. Tätigkeitsbericht (Nr. 5.5.2) habe ich darauf hingewiesen, daß bei zu vermutender Verletzung des Rechts auf informationelle Selbstbestimmung die Bekanntgabe der in nichtöffentlicher Sitzung gefaßten Beschlüsse anonym zu erfolgen hat. Vor allem die Hinweise auf die Behinderung eines Kindes führen in nicht hinnehmbarer Weise zu einer solchen Beeinträchtigung. Aber auch die Veröffentlichung der Kündigungsdaten beeinträchtigt das Recht auf informationelle Selbstbestimmung der Betroffenen - Personalvorgänge sind ihrer Natur nach vertraulich - und verstößt gegen § 31 Abs. 2 SächsDSG, wonach Beschäftigtendaten nur auf gesetzlicher Grundlage oder mit Einwilligung der Betroffenen veröffentlicht werden dürfen.

Die Gemeinde hat reagiert und beschlossen, daß personenbezogene Sachverhalte aus nichtöffentlichen Sitzungen nicht mehr veröffentlicht werden.

5.5.2 Video- und Tonbandaufnahmen in öffentlichen Gemeinderatssitzungen durch die Presse?

Entgegen der Ansicht des SMI bleibe ich dabei, daß Tonbandaufzeichnungen von Redebeiträgen in Gemeinderatssitzungen (z. B. zu Protokollzwecken) nur mit Kenntnis und Einwilligung der Betroffenen zulässig sind (vgl. Nr. 5.5.6 des 3. Tätigkeitsberichtes).

Die Frage des Redakteurs einer Lokalzeitung, ob dies auch für Tonbandaufnahmen durch die Presse gelte, habe ich bejaht und folgendes mitgeteilt:

Es entspricht allgemeiner Erfahrung, daß Tonbandaufnahmen von Redebeiträgen für das Verhalten der Betroffenen erhebliche Wirkung zeigen, weil sie jede Nuance der Rede, einschließlich der rhetorischen Fehlleistungen, der sprachlichen Unzulänglichkeiten und der Gemütsbewegungen des Redners, dauerhaft reproduzierbar konservieren. Weniger redegewandte Ratsmitglieder würden daher durch das Bewußtsein des Tonmitschnitts ihre Spontaneität verlieren, ihre Meinung nicht mehr "geradeheraus" vertreten oder schweigen, wo sie sonst gesprochen hätten. Die Willensbildung des Gemeinderats als demokratisch legitimierter Gemeindevertretung muß jedoch ungezwungen, freimütig und in aller Offenheit verlaufen.

Neben dem Persönlichkeitsrecht wäre das Recht der Ratsmitglieder auf freie Rede in Gemeinderatssitzungen betroffen (vgl. BVerwG NJW 1991, 119).
Demgegenüber bedeutet das Verbot von Tonbandaufzeichnungen in Gemeinderatssitzungen ohne Einwilligung der Betroffenen keinen Eingriff in die

Pressefreiheit, die nicht den freien Zugang zu Informationen einschließt. Außerdem wird lediglich die Art der Informationsbeschaffung und nicht die Informationsbeschaffung an sich beeinträchtigt.

Einer ähnlich lautenden Anfrage, ob Gemeinderatssitzungen durch den lokalen Fernsehsender visuell aufgezeichnet werden dürfen, habe ich wegen des denkbaren Einflusses auf das Abstimmverhalten ebenfalls in vorstehendem Sinne eine Absage erteilt.

5.5.3 Einsetzung einer Untersuchungskommission durch den Oberbürgermeister der Stadt Leipzig

Um einer in der Öffentlichkeit bekanntgewordenen Grundstücks- und Häuseraffäre, in die Mitarbeiter und ehemalige Berater der Stadt Leipzig verstrickt sein sollen, zu begegnen, setzte der Oberbürgermeister eine dreiköpfige unabhängige "Untersuchungskommission" ein, deren Mitglieder nicht aus den Reihen des Stadtrates stammten. Die Kommission sollte "unvoreingenommen und vollständig die relevanten Tatsachen feststellen und eine Bewertung unter juristischen und moralischen Gesichtspunkten vornehmen".

Der Oberbürgermeister hat auf meine Frage nach der Rechtsgrundlage mitgeteilt, daß die Untersuchungskommission auf der Grundlage formgültiger Einwilligungen sämtlicher Betroffener tätig werden solle. Ferner würden nur solche Unterlagen übermittelt und ausgewertet werden, die bereits ihrem vollständigen Inhalt nach öffentlich erörtert worden sind.

Trotz dieser beiden Voraussetzungen blieben nach Auffassung meiner Behörde folgende Bedenken bestehen:

1. Die vom Oberbürgermeister "eingesetzte" Untersuchungskommission hat nicht zuletzt durch den Text seiner Schreiben an die drei Mitglieder sowie durch die vom Pressedienst der Stadt Leipzig am 7. Februar 1996 herausgegebene Presseerklärung einen stark offiziellen und amtlichen Anstrich - dies gilt insbesondere für die Unabhängigkeit, die vollständige Tatsachenfeststellung und den Umfang des Bewertungsauftrages.
2. Die Klärung und Beurteilung der erhobenen Vorwürfe ist, soweit sie vom Oberbürgermeister erkennbar veranlaßt wurde, Verwaltungstätigkeit. Die Sächsische Gemeindeordnung sieht nicht vor, daß derartige Aufgaben in dieser Weise Privatpersonen zur Erledigung übertragen werden können. § 44 SächsGemO enthält insoweit abschließende und restriktive Vorschriften.

   Nach der Gemeindeordnung sind die drei berufenen Privatpersonen folglich unzuständig; ihr Tun ist als rein private und vollkommen unverbindliche Tätigkeit anzusehen.

3. Die Entgegennahme des Votums der Untersuchungskommission wäre eine Datenerhebung, die keinesfalls für die Erledigung von Verwaltungsaufgaben erforderlich ist. Das Wert- oder Unwerturteil eines "Tribunals" darf keinerlei Einfluß auf die rechtliche Bewertung des Verhaltens von kommunalen Bediensteten haben: Das "Tribunal" hat weder öffentliche Aufgaben noch Befugnisse; sein Votum ist irrelevant und deshalb zur Aufgabenerledigung ungeeignet.
4. Von Datenverarbeitung im Auftrag (§ 7 SächsDSG) kann nicht gesprochen werden, weil die Mitglieder der Untersuchungskommission weisungsfrei, unbeeinflußt und eigenverantwortlich handeln sollen.
5. Ob die sachgemäße Untersuchung der im Stadtrat und in der Öffentlichkeit erhobenen Vorwürfe gegen leitende Mitarbeiter der Stadtverwaltung Leipzig bzw. eines ihrer Unternehmen - nachdem sich der Stadtrat bereits mehrfach mit dieser Angelegenheit eingehend befaßt hat - zu den "Geschäften der laufenden Verwaltung" im Sinne des § 53 Abs. 2 Satz 1 SächsGemO gehört, vermag ich nicht abschließend zu beurteilen.
6. Es ist zu bezweifeln, daß sämtliche Personen, auf die sich diese Informationen beziehen, formgültig im Sinne des § 4 SächsDSG ihre Einwilligung erklären werden; jedenfalls dürfte es sehr aufwendig sein, dies im einzelnen sicherzustellen.
   Wesentlicher ist aber folgendes: Eine verfassungskonforme Auslegung des § 4 SächsDSG verbietet eine Ausdehnung der Aufgaben und der Befugnisse der öffentlichen Verwaltung auf alle Fälle, in denen die Betroffenen in die Verarbeitung ihrer personenbezogenen Daten einwilligen. Der Grundsatz der Gesetzmäßigkeit der Verwaltung verbietet eine Ausdehnung der Aufgaben öffentlicher Stellen in Bereiche hinein, die ersichtlich nicht zum gesetzlichen oder traditionellen Aufgabenkreis gehören. So ist anerkannt, daß die Einwilligung keinesfalls im hoheitlichen Bereich oder in der Personalverwaltung eine erlaubte Konstruktion oder ein Notbehelf zur sachgemäßen Erledigung von Verwaltungsaufgaben ist. Dies zum einen wegen der Begrenzung der Verwaltung auch in den genannten Bereichen auf gesetzliche Aufgaben und Befugnisse ("Wesentlichkeitstheorie"), und weil zum anderen der Betroffene in seiner speziellen Situation die Einwilligung nicht vollkommen freiwillig abgibt.
7. Die Zulässigkeit der Übermittlung personenbezogener Daten an Privatpersonen richtet sich folglich nach § 15 SächsDSG. Das Sächsische Datenschutzgesetz entzieht personenbeziehbare Informationen, die bereits öffentlich erörtert wurden oder aus anderen Gründen öffentlich zugänglich sind, nicht dem Schutzbereich der Norm. So sind gesammelte Presseinformationen, Protokolle öffentlicher Ratssitzungen, öffentlich erörterte Grundstücksveräußerungsvorgänge sowie die sonstigen Unterlagen, die den Mitgliedern der Untersuchungskommission bislang übergeben worden sind, personenbeziehbare Informationen.
   Auch die übrigen Voraussetzungen, an die § 15 SächsDSG eine zulässige Datenübermittlung an Private knüpft, liegen nicht vor: Insbesondere ist nicht ersichtlich, daß die Datenübermittlung zur Erfüllung einer Aufgabe der Stadt erforderlich wäre (siehe oben).
8. Der Oberbürgermeister hat der "Kommission" den Auftrag gegeben, "eine Bewertung unter juristischen *und moralischen* Gesichtspunkten vorzunehmen".

Nachdem er keinen Anlaß für weitere dienstliche und interne Untersuchungen sah, war die Angelegenheit - aus seiner Sicht - juristisch hinreichend aufgeklärt. Moralische Urteile stehen uns allen in der Verwaltung aber nicht zu; sie gehören nicht zur Aufgabe der öffentlichen Verwaltung.

9. Überdies: Zu einer weiteren juristischen Aufklärung erscheinen mir auch zwei der Kommissionsmitglieder aus fachlichen Gründen als für die Aufgabe ungeeignet. Außerdem wäre ein Verfahren mit dem Ziel der rechtlichen Aufklärung auf der Grundlage von vornherein feststehender beschränkter Aktenkenntnis - wie in Niedersachsen - ungeeignet.

Ich habe den Oberbürgermeister wegen der vorgenannten Bedenken dringend gebeten, von der weiteren Beauftragung der Untersuchungskommission abzusehen, und die Aufsichtsbehörde informiert.

Es zeichnet sich ab, daß der Oberbürgermeister bedauerlicherweise meine Warnungen nicht hinreichend berücksichtigt hat und die Angelegenheit datenschutzrechtlich daher noch nicht zu Ende ist.

5.5.4 Verbandstätigkeit eines Datenverarbeitungs-Zweckverbandes

Einer der drei Datenverarbeitungs-Zweckverbände, der in besonderer Weise die Lizenzverfahren aus Baden-Württemberg favorisierte, indem er gegenüber seinen Mitgliedsgemeinden den Eindruck erweckte, daß der Einsatz anderer kommunaler Verfahren unzulässig sei, verweigerte mir eine Stellungnahme. Er begründete seine ablehnende Haltung mit dem Hinweis, daß der Sachverhalt den Datenschutz "nicht betreffe".

Der Zweckverband wurde von mir daraufhin über die Rechtslage aufgeklärt:

Der Zweckverband ist als Körperschaft des öffentlichen Rechts gemäß § 25 Satz 1 SächsDSG verpflichtet, den Datenschutzbeauftragten und seine Beauftragten bei der Erfüllung ihrer Aufgaben zu unterstützen. Es gehört zu meinen Aufgaben, sächsischen öffentlichen Stellen Empfehlungen zur Verbesserung des Datenschutzes zu geben und sie in Fragen des Datenschutzes zu beraten (vgl. § 27 Abs. 4 SächsDSG). Um diesen Beratungsauftrag - der auch den Einsatz personenbezogener Verfahren in den Gemeinden umfaßt - erfüllen zu können, benötige ich umfassende, mit der kommunalen Datenverarbeitung unmittelbar und mittelbar im Zusammenhang stehende Informationen. So ist es für mich wichtig zu wissen, welche kommunalen Verfahren von wem angeboten bzw. aus welchem Grund bestimmte Verfahren nicht angeboten werden und welche Kommunen welche Verfahren im Rahmen ihrer verfassungsmäßig garantierten Organisationshoheit einzusetzen beabsichtigen. Wirkt nun der Zweckverband auf die kommunale Datenverarbeitungs-Infrastruktur und damit auf das kommunale Selbstverwaltungsrecht ein, indem er z. B. den Einsatz kommunaler Software anderer Hersteller zu verhindern sucht, ist sehr wohl meine Zuständigkeit

gegeben. Insoweit besteht für den Zweckverband die Unterstützungspflicht nach § 25 Satz 1 SächsDSG. Kommt der Zweckverband dieser Verpflichtung jedoch nicht nach, muß dies eine Beanstandung nach § 26 SächsDSG nach sich ziehen.

Nachdem ich auch die Kommunalaufsichtsbehörde eingeschaltet hatte, erhielt ich - wenn auch widerwillig - die gewünschten Informationen.

5.5.5 Übertragung von Vollstreckungsaufgaben auf Private

Ein Landratsamt bat mich um Stellungnahme, ob und ggf. unter welchen Voraussetzungen Vollstreckungen auf Private übertragen werden dürfen.
Ich kam zu dem Ergebnis, daß Vollstreckungen nach dem SächsVwVG zum Kernbereich hoheitsrechtlicher Verwaltung gehören, die nicht auf private Inkassobüros übertragen werden können.
Das Landratsamt hat auf die Beauftragung einer Privatfirma verzichtet.

5.5.6 Fernmeldeerschließung durch die Deutsche Telekom AG (Telekom)

Der Bürgermeister einer sächsischen Stadt informierte mich über das Vorhaben der Telekom, die Grundstücke in den Umlandgemeinden von Chemnitz "fernmeldemäßig" zu erschließen. Hierzu sollten der Telekom die Namen und Anschriften der Grundstückseigentümer im Wege der "Amtshilfe" zur Verfügung gestellt werden.

Die Frage der Zulässigkeit der Übermittlung von Grundstückseigentümerdaten an die Telekom habe ich wie folgt beurteilt:

Nach § 8 TKV 1995 kann die Telekom seit 1. Januar 1996 den Abschluß eines Vertrages, der die Inanspruchnahme von Monopoldienstleistungen zum Gegenstand hat (hierzu zählt auch ein Telefonanschluß), von der Vorlage einer Grundstückseigentümererklärung abhängig machen. Diese Bestimmung regelt also das Verhältnis zwischen Telekom und Grundstückseigentümer und ist nicht als Rechtsgrundlage für Datenerhebungen durch die Telekom bei den Gemeinden, aber auch nicht als Datenübermittlungsbefugnis für die Gemeinden zu verstehen.

Vielmehr ist vor Datenübermittlungen der von der Telekom gewünschten Art zu prüfen, ob Spezialvorschriften oder das Sächsische Datenschutzgesetz als Zulässigkeitsvoraussetzung in Frage kommen.

1. *Anwendung von Spezialvorschriften*
   Stammen die Grundstückseigentümerdaten aus der gemeindlichen Grundsteuerdatei, verböte § 30 AO (Steuergeheimnis) die Datenübermittlung an die Telekom, wenn diese keine öffentliche Stelle wäre. Solange der Telekom jedoch ein ausschließliches Recht nach dem Postgesetz oder dem Gesetz über Fernmeldeanlagen zusteht - und das ist bei der Fernmeldeerschließung der Fall - ist sie (bis spätestens 31. Dezember

1997) als öffentliche Stelle anzusehen.

Nach § 31 Abs. 3 AO sind die für die Verwaltung der Grundsteuer zuständigen Behörden (Stadtsteueramt) berechtigt, die nach § 30 AO geschützten Namen und Anschriften von Grundstückseigentümern u. a. zur Erfüllung "sonstiger öffentlicher Aufgaben" den hierfür zuständigen Behörden auf Ersuchen mitzuteilen, soweit nicht überwiegende schutzwürdige Interessen des Betroffenen entgegenstehen.

Auch wenn die Fernmeldeerschließung als öffentliche Aufgabe angesehen werden kann, sind jedoch bei der Abwägung, ob dem Auskunftsersuchen der Telekom gefolgt werden kann, die allgemeinen Grundsätze wie Verhältnismäßigkeit und Erforderlichkeit zu beachten.

Da die Grundstückseigentümer nicht verpflichtet sind, Grundstücke fernmeldemäßig erschließen zu lassen, manche diese Erschließung auch nicht wünschen, genügte eine Übermittlung der Daten aller Grundstückseigentümer an die Telekom dem Grundsatz der Erforderlichkeit nicht, sie wäre daher unzulässig. Der mit jeder Datenübermittlung einhergehende Eingriff in das Recht auf informationelle Selbstbestimmung ist außerdem schon deshalb nicht erforderlich, weil der Telekom zur Erreichung ihres Zwecks auch andere Mittel und Wege zur Verfügung stehen. Beispielsweise könnten die Grundstückseigentümer durch Postwurfsendung bzw. durch eine Medienkampagne motiviert werden, sich bei Interesse an einer Fernmeldeerschließung mit der Telekom in Verbindung zu setzen.

2. *Anwendung des Sächsischen Datenschutzgesetzes*
   Auch wenn die Daten aus anderen gemeindlichen Unterlagen stammen sollten, wäre das Ergebnis kein anderes. Die Voraussetzungen des § 13 SächsDSG sind insbesondere im Hinblick auf die fehlende Erforderlichkeit nicht erfüllt.

Von dieser Rechtsauffassung habe ich den anfragenden Bürgermeister, die Deutsche Telekom AG sowie den für die Datenschutzkontrolle der Telekom zuständigen Bundesbeauftragten für den Datenschutz und das Regierungspräsidium Chemnitz unterrichtet.

5.5.7 Ausstellung eines "Familienpasses" zur Erlangung von Vergünstigungen

Eine Stadtverwaltung beabsichtigte - ohne eine Rechtsgrundlage - die Ausstellung eines "Familienpasses" zur Erlangung von Vergünstigungen (bei Eintrittspreisen, bei Benutzung öffentlicher Verkehrsmittel usw.) u. a. vom Einkommen der Interessenten abhängig zu machen. Die Antragsteller sollten nachstehende Unterlagen vorlegen:
- Personalausweis / Reisepaß
- Familienstammbuch
- Kopie der Steuerkarte
- Kopie des vorjährigen Steuerbescheids
- Wohngeldbescheid / Mietvertrag
- Einkommensnachweise in Kopie

Diese Datenerhebungen habe ich wie folgt beurteilt:

1. Zulässigkeit der Datenerhebung und -speicherung

Während die Vorlage des Personalausweises oder des Reisepasses (als Identitätsnachweis) unproblematisch ist, soweit keine Speicherung bei der den Familienpaß ausgebenden Stelle erfolgt, bestehen hinsichtlich der anderen geforderten Unterlagen Bedenken.
Die Verpflichtung zur Vorlage des Familienstammbuches, in dem sich weitaus mehr Daten befinden, als zur Feststellung der Anzahl der Familienmitglieder erforderlich ist, erscheint unverhältnismäßig. Insbesondere aber die Forderung, *Kopien* von Steuerkarte, Steuerbescheid und Einkommensnachweisen vorzulegen, deutet darauf hin, daß die dem Antrag beizufügenden Unterlagen in den Familienpaßakten gespeichert werden sollen. Die Speicherung solch sensibler Daten in den Unterlagen der Familienpaßstelle ist jedoch nicht zur gesetzlichen Aufgabenerfüllung erforderlich und daher unzulässig. Vielmehr dürfte der *neutrale* Hinweis "Der Berechtigungsnachweis wurde erbracht" genügen.

2. Geeignetheit der geforderten Nachweise

Fraglich ist aber auch, ob die geforderten Unterlagen als Nachweis der Berechtigung geeignet sind. Außerdem würden bezüglich des Familienverbandes Doppelerhebungen und Doppelspeicherungen stattfinden: Die Meldebehörde hat diese Daten bereits vorliegen (Anzahl der Familienmitglieder kann dem Melderegister entnommen werden; Vorlage des Familienstammbuches ist nicht erforderlich).

a) Kopie der Steuerkarte

Die Steuerkarte des laufenden Jahres liegt beim Arbeitgeber und enthält noch keine Lohneintragungen. Die Steuerkarte des Vorjahres liegt beim Finanzamt. Die Steuerkarte ist zudem nicht geeignet, das Familienbruttoeinkommen nachzuweisen.

b) Kopie des vorjährigen Steuerbescheides
Der *vorjährige* Steuerbescheid liegt dem Antragsteller regelmäßig noch nicht vor. Steuerbescheide sind aus vielerlei Gründen auch nicht geeignet, das Familienbruttoeinkommen nachzuweisen.

c) Wohngeldbescheid / Mietvertrag
Beide sind nicht geeignet, das Familienbruttoeinkommen nachzuweisen.

d) Einkommensnachweise in Kopie
Wie a bis c.

Fazit:
Der mit der Antragstellung und Familienpaßerteilung verbundene Verwaltungsaufwand, der darüber hinaus nicht unerheblich die Privatsphäre der Antragsteller berührt, ist ungeeignet und - vorausgesetzt, die Daten wären geeignet - unverhältnismäßig.

Vorschlag:
Die Ausgabe der Familienpässe orientiert sich ausschließlich an der Anzahl der Kinder, also unabhängig vom Familieneinkommen. Dies wäre datenschutzgerecht, familienfreundlich und bürgernah. Dabei wird in Kauf genommen, daß sich auch (wohl nur wenige) Familien mit höherem Einkommen um den Familienpaß bemühen. Das wäre aber bei "reichen" Alleinerziehenden entsprechend dem Vorschlag der Gemeinde auch möglich gewesen.

Die Stadt hat mitgeteilt, daß auf die kritisierten Unterlagen verzichtet und meinem Vorschlag gefolgt wird. Dem "Familienpaß" wird das Familieneinkommen nicht mehr zugrundegelegt. Bei der Beantragung ist lediglich der Personalausweis oder der Schülerausweis vorzuzeigen.

5.5.8 Inhalt des Auskunftsanspruchs

Gemäß § 17 Abs. 1 Nr. 1 SächsDSG ist dem Betroffenen auf Antrag Auskunft über die zu seiner Person gespeicherten Daten zu erteilen. Aus dieser Formulierung ("über") folgerte eine Kommune, es sei ausreichend, wenn dem Antragsteller *allgemein* mitgeteilt wird, welche *Art* der Daten gespeichert sind (also z. B. anstelle von: "Müller, Gerd" lediglich: "Name, Vorname").

Ich habe der Kommune mitgeteilt, daß aufgrund des Auskunftsanspruchs den Antragstellern der *genaue Inhalt* der gespeicherten personenbezogenen Daten mitgeteilt werden muß. Nur in diesem Fall ist der Betroffene in der Lage, die gespeicherten personenbezogenen Daten auf Richtigkeit und Vollständigkeit zu prüfen und ggf. sein in § 18 SächsDSG gewährtes Recht auf Berichtigung geltend zu machen.

5.5.9 Personenbezogene Daten in einer Ortschronik

Eine Gemeinde hatte erkannt, daß die Veröffentlichung personenbezogener Daten in einer Ortschronik nicht unproblematisch ist, und bat um datenschutzrechtliche Beratung.

In einem Gespräch habe ich klargestellt, daß die Chronisten, die gemäß § 17 SächsGemO für ein gemeindliches Ehrenamt bestellt wurden und somit Amtsträger i. S. v. § 11 StGB sind, an die Verschwiegenheitspflichten des § 19 Abs. 2 SächsGemO ebenso gebunden sind wie an die Einhaltung sonstiger datenschutzrechtlicher Bestimmungen. Die Gemeinde habe ich aufgefordert, die Chronisten auf das Datengeheimnis zu verpflichten.

Die Chronisten wurden darauf hingewiesen, daß personenbezogene Datenerhebungen grundsätzlich nur auf freiwilliger Basis erfolgen dürfen. Die spätere Veröffentlichung der personenbezogenen Daten in der Ortschronik ist von der Einwilligung der (noch lebenden) Betroffenen abhängig (Art. 33 SächsVerf, § 4 Abs. 1 Nr. 2 und Abs. 2 und 3 SächsDSG). Dies gilt allerdings nicht für aus öffentlich zugänglichen Quellen entnommene Informationen und auch nicht für Daten von Personen der Zeitgeschichte (z. B. Bürgermeister, Gemeinderatsmitglieder, Dorfärzte u. ä.).

Abschließend habe ich darauf hingewiesen, daß eine Informationsbeschaffung aus behördlichen Unterlagen, z. B. aus dem Melderegister, aus dem Standesamt, aus dem gemeindlichen Steueramt oder aus einem Archiv auf die gesetzlichen Schranken des SächsMG, des PStG, der AO und des SächsArchG stieße.

Die Gemeinde sagte mir zu, daß die bisher erstellten Teile der Chronik im Hinblick auf evtl. Verletzungen des Persönlichkeitsrechts untersucht und bereinigt würden.

5.6 Baurecht; Wohnungswesen

Anbieterdatei im Hochbauamt

Ein Unternehmer teilte mir mit, daß das Hochbauamt Daten von sämtlichen ortsansässigen Unternehmern auf freiwilliger Grundlage speichert, um diese bei beschränkten Ausschreibungen oder freihändigen Vergaben zur Angebotsabgabe auffordern zu können.

Gegen das Anlegen einer solchen "Anbieterdatei" habe ich keine grundsätzlichen datenschutzrechtlichen Einwände erhoben. Allerdings müssen alle Firmen Gelegenheit haben, sich in die Listen einzutragen. Die Liste dürfte im übrigen wegen Betriebsschließungen und -eröffnungen schnell überholt sein. Für unverhältnismäßig

habe ich jedoch gehalten, daß die Unternehmer zum Nachweis ihrer "wirtschaftlichen und finanziellen Leistungsfähigkeit" (VOB/A 8 Abs. 2) die Ablichtung der letzten Beitragsentrichtung an die Krankenkasse beibringen sollten.

Das Hochbauamt hat das "Erfassungsblatt" daraufhin geändert. Verlangt wird von den Unternehmern nunmehr lediglich die *Erklärung*, daß sie ihrer Verpflichtung zur Zahlung fälliger Steuern und Abgaben sowie der Beiträge zur gesetzlichen Sozialversicherung nachgekommen sind. Hiergegen bestehen keine datenschutzrechtlichen Bedenken mehr. Außerdem wurde mir zugesagt, daß die bereits beigebrachten Ablichtungen der letzten Beitragsentrichtungen umgehend vernichtet werden.

5.7 Statistikwesen

5.7.1 VO über den Einsatz von Datenverarbeitungsanlagen in kommunalen Statistikstellen

Nach § 9 Abs. 1 SächsStatG dürfen Kommunalstatistiken nur von einer besonderen, aussschließlich für statistische Aufgaben zuständigen Stelle der Gemeinde (oder sonstigen kommunalen Körperschaft, vgl. § 9 Abs. 7 SächsStatG) durchgeführt werden, die räumlich, organisatorisch und personell von anderen Verwaltungsstellen getrennt ist. Das ist die sogenannte *kommunale Statistikstelle* (kStSt).

Für den Fall, daß in dieser kStSt Einzelangaben mittels Datenverarbeitungsanlagen (DVAen) verarbeitet werden, schreibt § 9 Abs. 2 SächsStatG *zusätzliche organisatorische, personelle und technische Maßnahmen* vor, welche die Abschottung gegenüber anderen Verwaltungsdaten sowie die Bindung der Daten an den statistischen Zweck gewährleisten sollen, und beauftragt und ermächtigt das SMI, Näheres dazu durch eine Rechtsverordnung zu bestimmen.

Diese VO ist am 1. März 1996 in Kraft getreten (KommStatVO, SächsGVBl. S. 81).

An der Ausarbeitung dieser Verordnung war ich beteiligt: Mit großem Aufwand habe ich viel an Verbesserungen gegenüber dem ursprünglichen Entwurf erreicht, und ich habe dabei in dieser Spezialmaterie auch selbst einiges dazugelernt. Um so ärgerlicher ist es, daß die Verordnung nunmehr an etlichen Stellen *gegen* meinen Rat Formulierungen enthält, die schwere handwerkliche Fehler darstellen.

Rechtsvorschriften, die gegen die Logik verstoßen oder völlig Überflüssiges enthalten, bringen den Gesetzgeber - hier den Verordnungsgeber - in Mißkredit und schaden dadurch dem Rechtsstaat im allgemeinen und im vorliegenden Fall auch dem Datenschutz im besonderen. Die Aufgabe, Rechtsvorschriften so zu gestalten, daß sie die Verfassungsgebote der Bestimmtheit und - im Falle des Datenschutzrechtes

bekanntlich von gesteigerter Bedeutung - der Klarheit erfüllen, wird durch handwerkliche Fehler in den Hintergrund gedrängt: Die Erfüllung dieser Gebote des Rechtsstaates scheint in unerreichbare Ferne gerückt zu werden.

Einzelheiten zur Anwendung dieser VO darzulegen - wofür ein praktisches Bedürfnis seitens der Kommunen besteht - müßte hier zu weit führen.

5.7.2 VO über die Frauenförderungs-Statistik

Das Sächsische Statistikgesetz steckt den rechtlichen Rahmen für alle Landesstatistiken sowie die Tätigkeit ab, die kommunale Körperschaften sowie die sonstigen der Aufsicht des Freistaates Sachsen unterstehenden juristischen Personen des öffentlichen Rechts auf dem Gebiet der Statistik entfalten dürfen. Für den Regelfall schreibt das Gesetz vor, daß die Durchführung einer Statistik einer Anordnung durch Rechtsvorschrift, also durch Gesetz, Satzung oder Rechtsverordnung, bedarf; vgl. §§ 6, 8 Abs. 1 Satz 2 SächsStatG, Ausnahmen sehen § 6 Abs. 4 sowie § 7 Abs. 1 vor.

Die erste Anordnung einer sächsischen Landesstatistik ist leider rechtlich weitgehend fehlgeschlagen. Es handelt sich um die im Einvernehmen mit dem SMI ergangene Verordnung der Sächsischen Staatsministerin für Fragen der Gleichstellung von Frau und Mann über die statistischen Angaben für die Frauenförderung in Dienststellen im Freistaat Sachsen, kurz die Sächsische Frauenförderungsstatistikverordnung (SächsFFStatVO), vom 22. August 1995.

Die Fehler, mit denen diese Verordnung behaftet ist, sind zusammengefaßt folgende:

(a) Die Verordnung schreibt erheblich mehr an Erhebung personenbezogener Daten vor, als das Gesetz, in der Ermächtigungsgrundlage § 5 SächsFFG, erlaubt.
(b) Die Staatsministerin hat in §§ 3 f. der Verordnung für die Durchführung der Statistik ein Verfahren vorgeschrieben, das die Aggregierung der Daten der einzelnen Dienststellen ganz beträchtlich hinausschiebt. Die Einzelangaben jeder Dienststelle werden erst den Ministerien gemeldet und von diesen dann der Staatsministerin überlassen, die die Daten dann zur Aggregierung dem Statistischen Landesamt mitteilt.
Diese Verzögerung der Aggregierung der Daten ist nicht erforderlich. Daher verstößt dieses Verfahren der Mitteilung der Daten nach §§ 3 f. der VO gegen das statistikrechtliche Grundgebot der frühestmöglichen Anonymisierung (§ 1 Abs. 2 SächsStatG). Die Einbeziehung der Ministerien und der Staatsministerin in die Übermittlungskette dürfte folglich rechtswidrig sein.
(c) Nach § 2 Abs. 3 SächsFFStatVO soll den mitteilungspflichtigen Dienststellen die Verwendung von Erhebungsvordrucken von der Staatsministerin durch Verwaltungsvorschrift vorgeschrieben werden.
Verwaltungsvorschriften können wirksam nur insoweit erlassen werden, als Fachaufsicht besteht. Es ist nicht ersichtlich, und die Staatsministerin hat bisher

zumindest mir gegenüber auch keinerlei Gründe dafür angeführt, daß diese Fachaufsicht z. B. gegenüber den anderen Ressorts, den Kommunen, den Universitäten und anderen Körperschaften des öffentlichen Rechts besteht. Die Staatsministerin ist nach geltendem Recht im Verhältnis zu diesen Stellen weder oberste Frauenförderungsbehörde noch obere Frauenförderungsstatistikbehörde.

(d) § 6 Abs. 8 (ähnlich § 8 Abs. 3) SächsStatG schreibt vor, daß bei der Vorbereitung von Rechts- und Verwaltungsvorschriften, durch die Statistiken angeordnet werden, der Sächsische Datenschutzbeauftragte zu beteiligen ist. Zwar konnte ich im Frühjahr 1995 - ausführlich und kritisch - zum damaligen Stand des Entwurfs Stellung nehmen. Später hat man mich jedoch nicht mehr in der vom Gesetz gebotenen Weise beteiligt. Ich habe diese Verfahrensweise förmlich beanstandet.

In meinen Stellungnahmen hatte ich frühzeitig darauf hingewiesen, daß im *staatlichen* Bereich für das von der Staatsministerin geplante Erhebungsprogramm gänzlich unabhängig von der Verordnung ein weiter Spielraum besteht: Als *Statistik im Verwaltungsvollzug* (§ 7 Abs. 1 SächsStatG) bedürfte die Erhebung der Daten keiner besonderen Rechtsgrundlage; lediglich die *pflichtweise* Beteiligung von Kommunen, Universitäten und anderen Selbstverwaltungskörperschaften läßt sich nur mittels einer Rechtsvorschrift erreichen.
Daß ich das Ziel, eine ausreichende gesetzliche Grundlage für eine aussagekräftige Statistik aller Dienststellen zustande zu bringen, unterstützen werde, habe ich der Staatsministerin gegenüber hervorgehoben.

5.7.3 Grundsatzfrage: Privatisierung der Durchführung amtlicher Statistiken, insbesondere kommunaler Statistiken

In der Frage, inwieweit amtliche Statistiken, insbesondere solche kommunaler Körperschaften (vgl. § 8 Abs. 4 SächsStatG), durch private Dritte durchgeführt werden dürfen, kann man noch nicht auf eine gesicherte Rechtspraxis zurückgreifen. Nach längeren Überlegungen meine ich zu einem zuverlässigen Ergebnis gekommen zu sein, mit dem von mir in der Vergangenheit bereits vereinzelt vertretene Lösungsansätze fortentwickelt werden. Dies gilt insbesondere für die von mir in der Bekanntmachung zur Datenverarbeitung im Auftrag (§ 7 SächsDSG) und zur Rechtsstellung des beauftragten Unternehmers (§ 2 Abs. 2 SächsDSG) vom 3. November 1993 (SächsABl. S. 1304) unter Nr. 12 angeführten Beispiele.

(1) § 9 Abs. 1 SächsStatG ist entgegen dem ersten Anschein nicht so auszulegen, daß Kommunen Statistiken vollständig (d. h. in sämtlichen Phasen der statistischen Datenverarbeitung) in dem Sinne ausschließlich von der kommunalen Statistikstelle durchführen lassen müssen, daß private Dritte daran nicht beteiligt werden dürfen. Vielmehr ist Regelungszweck des § 9 Abs. 1 SächsStatG, daß keine andere kommunale Stelle als die kommunale Statistikstelle mit der Durchführung von Statistiken betraut werden darf. Die Vorschrift begründet mithin innerhalb der gesamten Kommunalverwaltung eine ausschließliche sachliche Zuständigkeit der kommuna-

len Statistikstelle für die Durchführung von - amtlichen - Primärstatistiken. Das ergibt sich aus der Entstehungsgeschichte und dem Zweck der Institution der kommunalen Statistikstelle im deutschen Statistikrecht mit großer Eindeutigkeit.
Ein Verbot für die Kommunen, z. B. private Meinungsforschungsinstitute, Verkehrsplaner oder Wohnungswirtschaftsfachleute mit der Durchführung von Statistiken zu beauftragen, läßt sich daher dieser Vorschrift nicht entnehmen.

(2) Mangels eines solchen rechtlichen Verbotes bleiben die allgemeinen Vorschriften maßgebend: Daß im Sächsischen Statistikgesetz eine Vorschrift über Datenverarbeitung im Auftrag fehlt, besagt nicht, daß diese im Anwendungsbereich des Gesetzes verboten wäre. Sie ist in den von § 7 SächsDSG gezogenen Grenzen erlaubt. Es gibt keinen Grund, daß für die Datenverarbeitung durch den beauftragten Unternehmer, wie sie in § 2 Abs. 2 SächsDSG geregelt ist (sog. Funktionsübertragung), etwas anderes gelten sollte.

(3) Die Zulässigkeit der Beteiligung eines Dritten, insbesondere eines privaten Meinungsforschungsunternehmens, an der Durchführung - amtlicher - kommunaler Statistiken bemißt sich daher mangels einer einschlägigen Vorschrift im Statistikrecht nach allgemeinem Datenschutzrecht, insbesondere § 7 (*nachstehend Fallgruppe 3*) oder aber § 2 Abs. 2 (*nachstehend Fallgruppe 2*) SächsDSG.
Hiervon unterschieden werden muß die Beauftragung Privater mit der Durchführung einer nichtamtlichen Statistik (*nachstehend Fallgruppe 1*).

(4) Im einzelnen gilt für diese drei Fallgruppen der Beteiligung Privater an der Durchführung von Statistiken, die von öffentlichen Stellen veranlaßt werden, folgendes:

Fallgruppe 1:

Eine *nichtamtliche* Statistik wird durchgeführt, wenn der Private (Meinungsforschungsinstitut oder ähnliches) dem zu Befragenden gegenüber ausschließlich als Privater auftritt, so daß für den Befragten kein Bezug zu einer öffentlichen Stelle als Auftraggeber erkennbar ist. In diesem Fall steht der öffentliche Auftraggeber rechtlich nicht anders als ein privater Auftraggeber, der eine auf statistische Erhebungen gestützte Studie bestellt. Es kommt hier auf den objektiven Erklärungswert (das Erscheinungsbild für die Öffentlichkeit) des Verhaltens des auftretenden Privaten und auch seines Auftraggebers an.
Dies gilt jedoch nur, wenn dem öffentlichen Auftraggeber nicht die erhobenen personenbezogenen Daten bzw. Einzelangaben übermittelt werden, sondern nur Daten, die hinlänglich aggregiert sind, nämlich so, daß der öffentliche Auftraggeber keine Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (vgl. § 3 Abs. 1 SächsDSG) oder auch - wegen der größeren Reichweite des statistikrechtlichen Schutzes der Privatsphäre - juristischer oder toter natürlicher Personen übermittelt erhält. Anders ausgedrückt: Wegen des privatsphäreschützenden Zweckes des größten Teiles des Statistikrechtes muß so viel von den Phasen der Durchführung einer Statistik vom privaten Auf-

tragnehmer durchgeführt worden sein, daß der öffentliche Auftraggeber kein Datenmaterial erhält, welches noch die Anwendung dieser Schutzregelungen erforderlich machte. Für die Statistik-Phasen Darstellung und Analyse gilt dies nicht mehr.

Zusammengefaßt: Eine von einem Träger öffentlicher Gewalt veranlaßte Erhebung von Daten zu statistischen Zwecken ist dann keine amtliche Statistik - und damit weder dem Sächsischen Statistikgesetz noch dem Sächsischen Datenschutzgesetz unterworfen -, wenn der durchführende Private (a) in keiner Weise seinen öffentlichen Auftraggeber zu erkennen gibt und dieser auch nicht etwa selbst sich gegenüber der Öffentlichkeit 'hinter' die vom privaten Auftragnehmer durchgeführte Statistik stellt und wenn (b) die gesamte Statistik bis einschließlich der Phase der hinreichend anonymisierten Aufbereitung (als Tabellenwerk) dem Privaten übertragen, also nicht von dem öffentlichen Auftraggeber durchgeführt wird.

(Im Ergebnis genauso, allerdings den in § 1 Satz 1 BStatG, § 1 Abs. 1 Satz 1 SächsStatG nicht verwendeten Ausdruck "Auswertung" benutzend, der 17. TB des HessDSB von 1988, S. 104.)

Das erforderliche vollständig private Erscheinungsbild der Umfrage wird meiner Meinung nach nicht dadurch zerstört, daß die öffentliche Stelle den Umfrageauftrag in der gegebenenfalls rechtlich gebotenen Weise öffentlich ausschreibt.

Zu den nichtamtlichen Statistiken zählt es auch, wenn Statistiken von öffentlich-rechtlich organisierten *Hochschulen* zu Forschungszwecken durchgeführt werden, wenn diese also Daten über Massenerscheinungen erheben, sammeln, aufbereiten, darstellen und analysieren. Denn soweit diese Hochschulen nicht ihren bzw. den Lehr- und Forschungsbetrieb verwalten, also bei der Datenerhebung nicht an die Eigenschaft des Betroffenen, Hochschulangehöriger zu sein, anknüpfen, üben sie keine öffentliche Gewalt aus, sind die von ihnen mittels statistischer Methoden durchgeführten Untersuchungen keine amtliche Statistik.
Das bedeutet: Soweit die in öffentlich-rechtlicher Trägerschaft organisierte Hochschule forscht und dazu Massenerscheinungen mittels Erhebung personenbezogener Daten untersucht, handelt sie gerade nicht als Träger öffentlicher Gewalt und ist sie daher statistikrechtlich und allgemein datenschutzrechtlich wie ein Privater anzusehen.
Im Verschweigen des - in diesem Falle *öffentlichen* - Auftraggebers gegenüber den Befragten liegt kein Verstoß gegen Treu und Glauben (§ 28 Abs. 1 Satz 2 BDSG) oder gegen einen für Befragungsunternehmen bzw. empirisch tätige Sozialwissenschaftler geltenden Ehrenkodex.
In diesen Fällen bedarf eine Umfrage, d. h. die Durchführung einer Statistik, demzufolge keiner Rechtsvorschrift als Rechtsgrundlage.

Fallgruppe 2:

Durchführung einer amtlichen Statistik oder von Teilen einer amtlichen Statistik

durch einen beauftragten Unternehmer:

Gemäß § 2 Abs. 2 SächsDSG gelten natürliche und juristische Personen des Privatrechts als öffentliche Stellen im Sinne des Sächsischen Datenschutzgesetzes, soweit sie Aufgaben der öffentlichen Verwaltung wahrnehmen. Dem Beauftragten wird eine von Hause aus von einem Träger öffentlicher Verwaltung wahrzunehmende Aufgabe zur selbständigen Erledigung übertragen, und zwar nicht durch Rechtsvorschrift, sondern durch Vertrag. Im Vordergrund eines solchen Vertrages steht nicht die technische Hilfstätigkeit bei der Verarbeitung personenbezogener Daten, sondern die eigenständige, nach außen gerichtete Verwaltungstätigkeit. (Der Beauftragte nutzt die Datenverarbeitung nur als Hilfsmittel für diese eigene - und eigentliche - Aufgabe.) Der beauftragte Unternehmer tritt nach außen als solcher auf, d. h. er weist auf seinen Auftraggeber, das bestehende Auftragsverhältnis und den Umstand der Durchführung einer Aufgabe der öffentlichen Verwaltung durch sich hin oder gibt dies zumindest deutlich zu erkennen. Dazu gehört auch der Fall, daß der Träger öffentlicher Verwaltung nur einen Teil der Durchführung einer Statistik, aber eben nach außen erkennbar, dem Privaten überträgt, beispielsweise nur die Erhebung und vielleicht auch noch Sammlung, nicht aber die Aggregierung der Daten.

Beispiel: Die X-GmbH führt eine Umfrage zur Stadtentwicklung im Auftrag der Stadt von der Erhebung bis zur Analyse der Daten durch. Sie tritt den Befragten gegenüber offen als im Auftrag der Stadt handelnd auf ("ich komme von der Firma X; wir führen im Auftrag der Stadt eine Umfrage durch"; die schriftlichen Unterlagen weisen in gleicher Weise auf *beide* Akteure hin).

Oder: Ein Institut oder ein Lehrstuhl der Universität führt im Auftrag der Stadt eine Umfrage durch. Auf dem Briefkopf des Anschreibens erscheinen beide, die Universität und die Stadt.

Aus der Anwendbarkeit des § 2 Abs. 2 SächsDSG auf das Statistikrecht, insoweit es ein datenschutzrechtliches Spezialgebiet ist, folgt:

Der mit der Durchführung der Statistik beauftragte Unternehmer (Private) gilt als öffentliche Stelle. Genauer gesagt ist er nach denjenigen datenschutzrechtlichen Regeln zu behandeln, die für die Stelle gelten, die ihn beauftragt hat. Denn die Beauftragung (Privatisierung) soll (darf) ja am Datenschutz nichts ändern; das ist der hinter § 2 Abs. 2 SächsDSG stehende Gedanke.
Für die betreffende Tätigkeit des beauftragten Unternehmers gilt daher gemäß § 2 Abs. 1 i. V. m. Abs. 2 Satz 1 SächsDSG das Sächsische Datenschutzgesetz, und soweit diesem speziellere Rechtsvorschriften vorgehen, gemäß § 2 Abs. 4 Satz 1 SächsDSG eben diese spezielleren Regelungen.
Daraus folgt insbesondere: Die Voraussetzungen, die das Sächsische Statistikgesetz für die Durchführung einer Statistik aufstellt, z. B. das Gebot frühestmöglicher Anonymisierung gemäß § 1 Abs. 2, 2. Halbs. SächsStatG oder das Erfordernis, daß

eine Statistik im Regelfall, eine kommunale Statistik immer, einer Rechtsvorschrift als Ermächtigungsgrundlage bedarf, und zwar selbst dann, wenn die Erhebung ohne Auskunftspflicht erfolgen soll (§ 6 Abs. 6 i. V. m. § 8 Abs. 1 SächsStatG), gelten auch in diesem Falle!

Im Fall der Beauftragung durch eine *Kommune* darf sich an der besonderen ausschließlichen Zuständigkeit - und Erforderlichkeit - der kommunalen Statistikstelle (§ 9 Abs. 1 Satz 1 SächsStatG) durch die Beauftragung eines Privaten nichts ändern. Das bedeutet: Nur insoweit der Private der ihn beauftragenden Gemeinde (oder Landkreis oder sonstige kommunale Körperschaft) Daten in der durch Aggregierung hinreichend anonymisierten Form liefert, also so, daß das Zahlenwerk von der kommunalen Statistikstelle der Fachstelle bzw. der Öffentlichkeit bekanntgegeben werden dürfte, bedarf es der Einschaltung, ja der Existenz der kommunalen Statistikstelle nicht. Andernfalls ist jedoch die kommunale Statistikstelle erforderlich und auf seiten der auftragerteilenden Kommune ausschließlich zuständig.

Nicht zu vergessen: Was die betreffende Tätigkeit angeht, unterliegt der private beauftragte Unternehmer kraft Gesetzes der Kontrolle des Sächsischen Datenschutzbeauftragten (vgl. auch § 2 Abs. 4 Satz 2 SächsDSG).

Fallgruppe 3:

Datenverarbeitung im Auftrag, im Sinne von § 7 SächsDSG, liegt vor, wenn Hilfstätigkeiten von (öffentlichen oder privaten) Auftragnehmern wahrgenommen werden. Diese Hilfstätigkeiten dürfen nur den rein technischen Teil der Datenverarbeitung zum Gegenstand haben und erstrecken sich nicht auf das Verwaltungshandeln, dem die Verarbeitung der betreffenden Daten dient. Die eigentliche Verwaltungsaufgabe verbleibt beim Auftraggeber, der als die eigentlich datenverarbeitende Stelle uneingeschränkt für die Erfüllung der Verwaltungsaufgabe und die Einhaltung aller darauf anwendbaren Datenschutz-Vorschriften verantwortlich bleibt (vgl. dazu meine bereits genannte Bekanntmachung vom 3. November 1993, unter Nr. 8 f.).
Bei der Durchführung amtlicher Statistiken können Private, insbesondere Meinungsforschungsinstitute, im Rahmen eines Auftragsdatenverarbeitungs-Verhältnisses also nur einzelne, technische Hilfstätigkeiten wahrnehmen. Bleiben sie dabei den zu Befragenden ausnahmsweise nicht gänzlich verborgen, so muß es offensichtlich sein, daß sie ausschließlich eine Hilfstätigkeit ausüben (z. B. Adreßdrucker).
Dies ist meiner Meinung nach jedoch dann nicht mehr der Fall, wenn der Private - erkennbar im Auftrag der öffentliche Stellen - Fragebögen austeilt. Bekanntlich ist dies im Bereich der Statistik schon nahezu ein Verwaltungsakt (zum Streitstand vgl. Dorer/Mainusch/Tubies Rdnr. 22 zu § 15 BStatG). Dies wäre ein Fall des § 2 Abs. 2 SächsDSG, also der Tätigkeit eines beauftragten Unternehmers.
Ein Beispiel für Datenverarbeitung im Auftrag wäre hingegen: Die Gemeinde läßt lediglich die im Rahmen der Auswertung der erhobenen Daten erforderliche techni-

sche Aufbereitung des Datenmaterials von einem privaten Datenverarbeiter oder Meinungsforschungsunternehmen ausführen.
Gemäß § 7 SächsDSG ist in einem solchen Fall erforderlich:

- In dem mit dem Auftragnehmer abzuschließenden Vertrag muß der Auftragnehmer verpflichtet werden, sich einer den §§ 24 und 25 SächsDSG entsprechenden Kontrolle durch den Sächsischen Datenschutzbeauftragten, einschließlich eigener Unterstützungspflicht gegenüber diesem, zu unterwerfen (weitere Einzelheiten in der erwähnten Bekanntmachung unter Nr. 11).
- In dem Vertrag muß sich der Auftragnehmer ferner zur Wahrung des Statistikgeheimnisses im vollen Umfang des § 18 SächsStatG verpflichten.
- In den Fällen gesteigerter Schutzwürdigkeit der erhobenen Daten, zumindest ab der in der genannten Bekanntmachung unter Nr. 3 unter C genannten Schutzstufe, ist das Personal des Auftragnehmers, soweit es mit der Durchführung der Statistik betraut ist, nach dem *Verpflichtungsgesetz* förmlich zu verpflichten.

Weitere Anforderungen an die Durchführung einer Datenverarbeitung im Auftrag gemäß § 7 SächsDSG sind in der genannten Bekanntmachung erläutert.

5.7.4 Grundsatzfrage: Von öffentlichen Stellen durchgeführte Meinungsumfragen als amtliche Statistik

Ein Stadtratsbeschluß hatte den Oberbürgermeister beauftragt, sich mittels Fragebögen, die in Behörden mit größerem Publikumsverkehr ausgelegt werden sollten, einen Überblick darüber zu verschaffen, inwieweit die Einwohner mit dem Verhalten der städtischen Bediensteten ihnen gegenüber zufrieden sind.

Gefragt werden sollte also nach *Bewertungen*, vielleicht auch *Wünschen* der Befragten.

Ist die ersichtlich zu allgemeinen Planungszwecken - nicht zur individuellen Leistungskontrolle - vorgenommene massenweise Erhebung, Zusammenführung und Auswertung solcher Informationen über 'innere Tatsachen' rechtlich als *Statistik* anzusehen? Oder aber fällt unter den Begriff der Statistik im Rechtssinne nur die Erhebung von Daten über äußere ('objektive') Tatsachen, also z. B. über solche 'harten' Fakten wie bei der Frage nach der Anzahl der Zimmer oder der Art der Heizung, über die eine Wohnung verfügt (im Rahmen der GWZ 1995)?

In der Vergangenheit hatte ich mich in einem einzelnen Fall bereits implizit im Sinne der *ersten Auffassung* geäußert, also einen die Erhebung von Bewertungen, Wünschen oder auch Zukunftserwartungen - kurz: Meinungsumfragen - einbeziehenden rechtlichen Statistikbegriff vertreten. Von dieser Rechtsmeinung war auch die Stadt Dresden ausgegangen, als sie mir den unter 5.7.6 erörterten Satzungsentwurf im Hinblick auf § 8 Abs. 3 SächsStatG zur Stellungnahme vorgelegt hatte (in diesem Falle brauchte die Rechtsfrage jedoch nicht entschieden zu werden!). Jedoch hatten sich in der Zwischenzeit das Statistische Landesamt und das SMI gegenüber der betreffenden Stadt und mir auf die gegenteilige Rechtsmeinung festgelegt: Mit einer Begründung, die nicht über-

zeugen konnte - aber es war doch Anlaß genug, die Rechtsfrage noch einmal gründlicher zu untersuchen.

Auf eine gesicherte Rechtspraxis oder auch nur ein einheitliches Meinungsbild in den Tätigkeitsberichten der Datenschutzbeauftragten des Bundes und der Länder kann man nicht zurückgreifen. Aber es gibt eine offenbar bisher allenthalben übersehene Äußerung des Bundesverfassungsgerichts im Sinne der von mir schon bisher vertretenen, also Meinungsumfragen in die Statistik im Rechtssinne einbeziehenden Auffassung: In seiner Entscheidung vom 31. Juli 1958 zu den bremischen und hamburgischen Gesetzen über die Volksbefragung über Atomwaffen (E 8, 104 ff., 111) hat das Gericht, ohne die Frage näher zu problematisieren, "Statistik" im Rechtssinne dahingehend bestimmt, daß sich eine statistische Erhebung auch auf die Ermittlung sogenannter "innerer Tatsachen" und auf die Feststellung politischer Wertungen und Meinungen beziehen kann (ohne daß es sich um eine auf die Auslegung von Art. 73 Nr. 11 GG beschränkte Interpretation handelte).

Unter dem Gesichtspunkt des Schutzes des Grundrechts auf informationelle Selbstbestimmung ist dies auch heute noch die richtige Grenzziehung: Die Erhebung 'innerer Tatsachen' verdient denselben bereichsspezifischen Datenschutz wie diejenige äußerer Tatsachen; im Falle der Erhebung von Daten über Massenerscheinungen zu Planungszwecken ist dies der Schutz des Statistikrechtes, sofern man nicht ein zusätzliches gesetzliches Regelwerk für die Durchführung amtlicher Meinungsumfragen schaffen will, welches sich einerseits von der amtlichen Statistik und andererseits vom Recht der Volksabstimmungen unterschiede, also als drittes hinzukäme, was wohl kaum sinnvoll wäre.

Die Durchführung solcher Meinungsumfragen unterliegt demnach im vollen Umfang den Regeln des Sächsischen Statistikgesetzes, insbesondere ggf. denjenigen über die Durchführung von Kommunalstatistiken. In diesem Fall bedarf es einer vom Stadtrat zu verabschiedenden Satzung mit dem nach § 8 Abs. 1 Satz 2, 2. Halbs. i. V. m. § 6 Abs. 6 Satz 1 und 2 SächsStatG erforderlichen Inhalt, der zudem die Anforderungen des § 6 Abs. 3 SächsStatG erfüllt.

Ohne eine vom Stadtrat zu verabschiedende Satzung und ohne eine Beschränkung der Zuständigkeit für die Durchführung der Fragebogenaktion ausschließlich auf Bedienstete der kommunalen Statistikstelle wäre also die geplante Umfrage rechtswidrig gewesen.

5.7.5 Gebäude- und Wohnungszählung 1995: Zwischenbilanz

Im Berichtszeitraum hat auf der Grundlage von § 1 Nr. 1 WoStatG - wie insgesamt im Beitrittsgebiet - in Sachsen die erste statistische Großerhebung seit der Wiedervereinigung stattgefunden: Die Gebäude- und Wohnungszählung (GWZ) 1995, eine Vollerhebung mit Auskunftspflicht, mittels deren zuverlässige Datengrundlagen für Entscheidungen der Wohnungswirtschaft und der Wohnungspolitik gewonnen

werden sollen.

Die GWZ ist in Sachsen aus datenschutzrechtlicher Sicht im großen und ganzen bisher erfreulich problemlos verlaufen; gewichtige Verstöße gegen den Datenschutz sind bisher nicht bekannt geworden.

Ein Kontrollbesuch bei der Erhebungsstelle einer kreisangehörigen Stadt vermittelte einen entsprechenden Eindruck. Die Bediensteten waren den Erfordernissen des Datenschutzes gegenüber aufgeschlossen, nennenswerte datenschutzrechtliche Versäumnisse waren nicht festzustellen. Auch die gesetzlich vorgeschriebene (§ 6 Abs. 1 Satz 1 und 2 WoStatG) Abschottung der örtlichen Erhebungsstelle war gewährleistet: Die in der Erhebungsstelle tätigen Bediensteten der Stadt waren für die Dauer der gesamten Erhebung von ihren ursprünglichen Aufgaben entbunden, also ausschließlich mit der Durchführung der GWZ 1995 beschäftigt. Die Erhebungsstelle war in einem von der übrigen Stadtverwaltung entfernt gelegenen Gebäude untergebracht. Die Erhebungsbeauftragten (§ 7 WoStatG) waren sorgfältig ausgewählt worden. Insbesondere war darauf geachtet worden, nach Möglichkeit niemanden in der Erhebungsstelle oder als Erhebungsbeauftragten zu verwenden, der vor oder nach seinem Einsatz in der GWZ 1995 mit dem Vollzug des Abgaben- oder des Bauordnungsrecht oder im Melde- oder Wohnungswesen beschäftigt gewesen war oder sein würde.

Nachdem erste vorläufige Gesamtergebnisse der Presse bekanntgegeben worden sind, werde ich zukünftig darauf zu achten haben, daß die gemäß § 11 WoStatG für ausschließlich statistische Zwecke vorgesehene Übermittlung von Einzelangaben aus der GWZ an die Gemeinden und Gemeindeverbände in datenschutzrechtlich einwandfreier Weise stattfindet.

Im übrigen habe ich das Statistische Landesamt davon zu überzeugen vermocht, daß einer kommerziellen Verwertung der bei der GWZ 1995 erhobenen Daten, die sich auf einem niedrigen, insbesondere kleinräumigen Aggregationsniveau bewegt, enge Grenzen gezogen sind: Der in anderen Staaten, z. B. Österreich oder Ungarn, anscheinend zulässige Vertrieb von auf CD-ROM gespeicherten Daten mit sämtlichen Erhebungsmerkmalen aus einer Wohnungs- und Gebäudezählung oder einer Volkszählung, die es ermöglichen, durch Verknüpfen mehrerer Erhebungsmerkmale, insbesondere unter Verwendung des Erhebungsmerkmals "Gemeinde, Gemeindeteil", gezielt auf Einzeldatensätze zuzugreifen und damit gewissernmaßen in allen interessierenden Erhebungsbögen blättern zu können, wäre in Deutschland als Verstoß gegen das Statistikgeheimnis rechtswidrig (und sogar strafbar).

5.7.6 Befragung von Jugendlichen zu einem Straßenbauvorhaben

An die 16- und 17jährigen *Einwohner* Dresdens sollte die Frage gestellt werden "Sind Sie für den Bau der Autobahn Dresden-Prag entsprechend der abgebildeten Linienführung?" Die Stadtverwaltung leitete mir gemäß § 8 Abs. 3 SächsStatG den

Entwurf einer Satzung zur Stellungnahme zu, die diese Befragung regeln sollte.

Die Befragung konnte rechtlich eine *Abstimmung* im Sinne von Art. 20 Abs. 2 Satz 2 GG, Art. 3 Abs. 2 Satz 2 SächsVerf sein. Das lag deswegen besonders nahe, weil die geplante Befragung der Jugendlichen als Ergänzung des Bürgerentscheides - gemäß § 24 SächsGemO - ausgestaltet worden war, der zum selben Thema geplant war und dann später auch tatsächlich stattgefunden hat. Nach dieser Vorschrift der Gemeindeverordnung können nur *Bürger* in Gemeindeangelegenheiten über eine zur Abstimmung gestellte Frage entscheiden. Bürger sind die über 18 Jahre alten Deutschen (das kann sich in Zukunft ändern), die länger als drei Monate ihren Hauptwohnsitz in der Gemeinde haben (§ 15 Abs. 1 SächsGemO).
Die geplante Befragung wäre also eine Abstimmung neben dem Bürgerentscheid gewesen, nämlich eine Abstimmung eines Personenkreises, der sicher nicht das Alterserfordernis und in manchen Fällen auch nicht die genannten sonstigen Voraussetzungen des § 15 Abs. 1 SächsGemO erfüllt.
Abstimmungen auf Gemeindeebene, in denen entschieden wird (vgl. § 24 Abs. 4 SächsGemO), auch *dezisive* Volksbefragungen genannt, sind in §§ 24 f. SächsGemO abschließend geregelt. Für eine den Bürgerentscheid ergänzende ähnliche Befragung war daher kein Raum. Eine faktische Erweiterung des Kreises der Abstimmungsberechtigten durch eine ergänzende Abstimmung hätte als Umgehungsversuch gegen § 24 SächsGemO verstoßen. Dasselbe gilt aber auch für den Fall, daß die Befragung lediglich die Wirkung einer (partiellen) sogenannten *konsultativen* Volksbefragung haben sollte. Solche konsultativen Volksbefragungen verletzen das Prinzip der Volkssouveränität und sind daher aus verfassungsrechtlichen Gründen unzulässig (ausführlich dazu Krause, Verfassungsrechtliche Möglichkeiten unmittelbarer Demokratie, in: Handbuch des Staatsrechts der Bundesrepublik Deutschland, hrsg. von J. Isensee und P. Kirchhof, Bd. II, § 39 Rdnr. 17 f.).

Man konnte die geplante Umfrage aber rechtlich auch als *Statistik* betrachten. Davon war die Stadt Dresden ausgegangen.

Gemäß § 1 Abs. 1 Satz 1 SächsStatG, der nach § 2 Abs. 1 Nr. 4 SächsStatG auch für Kommunalstatistiken gilt, hat die amtliche Statistik die Aufgabe, entsprechend dem amtlichen *Informationsbedarf* Daten über Massenerscheinungen zu erheben, zu sammeln usw., vgl. § 1 Abs. 1 Satz 1 SächsStatG. Der Information bedarf ein Träger öffentlicher Verwaltung - in diesem Falle also die Landeshauptstadt Dresden - jedoch nur, soweit die Ergebnisse der durchzuführenden Statistik überhaupt geeignet sein können, eine Entscheidung des betreffenden Trägers öffentlicher Verwaltung zu beeinflussen. Daran fehlte es jedoch mit aller Eindeutigkeit: Würde ein Bürgerentscheid nach § 24 SächsGemO stattfinden, so würde durch die Abstimmungsberechtigten vorläufig maßgeblich (§ 24 Abs. 4 Satz 2 SächsGemO) über die zur Abstimmung gestellte Frage (nämliche welche Haltung die Landeshauptstadt Dresden gegenüber dem Autobahnplanungsvorhaben einnehmen würde) entschieden. Das Ergebnis der Erhebung des Willens der 16 und 17 Jahre alten Einwohner würde daneben keinerlei Rechtswirkungen entfalten können; und zwar aus den oben bereits

genannten Gründen.

Die geplante Satzung wäre also statistikrechtlich von der Satzungsermächtigung des § 8 Abs. 1 Satz 2, 1. Halbs. SächsStatG nicht gedeckt gewesen, weil es am nötigen Informationsbedarf gefehlt hätte.

Ich habe der Stadt Dresden mitgeteilt, daß die geplante Befragung als Abstimmung gegen die Sächsische Gemeindeordnung bzw. das Prinzip der Volkssouveränität, als Statistik gegen das Grundrecht auf informationelle Selbstbestimmung verstoßen würde.

5.7.7 Verkehrszählung mit und ohne Videoaufzeichnungen

Die Güterverkehrsströme auf dem Gebiet einer sächsischen Großstadt will deren Stadtplanungsamt untersuchen. Nach den Vorstellungen der Behörde sollte zur Datensammlung ein privates Verkehrsforschungsunternehmen im Auftrag der Stadt an einer Vielzahl von Erfassungsstellen neben dem genauen Zeitpunkt des Vorbeifahrens des Fahrzeuges das vollständige amtliche Kennzeichen sowie bestimmte Angaben zur Bauweise (z. B. "Hängerzug") und zur Nutzungsart (z. B. "Gefahrguttransport") aufzeichnen. An etlichen Erfassungsstellen mit besonders regem Verkehrsgeschehen sollten zunächst die Güterfahrzeuge mittels Videoaufzeichnungen erfaßt werden, aus denen dann die interessierenden Daten erhoben werden sollten. Durch Hinweisschilder wollte man rechtzeitig auf die Videoaufzeichnung aufmerksam machen, um den Lkw-Fahrern Gelegenheit zum Ausweichen zu geben.
Die Untersuchung sollte den Weg einzelner Fahrzeuge im Netz der Erfassungsstellen nachverfolgen und diese Einzelbewegungen zu Verkehrsströmen aggregieren. Eine Satzung als Rechtsgrundlage für die Durchführung dieser Datenerhebung war nicht vorhanden.

Ich habe zu dem Vorhaben in folgendem Sinne Stellung genommen (und ich wurde darin vom Statistikreferat des SMI erfreulich unterstützt):

Mit Videoaufzeichnungen greift man in das Grundrecht auf informationelle Selbstbestimmung ein. Zwangsläufig würden auch die Bilder der Lkw-Fahrer und -Beifahrer und darüber hinaus auch sonstige Verkehrsteilnehmer aufgezeichnet. Abgesehen von der Erfassung der Anwesenheit an einem bestimmten Ort zu einer bestimmten Zeit wären auch ggf. strafbare oder bußgeldbewehrte Verstöße gegen straßenverkehrsrechtliche oder umweltrechtliche Vorschriften (wie Überladung, verbotene Gefahrguttransporte, Nichteinhalten der Ruhe- und Lenkzeiten, Geschwindigkeitsübertretungen, Sicherheitsmängel am Fahrzeug usw.) erkennbar festgehalten.

In jedem Falle, auch ohne die Anfertigung von Videoaufzeichnungen, würde die geplante Verkehrszählung eine Statistik im Rechtssinne sein, nämlich die Sammlung usw. von Daten über Massenerscheinungen zu Planungszwecken (vgl. § 1 Abs. 1 Satz 1

SächsStatG). Als Kommunalstatistik bedürfte die Erhebung gemäß § 8 Abs. 1 Satz 2, 1. Halbs. SächsStatG einer Satzung als Rechtsgrundlage. Der Versuch der Stadt, die Datenerhebung auf § 11 Abs. 1 SächsStatG zu stützen, wonach zur Erfüllung eines kurzfristig auftretenden Datenbedarfes Landesstatistiken auf freiwilliger Grundlage auch ohne besondere Rechtsgrundlage durchgeführt werden dürfen, konnte nicht überzeugen: Abgesehen von dem Erfordernis einer besonderen Dringlichkeit des Datenbedarfes konnte trotz des vorhandenen Interesses des SMWA an den Ergebnissen der Verkehrszählung (für die Landesplanung) kein Zweifel daran bestehen, daß es sich um eine städtische und nicht um eine Landesstatitik handeln würde. Außerdem würde von einer freiwilligen Teilnahme der Lkw-Fahrer an der Verkehrszählung nicht die Rede sein können. Die Videoaufzeichnung würde ohne den Willen der Betroffenen stattfinden; denn der Verkehrsfluß und der Zeitdruck, unter dem die Lkw-Fahrer stehen, würden ein Ausweichen vor der Videokamera kaum zulassen.

Am Satzungserfordernis würde sich auch dann nichts ändern, wenn als Hilfsmerkmal lediglich die letzten drei Ziffern des amtlichen Kennzeichens erhoben würden, wenn dadurch auch die Erhebung frühzeitig weitgehend anonymisiert würde, dem Gebot des § 1 Abs. 2 SächsStatG entsprechend.

Das Stadtplanungsamt hat inzwischen den Entwurf der erforderlichen Statistiksatzung gemäß § 8 Abs. 3 SächsStatG vorgelegt. Meine erheblichen Einwände gegen die Erforderlichkeit der Datenerfassung mittels Videoaufzeichnungen haben ein Umdenken veranlaßt: Auf dieses Mittel wird vollständig verzichtet, und die wohl auch dadurch geförderte Vereinfachung der Datenerfassung durch Beschränkung auf die letzten drei Ziffern des amtlichen Kennzeichens sowie das Ortskennzeichen, also eine frühzeitige weitgehende Anonymisierung, wird nach den Erfahrungen von Fachleuten den Untersuchungszweck, nämlich die Verfolgung des Weges einzelner Güterkraftfahrzeuge im Netz der Erfassungsstellen, nicht beeinträchtigen.

Weil es sich um Datenverarbeitung im Auftrag handelt (vgl. dazu oben unter 5.7.3), muß in dem Werkvertrag mit dem ausführenden Unternehmen eine Kontrolle der Datenverarbeitung durch den Sächsischen Datenschutzbeauftragten gewährleistet werden.

5.7.8 Kommunale Gewerbestatistik

Durch Zufall erfuhr ich von der Absicht einer kreisangehörigen Gemeinde, die neu hinzukommenden Gewerbetreibenden gelegentlich der Abgabe ihrer Gewerbeanzeigen (§ 14 GewO) in den Amtsräumen der Gemeinde zusätzlich mündlich über

- die Anzahl der über 55 Jahre alten Beschäftigten in dem anzumeldenden Gewerbebetrieb,
- die Anzahl der Behinderten unter den Beschäftigten,
- die Entfernung zwischen Arbeits- und Wohnort der Beschäftigten

und einiges mehrzu befragen. Eine Pflicht zur Auskunft sollte es genausowenig geben wie eine Nacherhebung bereits früher angezeigter Gewerbe. Die betreffende Gemeindeverwaltung wollte sich so einen Überblick über die ortsansässigen Gewerbebetriebe verschaffen, angeblich insbesondere deshalb, um künftige Entwicklungstendenzen besser erkennen zu können.

Die beabsichtigte Befragung der Gewerbetreibenden hätte alle Merkmale einer Kommunalstatistik (§ 2 Abs. 1 Nr. 4 SächsStatG) erfüllt: Es wären Einzelangaben über die Gewerbetreibenden und deren Beschäftigte zu Planungszwecken erhoben, gesammelt, aufbereitet, dargestellt und analysiert worden (§ 1 Abs. 1 Satz 1 SächsStatG). Die Freiwilligkeit der Teilnahme an der Befragung hätte daran nichts geändert (§ 8 Abs. 1 Satz 2, 2. Halbs. i. V. m. § 6 Abs. 3 Satz 1 und Abs. 6 Satz 2 SächsStatG).

Eine grundsätzlich erforderliche Satzung (§ 8 Abs. 1 Satz 2, 1. Halbs. SächsStatG) war nicht vorhanden. Ob hier ausnahmsweise gemäß § 8 Abs. 1 Satz 2, 2. Halbs. i. V. m. § 6 Abs. 2 SächsStatG als Rechtsgrundlage statt einer Satzung eine Verordnung ausreichen würde, war sehr zweifelhaft, weil die Daten zumindest zum Teil nicht nur betriebsbezogen sein würden, sondern auch beschäftigtenbezogen. Zudem hatte man bisher nicht an § 8 Abs. 2 SächsStatG gedacht: Kommunalstatistiken sind nur zulässig, wenn der Gemeinde die für ihren Zuständigkeitsbereich benötigten statistischen Einzelangaben oder Ergebnisse vom Statistischen Landesamt nicht zur Verfügung gestellt werden können.

Das ist nach § 8 Abs. 2 immer zu prüfen, zweckmäßig über § 8 Abs. 3 hinaus auch im Ausnahmefall des § 6 Abs. 2 SächsStatG durch vorhergehende Anfrage beim Statistischen Landesamt. Man sollte eigentlich meinen, daß Gemeinden schon aus Kostengründen auf diesen Gedanken kämen!

Die betreffende Gemeinde hat aufgrund dieser Hinweise von der beabsichtigten Befragung Abstand genommen.

Siehe auch oben 5.1.23.

5.8 Archivwesen

5.8.1 DDR-Unterlagen über kirchliche Funktionsträger

Jemand, der das Verhältnis von Staat und Kirche unter der Herrschaft der SED am Beispiel einer sächsischen Stadt erforscht, will im Stadtarchiv die Berichte auswerten, die der ehemalige Referent für Kirchenfragen (RfK) beim Rat der Stadt über seine Gespräche mit Pfarrern und anderen kirchlichen Funktionsträgern geführt hat. Inwieweit ist in solchen Fällen Einsicht in die Unterlagen zu gewähren?

Ein schutzfristfreier Zugang der Forschung zu solchen Daten (vgl. § 10 Abs. 1 Satz 3, Abs. 2 Satz 2 SächsArchG) bestünde nur, falls der genannte Personenkreis unter die "Amtsträger" im Sinne von § 10 Abs. 2 Satz 3 SächsArchG zu subsumieren wäre. Waren Pfarrer, soweit sie in dienstlicher Tätigkeit gehandelt haben, "Amtsträger in Ausübung ihrer Ämter" in diesem Sinne?
Eine so weite Auslegung dieses Begriffes habe ich nicht empfehlen können. Immerhin nimmt § 1 Abs. 2 SächsArchG die öffentlich-rechtlichen Religionsgemeinschaften von der Geltung des Gesetzes aus. Auch sieht der BStU, wie ich in Erfahrung gebracht habe, neuerdings in den Pfarrern nicht mehr Amtsträger im Sinne von § 32 Abs. 1 Nr. 3, 1. Spiegelstrich StUG.
Zu Forschungszwecken kann es Zugang zu diesen Daten nur gemäß § 10 Abs. 4 Satz 2 SächsArchG geben (oder auch auf der Grundlage einer Einwilligung gemäß Satz 3 der genannten Vorschrift). Danach kann unter bestimmten Voraussetzungen eine Schutzfristverkürzung stattfinden, und sie *muß* sogar stattfinden, weil ja auch der Forschende ein Grundrecht geltend macht, an welches das Archiv als Teil der öffentlichen Gewalt ihm gegenüber gebunden ist. Maßgeblich ist eine umfassende Abwägung zwischen den schutzwürdigen Belangen der betroffenen Personen und dem öffentlichen Interesse an der Durchführung des Forschungsvorhabens.

Bei Anwendung dieses Maßstabes auf Pfarrer und andere kirchliche Funktionsträger, etwa Kirchengemeinderäte oder Synodale, ist zu berücksichtigen, daß nach dem Selbstverständnis der Kirche der Pfarrer zwar kein staatliches oder unter staatlicher Aufsicht stehendes Amt, jedoch ein Amt eigener, nämlich gemeindebezogener und damit zumindest kirchenintern öffentlicher Art wahrnimmt. Nach kirchlichem Selbstverständnis ist sogar des Privatleben des Pfarrers - viel stärker, als das beim Beamten im staatsrechtlichen Sinne der Fall ist - in einem vergleichsweise sehr engen Zusammenhang mit seiner eigentlichen dienstlichen Tätigkeit zu sehen.
Dies war auch in DDR-Zeiten nicht nur die kircheneigene Sicht. Auch in den Augen des staatlichen Gegenübers, und wohl auch aus der Sicht der Bevölkerung, war die Kirche nicht ein privater Verein, sondern eine - die einzige - nicht von Staates Gnaden existierende oder gar geschaffene, sich mit einer an jedermann gerichteten Botschaft identifizierende Institution, also eben mehr als ein bloßer 'Verein'.
Sowohl das kirchliche Selbstverständnis wie die Einstellung der außerkirchlichen Umgebung, auch zu DDR-Zeiten, entziehen also die dienstliche Tätigkeit kirchlicher Funktionsträger in vergleichsweise weitem Maße dem grundrechtlichen Schutz der Privatsphäre.
Für die einzelnen Typen personenbezogener Informationen, die sich in den Unterlagen über die vom Referenten für Kirchenfragen geführten sogenannten Pfarrergespräche finden, lassen sich meiner Meinung nach folgende Faustregeln aufstellen:
(1) Sogenannte Gruppengespräche, welche der RfK mit einer ganzen Gruppe von Pfarrern geführt hat, dürften in aller Regel - unter der Voraussetzung der Erforderlichkeit für das Forschungsvorhaben - offenzulegen sein, was die Tatsache betrifft, daß ein Pfarrer eine bestimmte Äußerung getan hat.

Sofern die Äußerung sich auf eine dritte Person bezieht, ist deren Schutzwürdigkeit zu

berücksichtigen: Ist sie z. B. kein kirchlicher Funktionsträger, sondern schlichtes Gemeindeglied oder sonstiger Privater, ist die Information insoweit völlig zu anonymisieren. Dabei ist zu beachten, daß diejenigen, die die örtlichen Vorgänge erforschen wollen, in der Regel über ortsbezogenes besonderes Zusatzwissen verfügen. Die Angabe z. B., daß das betreffende Gemeindeglied Inhaber oder Leiter einer Apotheke im Ortsteil A sei, darf dem Forscher also nicht zur Verfügung gestellt werden, das heißt konkret, sie muß in der Kopie, auf die sich die Einsichtnahme des Archivgutes beschränkt, geschwärzt sein. Die Schwärzung des Namens und der Anschrift reicht nicht aus. Wenn der Betroffene einwilligt, kann sein Name offenbart werden (§ 10 Abs. 4 Satz 3 SächsArchG). Das ist die eleganteste Lösung.

(2) Auftreten des RfK auf Geburtstagsfeiern von Pfarrern:
Erschien der RfK am Geburtstag im Pfarrhaus, so war für alle Beteiligten klar, daß die private oder doch jedenfalls gemeindeinterne Geburtstagsrunde nunmehr unterbrochen war, weil das Geburtstagskind, auf Grund seiner kirchlichen Dienststellung, Besuch von einem Vertreter der Staatsgewalt hatte.

Es handelte sich für die Zeit der Anwesenheit des RfK um eine Art erzwungenen Geburtstagsempfang.

Für Äußerungen, die der Pfarrer bei dieser Gelegenheit - laut dessen Protokoll - gegenüber dem RfK getan hat, gelten m. E. dieselben Regeln wie für die Gruppengespräche.

(3) Pauschalbewertungen eines Pastors durch staatliche Stellen:
Enthalten die Unterlagen etwa die Bewertung eines bestimmten Pfarrers als "positiv-fortschrittlich", so betrifft dies einen zentralen Gesichtspunkt pfarramtlicher Tätigkeit in der DDR: Wer in der DDR Pfarrer war, insbesondere dieses Amt neu übernahm, wußte, daß das SED-Regime jedem einzelnen Pfarrer eine Stellungnahme zum System abzufordern versuchte und sein dienstliches Verhalten zwangsläufig unter diesem Gesichtspunkt interpretieren und bewerten würde.
Unter der Voraussetzung der Erforderlichkeit für das Forschungsvorhaben ist daher die Bewertung bestimmter namentlich benannter Pfarrer hinsichtlich ihrer Einstellung zum SED-Staat bzw. zum sogenannten 'Wissenschaftlichen Sozialismus' (als dessen weltanschaulicher Grundlage) offenzulegen, also der Name und andere Identitätshinweise nicht zu schwärzen.

(4) Das (regelmäßige) Pfarrergespräch:
Auch dieses - unter vier Augen stattfindende - Gespräch mußte der Pfarrer in seiner dienstlichen Eigenschaft führen (über sich ergehen lassen). Die Tatsache, daß der Pfarrer in diesem Rahmen bestimmte Äußerungen getan hat, ist daher unter der Voraussetzung der Erforderlichkeit für das Forschungsvorhaben - unter Nennung des Namens des Pfarrers - offenzulegen.

Hat der Pfarrer sich etwa allgemein zu Fragen der Rüstung oder der sonstigen Politik,

zur Bewertung derjenigen, die Ausreiseanträge stellten, o. ä. geäußert, ist dies, sofern für das Forschungsvorhaben wichtig, offenzulegen.

Hinsichtlich Äußerungen des Pfarrers über Dritte gilt das zu (3) Ausgeführte.

So weit die Überlegungen zur Gewichtung der schutzwürdigen Belange innerhalb des § 10 Abs. 4 Satz 2 SächsArchG. Außerdem muß dann noch das Forschungsvorhaben gewürdigt werden, um das öffentliche Interesse an seiner Durchführung richtig bewerten und mit den genannten persönlichkeitsrechtlichen Belangen abwägen zu können.

Man sieht: Die Anwendung der Abwägungsklausel des § 10 Abs. 4 Satz 2 SächsArchG ist eine sehr anspruchsvolle Aufgabe, die an die Archivare hohe datenschutzrechtliche Anforderungen stellt und außerdem Arbeit mit sich bringt. Denn die in den Unterlagen enthaltenen vielen personenbezogenen Einzelinformationen sind jede für sich zu beurteilen! Anders ausgedrückt: Bei manchen Schriftstücken muß sich der Archivar nahezu für jedes einzelne Wort - nicht nur Namen! - überlegen, ob er es zu schwärzen hat oder gerade nicht schwärzen darf!

5.8.2 Archivbenutzung zum Zwecke der Erbenermittlung

Ein Kreisarchiv fragte an, unter welchen Voraussetzungen es einem Erbenermittlungs-Unternehmen Auskünfte aus archivierten Meldedaten geben dürfe. Beantragt worden war, die letzte Anschrift, ggf. auch die Wegzugsanschrift, von 1887 geborenen Eheleuten sowie ggf. Namen und Anschrift der vermutlich noch lebenden, aber vielleicht weggezogenen Kinder dieses Ehepaares mitzuteilen. Ich habe das Archiv auf folgendes hingewiesen:

Gemäß § 5 Abs. 7, 2. Halbs. SächsArchG (hier in Verbindung mit § 13 Abs. 3 Satz 1 SächsArchG) haben die Archive bei der Nutzbarmachung des Archivgutes die Vorschriften über die Verarbeitung und Sicherung zu beachten, die für die abgebende Stelle, in diesem Falle also die Meldebehörde, gelten (vgl. auch § 27 SächsMG).

Die von dem Erbenermittlungs-Unternehmen beantragte Auskunft aus den archivierten Meldeunterlagen, also die Benutzung des Archivgutes (§ 9 SächsArchG), war damit nur unter den Voraussetzungen zulässig, die für eine von der Meldebehörde selbst zu erteilende Auskunft gelten. Gemäß § 26 Abs. 4 SächsMG darf die Meldebehörde folgende Daten eines Verstorbenen oder Weggezogenen übermitteln:

- Familiennamen,
- Vornamen, unter Kennzeichnung des gebräuchlichen Vornamens (Rufname),
- frühere Namen,
- Doktorgrad,
- [gegenwärtige,] frühere und künftige Anschriften, Haupt- und Nebenwohnung, ggf. Wohnungsnummern,

- Sterbetag und -ort.

Folgende weitere Daten Verstorbener dürfen übermittelt werden, wenn dies zu wissenschaftlichen Zwecken oder zur Behebung einer bestehenden Beweisnot erforderlich ist:
- Ordensnamen/Künstlernamen,
- Tag und Ort der Geburt,
- Geschlecht,
- gesetzliche Vertreter, Eltern von Kindern bis zur Vollendung des 18. Lebensjahres (Vor- und Familiennamen, Doktorgrad, Anschrift, Tag der Geburt, Sterbetag),
- Staatsangehörigkeiten,
- Tag des Ein- und Auszugs,
- Familienstand, bei Verheirateten zusätzlich Tag und Ort der Eheschließung,
- Übermittlungssperren.

Das Kreisarchiv durfte also die früheren Anschriften der betreffenden Personen sowie ggf. deren Wegzugsanschrift und Sterbetag und -ort an das Erbenermittlungs-Unternehmen übermitteln. Außerdem durfte es unter der Voraussetzung, daß dies zur Behebung einer bestehenden Beweisnot erforderlich ist, auch die Namen und Anschriften der Kinder der betreffenden Personen übermitteln. Sofern nicht Anhaltspunkte für das Gegenteil vorliegen, kann man davon ausgehen, daß die Beweisnot der Auftraggeber durch die Beauftragung eines Erbenermittlungs-Unternehmens hinreichend nachgewiesen ist.

Ich habe zuweilen den Eindruck, daß sich die kommunalen Archive im Freistaat Sachsen mit der Benutzung der Archivalien durch Private noch schwertun. Deshalb sei auch an dieser Stelle darauf hingewiesen: Archive sind zum - befugten - Benutzen und für die - befugten - Benutzer da. Gewissermaßen 'vorsichtshalber' eine befugte Benutzung doch lieber nicht zuzulassen ist rechtswidrig; auf die befugte Benutzung besteht ein *Anspruch* (§ 9 Abs. 1 SächsArchG, hier i. V. m. § 13 Abs. 3 Satz 1 SächsArchG).

5.8.3 Einstellung freier Mitarbeiter im Stadtarchiv

Ein Stadtarchiv wandte sich mit der Frage an mich, welche Anforderungen an die Eignung von vorübergehend im Stadtarchiv zu beschäftigenden freien Mitarbeitern zu stellen und welche personellen Maßnahmen zur Gewährleistung des Datenschutzes gemäß § 9 Abs. 1 SächsDSG zu treffen sind. (Im Vorfeld eines Stadtjubiläums sollten für die Sichtung der Unterlagen aus der jüngeren Vergangenheit die personellen Kapazitäten zeitweise aufgestockt werden.)

Ich habe dem Stadtarchiv folgendes mitgeteilt:

Bei der Einstellung freier Mitarbeiter im Stadtarchiv, die Unterlagen aus der Zeit der

DDR sichten sollen, stellt die Verwendung des sog. "MfS-Fragebogens" und die Erhebung von Angaben zur beruflichen Tätigkeit - wie bei den übrigen städtischen Bediensteten - eine ausreichende personelle Maßnahme zur Gewährleistung des Datenschutzes gemäß § 9 Abs. 1 SächsDSG dar. Bei der Einstellung müssen die freien Mitarbeiter gemäß § 6 SächsDSG belehrt und gemäß dem Verpflichtungsgesetz auf die gewissenhafte Erfüllung ihrer Obliegenheiten verpflichtet werden. In technisch-organisatorischer Hinsicht sind ferner Maßnahmen zur Überwachung der Arbeit (Fälschung/Vernichtung/Unordnung) und einer Ein- und Ausgangskontrolle (Diebstahl) der freien Mitarbeiter zu treffen.

Siehe auch Abschnitt 9.4.2

5.9 Polizei

5.9.1 Kontrollbesuche bei der Polizei

Den datenschutzrechtlichen Standard sächsischer Polizeidienststellen habe ich im Berichtszeitraum bei einem Polizeipräsidium, zwei Polizeidirektionen, einem Polizeirevier sowie beim Landeskriminalamt kontrolliert.

Dabei wurde deutlich, welche Bedeutung der Nachvollziehbarkeit der Aktenführung zukommt: Nur wenn dokumentiert wird, welche Gründe zu einer Datenerhebung und -speicherung führten und warum bestimmte Ermittlungsschritte eingeleitet wurden, ist gewährleistet, daß polizeiliches Handeln dienstintern und extern (durch den Sächsischen Datenschutzbeauftragten) in rechtsstaatlich gebotener Weise kontrolliert werden kann. Wie meine Kontrollen zeigten, wird dieser Grundsatz nicht immer in der gebotenen Konsequenz eingehalten.

Schwerpunkte der Kontrollen waren:
- Bereinigung von Kriminalakten,
- Führung und Aufbewahrung von Kriminalakten,
- Umgang mit Personaldaten,
- Führung verschiedener polizeilicher Arbeitsdateien (z. B. "Fußballkartei", "Bandenmäßig organisierte Kriminalität"),
- Polizeiliche Beobachtung,
- Geldwäsche,
- Telefonabhörmaßnahmen,
- Bereinigung von Fingerabdruckblättern,
- Aufbewahrung von Altakten.

Erfreulich ist, daß sich sämtliche kontrollierten Dienststellen bemüht haben, meine Empfehlungen umzusetzen und weiterzuleiten. So veranlaßte das SMI als Folge meiner Mängelfeststellung bei einer Polizeidirektion eine erneute landesweite Bereinigung der

Kriminalakten. Als Arbeitshilfe wurden den Polizeidienststellen - wie von mir bereits im Jahr 1993 empfohlen - Richtlinien ausgehändigt, aus denen sich ergibt, welche Aktenbestände, die zu DDR-Zeiten angelegt wurden, aus rechtsstaatlichen Gründen auszusondern sind. Auf meine Veranlassung hin wurde auch sichergestellt, daß zahlreiche alte DDR-Vordrucke, mit denen noch unzulässigerweise Daten erhoben wurden, zukünftig nicht mehr verwendet werden.

5.9.2 Rücknahme sächsischer Daten aus Beständen des Bundeskriminalamts (BKA)

Beim BKA wird als bundesweite Verbunddatei ein Kriminalaktennachweis (KAN) über schwere und überregional bedeutsame Straftaten geführt. Zusätzlich gibt es in den einzelnen Bundesländern automatisierte Aktennachweissysteme, in denen Kriminalakten zu Straftaten von regionaler Bedeutung nachgewiesen werden. Weil im Freistaat Sachsen zunächst kein Kriminalaktennachweis dieser Art vorhanden war, erklärte sich das Bundeskriminalamt im Jahre 1991 damit einverstanden, für eine Übergangszeit von fünf Jahren sächsische "U-Gruppen" (d. h. Nachweisdaten zu angefertigten personenbezogenen Akten) in den Bundes-KAN einzustellen, auch wenn die Voraussetzungen für eine dortige Speicherung (schwere, überregional bedeutsame Straftaten) nicht vorlagen. Nach Auskunft des LKA erfolgte dabei eine Speicherung von 68.000 sächsischen U-Gruppen. Dies führte in der Praxis dazu, daß von sächsischen Dienststellen eingegebene Kriminalaktennachweise bundesweit recherchierbar waren, obwohl dies nicht zur Aufgabenerfüllung aller deutschen Polizeidienststellen erforderlich und damit unzulässig war. Da zwischenzeitlich auch in Sachsen ein Kriminalaktennachweis in Form des PASS-Systems vorhanden ist, hat das LKA angekündigt, zu überprüfen, inwieweit eine Übernahme der im Bundes-KAN gespeicherten Daten in PASS oder eine fortgesetzte Speicherung im Bundes-KAN gerechtfertigt ist. Ich gehe davon aus, daß ab dem Jahre 1996 im Bundes-KAN nur noch Daten zu schweren, überregional bedeutsamen Straftaten gespeichert werden. Eine abschließende schriftliche Bestätigung dazu liegt aber noch nicht vor.

5.9.3 Aufbewahrung von Blutentnahmeprotokollen bei den Untersuchungsstellen

Die Polizei führt den Betroffenen zu einem Amtsarzt, der eine Blutprobe entnimmt und ein Protokoll über den Zustand des Betroffenen fertigt. Die Niederschrift enthält neben dem Namen die Anschrift und den Beruf sowie auch zahlreiche weitere Daten des Untersuchungsbefunds (Konstitution, Gang, Bewußtsein, Sprache, Verhalten, Stimmung, Denkablauf etc.). Dieses Protokoll wird zur Ermittlungsakte genommen. Eine Durchschrift wird zusammen mit der Blutprobe den drei wissenschaftlichen Untersuchungsstellen in Chemnitz, Leipzig und Dresden übersandt. Dort werden die Protokolle langfristig aufbewahrt. Bei diesen Stellen entstehen demgemäß umfangreiche Sammlungen personenbezogener Daten potentieller Alkoholsünder,

obwohl die Blutalkoholprotokolle zur Aufgabenerfüllung der Untersuchungsstellen grundsätzlich nicht erforderlich sind. Sofern die Untersuchungsstellen - wie in der Mehrzahl der Fälle - nur beauftragt sind, den Alkoholgehalt der Blutprobe festzustellen, benötigen sie die Angaben aus dem Blutentnahmeprotokoll nicht. Sichergestellt werden muß nur, daß die Blutproben einwandfrei der entsprechenden Person zugeordnet werden können. Dies ist auch ohne die detaillierten personenbezogenen Angaben aus dem Blutentnahmeprotokoll möglich. Daß es nicht zwingend erforderlich ist, die Protokolle an die Untersuchungsstellen zu übersenden, ergibt sich im übrigen auch aus der seit 1. Juni 1995 geltenden neuen "Bundeseinheitlichen Verwaltungsvorschrift über die Feststellung von Alkohol im Blut bei Straftaten und Ordnungswidrigkeiten und über die Sicherstellung und Beschlagnahme von Fahrausweisen". Danach ist das Protokoll, sofern eine Ausfertigung der Untersuchungsstelle übersandt wird, zu anonymisieren.

Ich habe das SMI deshalb gebeten, sicherzustellen, daß die Blutentnahmeprotokolle von der Polizei nicht mehr an die Untersuchungsstellen übersandt werden. Dieser Anregung ist das SMI bisher nicht gefolgt. Die Protokolle werden wie bisher an die Untersuchungsstellen gesandt. Ich betrachte die Angelegenheit noch nicht als erledigt.

5.9.4 Geplante Dienstanweisung für verdeckte Ermittler bei Gefahrenabwehr

Ein Einsatz verdeckter Ermittler als Mittel zur Abwehr einer konkreten Gefahr kommt praktisch nicht in Betracht, weil dazu in einer aktuellen Gefahrenabwehrsituation meist keine Zeit ist. Deshalb sollte in der geplanten Verwaltungsvorschrift der Einsatz verdeckter Ermittler ausdrücklich auf den Bereich der vorbeugenden Verbrechensbekämpfung gemäß § 39 Abs. 1 Nr. 2 SächsPolG beschränkt werden. Nach dieser gesetzlichen Regelung, die die tatbestandlichen Voraussetzungen für polizeiliches Tätigwerden zum Zwecke der vorbeugenden Verbrechensbekämpfung nennt, können besondere polizeiliche Erhebungsmethoden (also auch ein Einsatz verdeckter Ermittler) nur angewandt werden, wenn konkrete Tatsachen (oder die Gesamtwürdigung der Person) die Annahme rechtfertigen, daß eine Person bzw. ein individualisierbarer Täter(kreis) Straftaten von erheblicher Bedeutung begehen werde. Ein unbestimmtes, auf Dauer angelegtes Verweilen der Ermittlung in der kriminellen Szene wäre auf jeden Fall unzulässig. Vielmehr darf der verdeckte Ermittler bei der vorbeugenden Verbrechensbekämpfung nur mit konkretem Ermittlungsauftrag zeitlich begrenzt eingesetzt werden, wobei die Anordnung seines Einsatzes eine nachvollziehbare Beschreibung des Einsatzzieles enthalten muß, um eine flächendeckende Ausforschung ganzer "Szenen" zu vermeiden. Eine Stellungnahme des SMI zu meinen Überlegungen steht noch aus.

5.9.5 Speicherung des Merkmals "homosexuell" bei der Datenerfassung durch Polizeibehörden

In meinem 3. Tätigkeitsbericht (5.9.4) habe ich gefordert, die Möglichkeit einer Recherche nach Homosexuellen in PASS technisch auszuschließen, da sie zur Aufgabenerfüllung der Polizei nicht erforderlich ist. Auch wenn die Speicherung des Datums "homosexuell" unter bestimmten Umständen geboten sein kann, z. B. bei einem vermuteten anti-homosexuellen Hintergrund der Tat, muß jedenfalls verhindert werden, daß die Polizei Listen sämtlicher gespeicherter Homosexueller erstellen und zu unterschiedlichen Zwecken auswerten kann.

Das SMI hat uns daraufhin mitgeteilt, daß seitens des LKA Sachsen an einer Lösung gearbeitet werde, die mißbräuchliche Recherchierbarkeit des Datums "homosexuell" für Listen Homosexueller technisch zu unterbinden. Dies soll insbesondere durch die Einschränkung des Kreises der Berechtigten sowie durch ein Protokollierungsverfahren erreicht werden. Nähere Einzelheiten hierzu sind uns noch nicht bekannt. Leider enthält die Stellungnahme der Staatsregierung zu meinem 3. Tätigkeitsbericht (Landtagsdrucksache 2/2753) kein klares Votum für eine datenschutzgerechte Lösung: So heißt es lapidar, daß die entsprechenden technischen Vorkehrungen direkt vom Landeskriminalamt geprüft würden. Ich hoffe nicht, daß "technischer Aufwand" als Vorwand angeführt wird, um grundrechtsschützende Verwaltungsmaßnahmen zu unterlassen.

5.9.6 Aufzeichnung eingehender Anrufe

Im Land Brandenburg werden durch ein digitales Aufzeichnungssystem bei den Polizeidienststellen grundsätzlich alle dort eingehenden Anrufe gespeichert. Ich habe die Praxis der Speicherung eingehender Anrufe bei den sächsischen Polizeidienststellen überprüft. Nach Auskunft des SMI werden in Sachsen nur die über Notrufnummern und die im Polizeisondernetz geführten Gespräche in den Lagezentren der Polizeidienststellen durchweg aufgezeichnet. Bei Telefonaten, die im Polizeisondernetz geführt werden, handelt es sich nur um (dienstliche) Gespräche zwischen Polizeibediensteten, die über die Aufzeichnungsfunktion informiert sind. Die Aufzeichnung von Notrufen ist erforderlich, damit wichtige Informationen in eiligen Notfällen nicht verlorengehen. Alle anderen Ferngespräche können nur manuell bei Bedarf aufgezeichnet werden, wenn dies zur polizeilichen Aufgabenerfüllung im konkreten Einzelfall aus Gründen der Gefahrenabwehr oder zum Zweck der Strafverfolgung erforderlich ist. Eine Aufzeichnung des gesamten ankommenden und abgehenden Fernsprechverkehrs, insbesondere über den Vermittlungsplatz, erfolgt nicht. Das SMI hat dies inzwischen auch im Erlaßwege geregelt.

5.9.7 Speicherung von Wiederholungsfällen bei Verstößen im ruhenden Verkehr

Im Zusammenhang mit einer Eingabe habe ich untersucht, ob in Sachsen örtliche Karteien oder Dateien geführt werden, in denen personenbezogene Daten zu Parkverstößen gespeichert werden, um Mehrfachtäter erkennen zu können. Die Zulässigkeitsvoraussetzungen für die Speicherung von Daten auf dem Gebiet des Verkehrsrechts sind in den §§ 28 bis 30 a StVG abschließend geregelt. Nach diesen Vorschriften rechtfertigen Verstöße im ruhenden Verkehr, also meist Ordnungswidrigkeiten mit Bagatellcharakter, die mit einem Verwarnungsgeld geahndet werden, keine Speicherung. Damit wären örtliche, bei den Ordnungsämtern der Städte und Gemeinden oder den Bußgeldstellen der Landratsämter geführte manuelle Karteien oder elektronische Dateien unzulässig. Das gleiche gilt für systematische Auswertungen der aus kassentechnischen Gründen zu Verwarnungsgeldverfahren geführten örtlichen Dateien. Auch solche wären einer "Verkehrssünderkartei" gleichzusetzen und damit unzulässig.

Auf meine Initiative hin hat das SMI dies alles durch Erlaß sichergestellt.

5.9.8 Bildaufzeichnungen bei Demonstrationen

Bei zwei friedlich verlaufenen Demonstrationen im April 1995 in Dresden setzte die Polizei Videotechnik ein. Dies nahm ich zum Anlaß, den zuständigen Stellen die datenschutzrechtlichen Grenzen polizeilicher Bildaufzeichnungen aufzuzeigen:

Bei Bildaufzeichnungen, die im Zusammenhang mit Versammlungen angefertigt werden, ist stets zu beachten, daß das Grundrecht der Versammlungsfreiheit (Art. 8 GG, Art. 23 SächsVerf) zu den grundlegenden und unentbehrlichen Funktionselementen eines demokratischen Gemeinwesens zählt. Weil auch die innere Entschlußfreiheit, an einer Versammlung teilzunehmen, geschützt wird, liegt nach der Rechtsprechung des Bundesverfassungsgerichts bereits ein Eingriff in dieses Grundrecht vor, wenn die Angst vor staatlicher Überwachung dazu führt, daß man lieber auf die Grundrechtsausübung verzichtet (BVerfGE 65, 1 [43]). Somit sind "exzessive Observationen und Registrierungen" bei Demonstrationen Grundrechtseingriffe (BVerfGE 69, 315 [349]).

Im Zusammenhang mit öffentlichen Versammlungen unter freiem Himmel dürfen deshalb Bild- und Tonaufnahmen nur nach besonders sorgfältiger Abwägung unter den in § 19a i. V. m. § 12a VersammlG genannten Voraussetzungen angefertigt werden. Das heißt, daß Bildaufnahmen nur zulässig sind, wenn Anhaltspunkte für die Annahme vorliegen, daß von den Teilnehmern erhebliche Gefahren für die öffentliche Sicherheit oder Ordnung ausgehen. Nur dann dürfen mitgeführte Kameras gezeigt und aktiviert werden; zuvor sollten sie auch nicht (drohend) gezeigt oder ersichtlich abgedeckt werden.

Bei der datenschutzrechtlichen Überprüfung des eingangs geschilderten Sachverhalts habe ich festgestellt, daß gewisse Anhaltspunkte für die Annahme erheblicher Gefahren für die öffentliche Sicherheit und Ordnung vorlagen und somit die Voraussetzungen des § 12a Abs. 1 VersG wohl erfüllt waren. Ferner konnte ich mich davon überzeugen, daß einige Bildaufzeichnungen zulässig zur Verfolgung von Straftaten der Staatsanwaltschaft übergeben wurden. Die übrigen Aufzeichnungen wurden gemäß dem Versammlungsgesetz gelöscht.

5.9.9 Polizeiliche Einsichtnahme in das Personalausweis- und Paßregister

Aus der Eingabe eines Petenten ergab sich, daß das bei einer Geschwindigkeitsmessung angefertigte Beweisfoto mit dem Personalausweis- und Paßregister abgeglichen worden war. Nach einem neueren Beschluß des Bund-Länder-Fachausschusses für Straßenverkehrsordnungswidrigkeiten soll künftig ein Abgleich des Beweisfotos mit dem Personalausweis- und Paßregister nicht mehr - wie bisher - auf Verstöße beschränkt werden, die zur Eintragung ins Verkehrszentralregister führen, sondern auch bei Verstößen im Verwarnungsbereich zulässig sein.

Einen pauschalen Abgleich des Beweisfotos mit dem im Personalausweis und Paßregister abgelegten Paßbild bei Verstößen, die im Verwarnungsbereich begangen werden, halte ich im Hinblick auf das verfassungsrechtliche Verhältnismäßigkeitsgebot für problematisch. Zumindest muß vor der Durchführung des Bildabgleichs in jedem Einzelfall geprüft werden, ob es nicht andere Maßnahmen gibt, die auch zum Erfolg führen; insbesondere darf gemäß § 2b Abs. 2 Nr. 3 PAuswG nur abgeglichen werden, wenn es nicht möglich war, den Betroffenen vorher aufzusuchen oder vorzuladen, um ihn bei dieser Gelegenheit zu identifizieren. Das Aufsuchen und die Vorladung sind mildere Mittel als der - ohne Kenntnis des Betroffenen erfolgende - Bildabgleich und sollten zuvor versucht werden. Das SMI hat bereits in Aussicht gestellt, meine Anregungen in den Erlaß zu übernehmen.

5.9.10 Lichtbilder bei Verkehrsüberwachung

Verkehrsüberwachungsstellen der Landratsämter, der kreisfreien Städte und des Polizeivollzugsdienstes fertigen bei Verkehrsüberwachungen an Ampelanlagen und zur Geschwindigkeitskontrolle Lichtbilder an, um den Täter des konkreten Verkehrsverstoßes zu ermitteln. Im Ordnungswidrigkeitenverfahren wird dann ein als Beweismittel dienendes Foto dem Halter des Kraftfahrzeugs übersandt.
Wie ich erfahren habe, wird dabei nicht von allen Verkehrsüberwachungsstellen des Freistaates Sachsen das Bild des auf diesen Fotos erkennbaren Beifahrers geschwärzt. Die Ablichtung des Beifahrers ist jedoch zur Aufgabenerfüllung der Verkehrsüberwachung nicht erforderlich - somit unzulässig.
Auf meine Empfehlung hin hat das SMI durch Erlaß festgelegt, daß die zuständigen Stellen vor der Versendung der Lichtbildaufnahmen die darauf abgebildete Person des Beifahrers schwärzen.

5.9.11 Datenübermittlung der Polizei an Fußballvereine zur Erteilung von Stadionverboten

Von der "Bundesarbeitsgemeinschaft Fanprojekte" erfuhr ich, daß einige Polizeidienststellen zur Durchsetzung von Stadionverboten polizeiliche personenbezogene Daten an Fußballvereine übermitteln sollen. Auf der Grundlage dieser Daten würden Stadienverbote vorbereitet, um gewaltbereite Fußballfans an Gewalttaten zu hindern.

Sofern es sich hierbei um eine regelmäßige Übermittlung personenbezogener Daten von Amts wegen handelt, richtet sich die Zulässigkeit nach § 45 Abs. 1 SächsPolG. Danach darf die Polizei von Amts wegen personenbezogene Daten an Private nur übermitteln, soweit sie damit ihre Aufgaben (Gefahrenabwehr, Straftatenverfolgung) erfüllt. Der Erlaß eines Stadionverbotes wird zwar durch das Hausrecht des Fußballvereins gedeckt, ist jedoch keine Maßnahme polizeilicher Gefahrenabwehr. Diese Aufgabe fällt allein in den Zuständigkeitsbereich der Polizei. Da die der Ausübung des Hausrechts dienende Datenübermittlung zur polizeilichen Aufgabenerfüllung (Gefahrenabwehr) nicht erforderlich ist, ist sie - soweit sie regelmäßig und von Amts wegen erfolgt - unzulässig. Ob es zulässig ist, daß die Polizei auf Antrag der nicht-öffentlichen Stelle (hier des Fußballvereins) nach § 45 Abs. 2 SächsPolG personenbezogene Daten übermittelt, hängt vom jeweiligen Einzelfall ab.
Nichts spricht dagegen, wenn sich der Fußballverein als Inhaber des Hausrechts selbst - neben den Bemühungen der Polizei - gegen Gefahren, die sein Objekt oder die sich darin aufhaltenden Personen betreffen, schützt. Dies kann auch durch Einstellung eigener oder fremder Ordnungskräfte geschehen, die sich untereinander nach Maßgabe des Bundesdatenschutzgesetzes Daten übermitteln dürfen. Eine Zusammenarbeit zwischen Polizei und Fußballvereinen darf jedoch nicht dazu führen, daß personenbezogene Daten, die von der Polizei unter Umständen aufgrund besonderer hoheitlicher Befugnisse gewonnen werden, an Private übermittelt werden, die diese

Daten möglicherweise selbst nicht hätten erheben dürfen.
Das SMI hat die Polizeipräsidien angewiesen, entsprechend meiner Rechtsauffassung zu verfahren. Bislang seien den Polizeipräsidien jedoch keine polizeilichen Datenübermittlungen an Fußballvereine zur Durchsetzung von Stadionverboten bekanntgeworden.

5.9.12 Praktikanten bei der Polizei

Datenschutzrechtlichen Bedenken begegnet der Einsatz von Schülern im Rahmen von Betriebspraktika bei Polizeibehörden. Soll den Schülern mit diesen Veranstaltungen ein Eindruck von der praktischen Arbeit der Polizei vermittelt werden, ist es nämlich unvermeidbar, daß die Praktikanten personenbezogene Daten von Dritten zur Kenntnis erhalten, ihnen also im rechtlichen Sinne Daten der Betroffenen übermittelt werden. Für diesen Eingriff in das Grundrecht auf informationelle Selbstbestimmung fehlt die rechtliche Voraussetzung, nämlich eine gesetzliche Grundlage. Auf § 45 Abs. 1 SächsPolG können solche Datenübermittlungen schon deshalb nicht gestützt werden, weil es sich bei diesen Praktika um schulische Veranstaltungen handelt, deren Durchführung nicht zu den in § 2 SächsPolG festgelegten Aufgaben der Polizeidienststellen gehört.

Aus Anlaß entsprechender Informationsveranstaltungen der nordrhein-westfälischen Polizei, die der Landesbeauftragte für den Datenschutz Nordrhein-Westfalen beanstandet hat, habe ich das SMI auf die datenschutzrechtliche Unzulässigkeit hingewiesen. Das SMI teilte mir erfreulich klar mit, daß Schülerbetriebspraktika in Sachsen nicht bei Polizeibehörden durchgeführt werden und auch zukünftig - allerdings im Hinblick auf Sicherheitsaspekte und die damit verbundene versicherungsrechtliche Problematik - nicht geplant sind.

5.9.13 Eingaben

Auch in diesem Jahr wandten sich wieder zahlreiche Bürger an mich, die sich durch die Datenverarbeitung der Polizei in ihrem Persönlichkeitsrecht subjektiv verletzt sahen. Die Petenten beklagten unzulässige polizeiliche Erhebungen, Speicherungen oder Übermittlungen ihrer personenbezogenen Daten. In einigen der von mir untersuchten Fälle lag dies daran, daß tatsächlich andere Stellen die Polizei nicht in der nötigen Weise unterrichtet hatten. So speicherte in einem Fall die Polizei die Daten eines Betroffenen im Polizeilichen Auskunftssystem Sachsen (PASS), obwohl die Gründe für eine Speicherung durch eine Verfahrenseinstellung schon entfallen waren. Über die Verfahrenseinstellung war die Polizeidienststelle jedoch vom Gericht nicht rechtzeitig informiert worden.

In einem anderen Fall wurden schwerwiegende polizeiliche Maßnahmen (erkennungsdienstliche Behandlungen) allein aufgrund von Angaben in einer privaten

Strafanzeige ergriffen. Im nachhinein stellte sich heraus, daß infolge - von der Polizei nicht aufgeklärter - bestimmter Umstände Polizeieinsatz nicht gerechtfertigt gewesen war.

In allen Fällen habe ich mich davon überzeugt, daß die Daten der Betroffenen unverzüglich gelöscht wurden.

5.10 Verfassungsschutz

5.10.1Internes Informationssystem

Das Landesamt für Verfassungsschutz wird demnächst ein internes Informationssystem betreiben. Mit der automatisierten Datei will das Landesamt den Informationsfluß zwischen den eigenen Fachbereichen intensivieren sowie das Auffinden von Informationen und das Recherchieren nach Fundstellen verbessern. Darüber hinaus wird das System für die Vorgangsverwaltung und Aktenführung im Rahmen der gesetzlichen Aufgabe des Landesamtes, bei Sicherheitsüberprüfungen mitzuwirken, eingesetzt werden.

Von Beginn der konzeptionellen Vorarbeiten an hat mich das Landesamt fortlaufend über den Stand seines Vorhabens unterrichtet. Wie der mir vom SMI vorgelegte Entwurf einer Einrichtungsanordnung zeigt, verfügt das automatisierte Verfahren über einen hohen Datenschutzstandard. So werden wegen der Sensibilität der umfangreichen Verknüpfungsmöglichkeiten streng definierte Zugriffsberechtigungen technisch abgesichert. Die detaillierte Arbeitsanweisung enthält abgestufte Regelungen zu den Überprüfungsfristen und ermöglicht damit eine individuell auf den Einzelfall abgestimmte Speicherungsdauer.

5.10.2 Eingaben

Mehrere Petenten haben mich um datenschutzrechtliche Überprüfung der möglicherweise ihre Person betreffenden Datenverarbeitung des Landesamtes für Verfassungsschutz gebeten. Bei meinen Kontrollen habe ich keine Verstöße gegen datenschutzrechtliche Vorschriften festgestellt.

Aus Anlaß einer Eingabe, die ich nach einer datenschutzrechtlichen Überprüfung mit einem Bescheid beantwortet habe, gegen den sich der Petent mit einer Klage beim Verwaltungsgericht gewandt hat, weise ich darauf hin, daß von Bescheiden meiner Behörde keine unmittelbare rechtliche Wirkung auf die Rechte und Pflichten des Betroffenen oder der datenverarbeitenden Stelle ausgeht. Diese Bescheide sind nicht als Verwaltungsakte angreifbar.

5.11 Landessystemkonzept / Landesnetz

Im August 1995 hat das SMI nach Abschluß des Modellversuches (3. Tätigkeitsbericht, S. 58) einen Berichtsentwurf „Modellversuch zum Landesnetz des Freistaates Sachsen“ vorgelegt. Darin werden mehrere Betreibermodelle für die Leitungs ebene des Landesnetzes vorgeschlagen. Mögliche Betreiber sind dabei die Polizei, eine andere öffentliche Stelle, private Auftragnehmer bzw. Mischformen. Die erste Variante wird bislang vom SMI favorisiert.

Beim Betrieb der Leitungsebene fallen personenbezogene Daten an (Verbindungsdaten). In meiner Stellungnahme habe ich aufgeführt, daß die Zulässigkeit polizeilicher personenbezogener Datenverarbeitung sich nach dem Sächsischen Polizeigesetz bemißt: Grundvoraussetzung ist danach, daß die Datenverarbeitung zur Erfüllung polizeilicher Aufgaben erfolgt (§ 35 i. V. m. § 1 SächsPolG), also dem Schutz der freiheitlichen demokratischen Grundordnung, der Gewährleistung der ungehinderten Ausübung der Grundrechte und der staatsbürgerlichen Rechte, der Verhinderung und vorbeugenden Bekämpfung von Straftaten sowie der Abwehr künftiger Gefahren dient.

Von diesem Aufgabenkatalog wird der Betrieb eines Telekommunikationsnetzes für polizeiexterne Stellen ersichtlich nicht erfaßt; die Verarbeitung personenbezogener Daten im Kommunikationsnetz kann mithin nicht auf die polizeispezifischen Rechtsvorschriften der §§ 36 ff. SächsPolG gestützt werden.
Für den - über § 35 SächsPolG grundsätzlich eröffneten - Rückgriff auf die Auffangvorschriften des Sächsischen Datenschutzgesetzes - und damit eine mögliche Klassifizierung des geplanten Netzbetriebes als Datenverarbeitung im Auftrag - ist ebenfalls kein Raum: Selbst als Auftragnehmerin müßte die Polizei in Erfüllung ihrer Aufgaben (§ 35 SächsPolG) handeln. Diese Voraussetzung kann unter keinem Aspekt erfüllt werden. Ein rein polizeibezogenes Betreibermodell für die Leitungsebene des gesamten Landesnetzes wäre demnach mit dem geltenden Recht nicht vereinbar.
In der Zwischenzeit hat das SMI den Vorschlag unterbreitet, das Polizeinetz als Teil des Landesnetzes zu benutzen, dabei aber in diesem Teil auf der Leitungsebene personenbezogene Daten nicht zu verarbeiten. Für die Abrechnung der geführten Telefonate werden bei einem Gespräch nur die Anlagenkennzahl der mit dem Polizeinetz verbundenen TK-Anlage (z. B. Anlage der Staatsregierung in Dresden) und die im öffentlichen Telefonnetz angefallenen Gebühreneinheiten durch die Polizei erfaßt. Die Verbindungsdaten fallen nur in der mit dem Polizeinetz verbundenen TK-Anlage an. Die technische Umsetzung dieses Vorschlages werde ich begleiten.
Zu bedenken bleibt, daß das Landesnetz bei einer solchen Konstruktion vom Zuschnitt des Polizeinetzes "abhängig" (also an Entscheidungen der Innenminister auf Bundes- und Landesebene gebunden) ist und sich wohl auchdem Bedarf der Polizei "unterzuordnen" hat. Ob daraus auch datenschutzrechtliche Probleme entstehen, wird sich erweisen.

Die Bedarfsanalyse im letzten Berichtsentwurf des SMI vom Dezember 1995 ist allerdings insgesamt nicht nachvollziehbar: das Ressortprinzip macht eine

Bedarfsanalyse schwierig; wertvolle Einzelergebnisse können eine Gesamtsicht nicht ersetzen.

Die im Juni 1995 bei der Staatskanzlei neugegründete „Koordinierungs- und Beratungsstelle für Informations- und Kommunikationstechnik (KoBIT)“, die die Arbeit der BIT (3. Tätigkeitsbericht, S. 58 f.) fortführt, hat sich unter anderem dieser Aufgabe angenommen und ist nach dem Kabinettbeschluß vom 13. Februar 1996 mit der Erarbeitung eines Konzeptes „InfoHighway Landesverwaltung“ beauftragt. Ich werde mich an diesen Arbeiten weiter engagiert beteiligen.

5.12 Sonstiges

Ehrung von Alters- und Ehejubilaren durch den Bundespräsidenten

Das SMI hat eine Bekanntmachung über die Neufassung der Grundsätze über die Ehrung von Alters- und Ehejubilaren durch den Bundespräsidenten vom 10. Oktober 1995 im SächsABl. Nr. 50, S. 1264 veröffentlicht. Darin werden die "zuständigen" Behörden zu Datenerhebungen (u. a. über die finanziellen und gesundheitlichen Verhältnisse der Jubilare) angehalten.

Ich habe das SMI um Stellungnahme zu folgenden Fragen gebeten:
- Wer sind die "zuständigen" Behörden?
- Woher bzw. von wem stammen die der Ehrung zugrundeliegenden Angaben (insbesondere über die finanziellen Verhältnisse)?
- Welche Rechtsgrundlagen ermächtigen zur Datenerhebung und zur Datenübermittlung (an das Bundespräsidialamt)?

Vom SMI erhielt ich nach geraumer Zeit die Nachricht, daß meine Anfrage an die Staatskanzlei abgegeben worden sei. Dort werden die Fragen noch geprüft; eine abschließende Stellungnahme liegt noch nicht vor.

6 Finanzen

6.1 Automatisierte Datenübermittlung der Vermessungsämter an die Finanzbehörden

Nach Nr. 6.5 meines 3. Tätigkeitsberichtes habe ich gegen den Entwurf einer Vereinbarung zwischen SMF und SMI über die beabsichtigte automatisierte Datenübermittlung der Vermessungsämter an das LfF keine Einwände vorgebracht.

Diese Vereinbarung kam jedoch zunächst nicht zustande, weil nach Ansicht des SMI § 23 Nr. 6 SVermG eine entsprechende Verordnung erforderlich mache.

Das SMF bat mich um Stellungnahme, die wie folgt lautete:

Obwohl § 29 Abs. 3 BewG *regelmäßige* Datenübermittlungen an die Finanzämter *nicht ausdrücklich zuläßt* und wenig normenklar ist (nach BVerfGE 65, 1 ff. muß für den Betroffenen aus dem Gesetz erkennbar sein, welche personenbezogenen Daten verarbeitet werden sollen), wird die Vorschrift von der einschlägigen Kommentarliteratur als ausreichende Rechtsgrundlage auch für regelmäßige Datenübermittlungen sämtlicher Behörden (also u. a. der Katasterbehörden) an die Finanzbehörden angesehen. Danach verdrängt § 29 Abs. 3 BewG als spezielle *bundesgesetzliche* Datenübermittlungsvorschrift die *landesrechtliche* Regelung in § 23 Nr. 6 SVermG, wonach regelmäßige Datenübermittlungen der Katasterverwaltung an andere Behörden nur aufgrund einer Rechtsverordnung zulässig wären.

Einer Rechtsverordnung des SMI für die beabsichtigten regelmäßigen Datenübermittlungen zwischen den Kataster- und Finanzbehörden bedarf es daher nicht.

6.2 Beauftragung des e-Postdienstes der Deutschen Post AG mit dem Druck, der Kuvertierung und dem Versand von Grund- und Gewerbesteuerbescheiden

Im Angebot des e-Postdienstes befindet sich auch der Druck, die Kuvertierung und der Versand von Grund- und Gewerbesteuerbescheiden. Eine Stadtverwaltung fragte, ob eine solche Auftragsvergabe zulässig sei.

Da eine solche Verfahrensweise mit § 30 AO (Steuergeheimnis) kollidiert, habe ich das SMF um Stellungnahme gebeten.

Von dort war zu hören, daß der Einsatz des e-Postdienstes im Besteuerungsverfahren zwischen den obersten Finanzbehörden des Bundes und der Länder erörtert würde. Anfang Januar 1996 teilte mir das SMF mit, daß sich die AO-Referenten zwar mit der e-Post-Frage befaßt hätten, die Angelegenheit jedoch noch nicht entscheidungsreif sei.

Weil im e-Post-Verfahren nicht ausgeschlossen werden kann, daß Unbefugte durch Einloggen in das Netz Kenntnis von steuerrelevanten Daten erhalten, bleibe ich 'am Ball'.

7 Kultus

7.1 Schule

Entwurf der "Verordnung des SMK über Förderschulen im Freistaat Sachsen (Schulordnung Förderschulen - SOFS)"

Der Aufbau der Förderschulen und ihre Aufgaben sind bisher nicht in einer Rechtsvorschrift geregelt. Diesem Zustand soll durch die *Schulordnung Förderschulen* abgeholfen werden.

Von besonderem datenschutzrechtlichem Interesse ist die Regelung des Verfahrens zur Aufnahme der Schüler. Bisher schreibt die "Verwaltungsvorschrift des Sächsischen Staatsministeriums für Kultus über die im Rahmen des Aufnahmeverfahrens an Förderschulen zu verwendenden Formblätter" vom 12. Januar 1994 eine sehr umfangreiche "Pädagogisch- psychologisch-medizinische Dokumentation" mit Gutachten verschiedener Stellen vor.

Nun bestimmt § 12 Abs. 4 des Entwurfes der SOFS, daß bei Einleitung und Durchführung des Aufnahmeverfahrens für Kinder, die eine Förderschule besuchen sollen, die Datenschutzbestimmungen zu beachten sind. Damit wird auf das Sächsische Datenschutzgesetz und, soweit die Gesundheitsämter betroffen sind, auf das SächsGDG verwiesen.

Ich habe mich bereits im Hinblick auf die ursprüngliche Fassung des Entwurfs dafür ausgesprochen, in der SOFS als bereichsspezifischer Norm die erforderlichen datenschutzrechtlichen Bestimmungen zu treffen. Eine solche Regelung kann und muß nicht jedes Detail des Aufnahmeverfahrens erfassen. Sie sollte jedoch so weit wie möglich bestimmen, welche Stelle zu welchen Zwecken welche Daten erhebt, an wen sie übermittelt werden und wie der Empfänger sie nutzen darf. Dies gebietet die Tatsache, daß höchst sensible Daten über Kinder, auch ihr soziales Umfeld, verarbeitet werden. Insbesondere ist klarzustellen, daß personenbezogene Daten nur im erforderlichen Umfang zu erheben und zu übermitteln sind, Art und Nutzung also je nach Behinderung sehr unterschiedlich sein können. Bisher ist diese Präzisierung nicht erfolgt.

Neben der Regelung in der Rechtsverordnung wird die Gestaltung der oben erwähnten Dokumentation von großer Bedeutung sein. Mein Vorschlag, der Schulaufsichtsbehörde, die die Entscheidung über den Besuch einer Förderschule trifft, nicht Befunde und Diagnosen, sondern, ähnlich wie bei einer Einstellungsuntersuchung im öffentlichen Dienst, nur Ergebnisse zugänglich zu machen, ist nach Auffassung des SMK nicht realisierbar. Die Ergebnismitteilung genüge nicht, weil die Schulaufsichtsbehörde den Verwaltungsakt der Aufnahme oder Nichtaufnahme begründen und daher auch die Grundlagen der Empfehlung durch die begutachtenden

Stellen kennen müsse.

Die Dokumentation ist in einer Reihe von Punkten zu überprüfen, insbesondere, um eine nach Art der Behinderung differenzierte Datenverarbeitung zu erreichen. Die Gespräche zu dieser Dokumentation werden in Kürze aufgenommen.

7.2 Datenschutz im kirchlichen Bereich

Benutzung kirchlicher Archive

Ein Petent bat mich, einige Fragen aus einem kirchlichen Archivbenutzungs-Antragsformular auf ihre datenschutzrechtliche Zulässigkeit hin zu überprüfen. Er war der Ansicht, daß nicht alle in dem Antragsformular gestellten Fragen zur Entscheidung über sein Recht auf Einsicht in das kirchliche Archiv, mithin zur Aufgabenerfüllung des kirchlichen Archivs, erforderlich seien.

Ich habe dem Petenten mitgeteilt, daß ich für die Beurteilung derartiger Einzelfragen wegen der insofern bestehenden Kompetenzkompetenz der Kirchen (vgl. BVerfGE 7, 198 [207] und ständige Rechtsprechung), die aus dem kirchlichen Selbstbestimmungsrecht (Art. 140 GG i. V. m. Art. 137 Abs. 3 WRV) herrührt, nicht zuständig bin. Im Verhältnis zu den als Körperschaften des öffentlichen Rechts anerkannten Religionsgesellschaften habe ich mich auf die Feststellung zu beschränken, daß im Bereich der Kirchen ausreichende Datenschutzregelungen (§ 14 SächsDSG) bzw. ausreichende Datenschutzmaßnahmen (§ 30 Abs. 3 SächsMG) gelten bzw. getroffen sind. Daß dies in Sachsen der Fall ist, habe ich in meinem 2. und 3. Tätigkeitsbericht jeweils unter 7.2 dargelegt.

Ich habe den Petenten an den Datenschutzbeauftragten der betreffenden Kirche verwiesen.

8 Justiz

8.1 Verwaltungsvorschrift über das Justizpressewesen

Trotz meiner eingehenden Kritik im 3. Tätigkeitsbericht (Nr. 8.4) und trotz mehrerer Besprechungen, in denen ich die - in diesem Fall einfach gelagerten - datenschutzrechtlichen Zusammenhänge nochmals aufzeigen mußte, hat das SMJus die gebotene Überarbeitung der Verwaltungsvorschrift über das Justizpressewesen vom 5. Dezember 1994 (Sächsisches Justizministerialblatt Nr. 11/1994) abgelehnt. Ich habe daher die Regelung des § 6 Abs. 2 der Verwaltungsvorschrift, wonach der Presse die Anklageschrift vor Beginn der Hauptverhandlung zur Einsichtnahme zugänglich

gemacht werden kann, wenn anzunehmen ist, daß das Strafverfahren in der Öffentlichkeit eine besondere Beachtung finden werde, förmlich beanstandet (Wortlaut NJW 1996, 977).

Abgesehen davon, daß die Verwaltungsvorschrift - im folgenden kurz als "VwV" bezeichnet - wegen fehlender Normqualität ohnehin nicht als Rechtsgrundlage für die Übermittlung personenbezogener Daten in Betracht kommt, waren folgende Überlegungen Inhalt meiner Kritik:

- Die in § 4 Abs. 3 VwV enthaltenen Restriktionen sind nach dem Aufbau der Vorschrift, insbesondere wegen der in § 6 VwV gewählten Überschrift "Sonderregelungen für Strafverfahren" nach dem Willen des Staatsministers der Justiz - dieser Wille kommt auch in dieser Gliederung und in dieser gewählten Überschrift zum Ausdruck - gerade nicht heranzuziehen. Die Heranziehung dieser systematisch voneinander unabhängigen Vorschriften ist auch deshalb offenbar nicht vorgesehen, weil jede Veröffentlichung personenbezogener Daten dem Persönlichkeitsschutz zuwiderläuft, ein schutzwürdiges privates Interesse verletzt und daher in allen Fällen eine Veröffentlichung nicht statthaft wäre. Die in § 6 Abs. 2 VwV enthaltenen "Sonderregelungen für Strafverfahren" wären folglich insgesamt obsolet.

- Schon § 4 Abs. 2 Buchst. a VwV zeigt ein mangelhaftes Verständnis vom Vorbehalt des Gesetzes. Denn wegen des Grundrechtsschutzes personenbezogener Daten (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG; Art. 33 SächsVerf) ist nicht die Suche nach einer Verbotsnorm, sondern die Suche nach einer Erlaubnisnorm geboten.

- Besondere Schutzvorschriften zugunsten jugendlicher und heranwachsender Angeschuldigter/Angeklagter fehlen (§ 48 JGG). Auch die übrigen, die Nichtöffentlichkeit der Hauptverhandlung regelnden Vorschriften (§§ 169 ff. GVG) werden nicht hinreichend deutlich berücksichtigt, zumal die Entscheidung über die Nichtöffentlichkeit durch Beschluß in der Hauptverhandlung getroffen wird. Betrifft ein solcher Beschluß auch die Verlesung des Anklagesatzes, so läuft der Beschluß ins Leere, wenn der Anklagesatz zuvor veröffentlicht worden ist. .

- Das öffentliche wörtliche Mitteilen der Anklageschrift ist strafbar, § 353 d Nr. 3 StGB. Würde ein Behördenleiter oder ein Pressereferent entsprechend der Verwaltungsvorschrift handeln, wäre stets zu prüfen, ob Anstiftung zu diesem Delikt seitens des Sächsischen Staatsministers der Justiz vorliegt. Denn bereits jede wörtliche Mitteilung aus der Anklageschrift an die Presse ist eine öffentliche Mitteilung und erfüllt den Straftatbestand. Von einer "vertraulichen" Mitteilung, bei der man über das Tatbestandsmerkmal "öffentlich" diskutieren könnte, ist in der Verwaltungsvorschrift keine Rede. Teilnahme kann nicht schon deshalb ausgeschlossen werden, weil nach § 6 Abs. 2 Satz 5 VwV der mitteilenden Stelle eine Pflicht zum Hinweis auf § 353 d StGB auferlegt wird. Dieser Hinweis ist ein Widerspruch in sich. Diese Kritik teilt auch der Deutsche Anwaltverein, wenn er in seiner Stellungnahme zur Verwaltungsvorschrift (Schreiben vom 1.12.1995) ausführt: "Bei dieser Unterstützung

an Anstiftung oder Beihilfe, wenn nicht gar Mittäterschaft zur Verwirklichung des Tatbestandes des § 353 d Ziffer 3 StGB zu denken liegt nicht fern".

- Das Bundesverfassungsgericht (BVerfGE 71, 206 ff.) hat die Zwecktauglichkeit der Vorschrift des § 353 d Nr. 3 StGB - wie üblich insoweit zurückhaltend - bewertet und sie nicht "schlechthin" und "objektiv" für ungeeignet zum Schutz der Rechtsgüter (Unbefangenheit der Verfahrensbeteiligten - Schöffen, Zeugen, Sachverständige -; Schutz vor vorzeitiger Bloßstellung und Unschuldsvermutung) gehalten. Es führt u. a. aus, gegenüber der erkennbaren Meinungsäußerung komme dem Zitat die besondere Überzeugungs- und Beweiskraft des Faktums zu (BVerfG a.a.O. S. 216 m.w.N.). Eine wortgetreue Wiedergabe von Aktenteilen erwecke - zu Recht - den Eindruck amtlicher Authentizität und bezwecke dies auch. Gerade die wortgetreue Wiedergabe gefährde die Rechtsgüter in besonderer Weise.

  Wäre bekannt, daß "Gerichtsberichterstatter" (Wer ist das? Wie man zu einem Presseausweis kommt, ist bekannt; will man unter Mißachtung des Grundrechts der Pressefreiheit im Freistaat Sachsen differenzieren?) jedoch besonders Authentisches - wenn auch nicht wörtlich, weil dies strafbar wäre - aus den selbst eingesehenen Akten berichten, so könnten sich die Berichte "das Gewicht amtlicher Authentizität beilegen", was aber - so BVerfGE a.a.O. S. 219 - gerade vermieden werden soll. Die Vorschrift des § 353 d Nr. 3 StGB, die gerade den Eindruck verhindern soll, "als sitze der interessierte Journalist neben dem interessierten Staatsanwalt und tippe dessen Verfügungen unvermittelt ins Blatt" (Hassemer in NJW 1985, S. 1923), würde inhaltsleer.

- Anklagen in großen Strafsachen werden in Einzelfällen nur modifiziert zugelassen. Werden die die ursprüngliche Anklageschrift modifizierenden Zulassungsbeschlüsse veröffentlicht, müssen sich Staatsanwaltschaft und Gericht in ihrer die Hauptverhandlung vorbereitenden Arbeit dem Votum der Öffentlichkeit stellen.

- Auch in der Zeit zwischen der Eröffnung des Hauptverfahrens und der Verlesung des Anklagesatzes in öffentlicher Hauptverhandlung kommt es nicht selten zu zulässigen Absprachen zwischen Staatsanwaltschaft, Verteidigung und Gericht in bezug auf eine Verfahrenskonzentration, insbesondere auf die Entscheidung, Verfahrensteile durch endgültige oder einstweilige Einstellung abzuschließen. Sollten derartige vernünftige Prozeduren zur Verfahrensökonomie öffentlich gemacht werden? (Denn die in der Hauptverhandlung verlesene Anklage entspräche nicht - mehr - der Fassung, in die Einblick gewährt wurde.) Schließlich ist zu bedenken, daß in der fraglichen Zeit auch Verfahrensbeendigungen ohne Hauptverhandlung möglich sind.

- Durch die Regelung des § 6 Abs. 2 VwV werden die Schöffen schlechter gestellt als die Presse: Sie erfahren aus den Medien Einzelheiten, die ihnen bis zur Hauptverhandlung verborgen bleiben sollen; ein zentraler Schutzzweck des § 353 d StGB, die Unbefangenheit von Verfahrensbeteiligten, würde unterlaufen. Es erscheint nicht ausgeschlossen, daß Laienrichter, welche der Presse bereits vor Prozeßbeginn

den authentischen, wenn auch formell nicht wörtlichen Inhalt von Teilen der Akten im Wortlaut haben entnehmen können, ihr Urteil nicht mehr allein auf der Grundlage der Hauptverhandlung bilden, wie die Strafprozeßordnung das im Interesse eines rechtsstaatlichen Verfahrens voraussetzt. Ebenso kann die Zuverlässigkeit von Zeugenaussagen unter vorzeitiger Unterrichtung leiden (siehe BVerfGE a.a.O. S. 217).

- Öffentlichkeit ist im deutschen Strafverfahrensrecht erst für die Hauptverhandlung vorgesehen. Die vorausgehenden Verfahrensstadien dagegen sind, guten alten rechtstheoretischen Grundsätzen folgend, ganz bewußt nicht öffentlich.
- Die bloße Schwärzung von Namen führt erfahrungsgemäß nur in wenigen Fällen zu einer wirklichen Anonymisierung. Dies gilt insbesondere für spektakuläre Verfahren. Überdies ist unklar, ob sich "dabei" in § 6 Abs. 2 S. 4 VwV auf die Anklageveröffentlichung oder nur auf die Anklagesatz-Veröffentlichung bezieht. Im übrigen führen Schwärzungen auch zur Sinnentstellung und Verwirrung.
- Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat am 9./10. November 1995 in einer Entschließung u. a. ausgeführt: "Bis zur rechtskräftigen Verurteilung ist die Unschuldsvermutung zugunsten des Beschuldigten oder Angeklagten zu beachten. Zu unterlassen sind alle Auskünfte oder Erklärungen, die geeignet sind, die Unbefangenheit der Verfahrensbeteiligten zu beeinträchtigen. *Akteneinsicht durch Medienvertreter kommt nicht in Betracht.*"
- Der Sächsische Richterverein hat mit Schreiben vom 27. Dezember 1995 u. a. ausgeführt: "Da jedoch die in § 6 Abs. 2 Satz 1 VwV vorgesehene Möglichkeit, soweit uns dies bekannt ist, von der Presse ebensowenig genutzt wird wie diejenige, bereits vor der Hauptverhandlung der Presse den Anklagesatz mitteilen zu können, halten wir die Streichung dieser Passage für empfehlenswert, sehen aber darin keinen Grund, die Regelung insgesamt anzugehen."
- Der Deutsche Anwaltverein hat mit Schreiben vom 1. Dezember 1995 mitgeteilt, daß meine Bedenken vollinhaltlich geteilt werden.

Angesichts der in anderen Bundesländern (z. B. Hamburg, Hessen) praktizierten - durchaus verfassungskonformen - Auskunftsverfahren der Justizbehörden sollte es dem Sächsischen Staatsministerium der Justiz auf einfache Weise möglich sein, einen rechtsstaatlich sicheren Weg zu finden, dem Informationsrecht der Presse Genüge zu tun.

Die mir vorliegenden Einschätzungen des Präsidenten des Hanseatischen Oberlandesgerichts, des dortigen Generalstaatsanwalts sowie des Generalstaatsanwalts beim Oberlandesgericht Frankfurt am Main lassen ein hohes Maß an verfassungsrechtlicher Sensibilität erkennen. Demgemäß wird in ihrem Zuständigkeitsbereich der Anklagesatz nicht bekanntgegeben, um eine "doppelte Prangerwirkung" (Präsident des Hanseatischen Oberlandesgerichts vom 28.8.1995, Az.: 4103-1c/1/7/) zu vermeiden, der der Angeklagte durch Veröffentlichung des Anklagevorwurfs sowohl vor als auch nach Beginn der Hauptverhandlung ausgesetzt wäre.

Beispielhaft hervorzuheben ist auch die in den vom Generalstaatsanwalt beim Oberlandesgericht Frankfurt am Main herausgegebenen Richtlinien für die Zusammenarbeit der Staatsanwaltschaften mit den Medien enthaltene Weisung, in Pressemitteilungen grundsätzlich keine Namen von Jugendlichen zu nennen.

8.2 Justizvollzug

8.2.1 Kontrolle der Justizvollzugsanstalt Justizpressewesen

Die bereits im Jahr 1994 begonnene Querschnittskontrolle der Datenverarbeitung der JVA Waldheim habe ich nunmehr abgeschlossen. Folgende Themen standen dabei im Vordergrund:
- Briefkontrolle
- Gefangenenpersonalakten
- Anstaltsarzt
- Besuchskontrolle
- Anfertigung von Lichtbildern
- Telekommunikationsanlage
- Automatisierte Datenverarbeitungstechnik.

Weil es im Strafvollzug an bereichsspezifischen Rechtsgrundlagen fehlt, ist die Zulässigkeit der Verarbeitung personenbezogener Daten nicht einfach zu beurteilen. Das Strafvollzugsgesetz gibt mit seinen Generalklauseln lediglich vage Zulässigkeitskriterien vor, ohne Art und Umfang der Datenverarbeitung im einzelnen klar und für den Einzelnen erkennbar zu umreißen. Nur als Auslegungshilfe können die für die Justizvollzugsanstalten geltenden Verwaltungsvorschriften herangezogen werden. Weil die genannten Regelungen aber keine ausreichend normenklaren Rechtsgrundlagen sind, die einen Eingriff in das Persönlichkeitsrecht der Gefangenen rechtfertigen könnten, muß sich die Datenverarbeitung im Justizvollzug auf das notwendige Maß beschränken. Einzig in Betracht kommende Kriterien sind demnach die Behandlung der Gefangenen und Sicherheitsaspekte. Die Übermittlung von Daten der Gefangenen an Stellen außerhalb der Anstalt kann nur ausnahmsweise zulässig sein. Das Recht auf informationelle Selbstbestimmung, das als Grundrecht natürlich auch und gerade Gefangenen zusteht, zwingt dazu, jeden einzelnen Schritt der Datenverarbeitung auf seine Erforderlichkeit hin zu überprüfen.

Bei meiner Kontrolle habe ich festgestellt, daß dieser Grundsatz nicht durchgängig beachtet wird. So sind Daten, die von der Justizvollzugsanstalt rechtmäßig für einen bestimmten Zweck erhoben wurden, anschließend zu offenen, ungeregelten Zwecken anstaltsintern weitgehend frei verfügbar. Die Anstaltsleitung vertrat zunächst hierzu den Standpunkt, daß die Daten anstaltsintern aus Sicherheits- und Behandlungsgründen relativ frei verfügbar sein müßten. Etwas anderes gelte nur für die Weitergabe von Daten "nach draußen". Dies sei ihrer Ansicht nach nur unter ganz engen

Voraussetzungen zulässig.

Diese Auffassung ist aus den eingangs genannten Gründen nicht haltbar. Vollzugsbedienstete sollten sich vielmehr nur dann von personenbezogenen Daten Kenntnis verschaffen dürfen, wenn dies zur Erfüllung der ihnen jeweils obliegenden Aufgaben erforderlich ist. Beispielsweise dürften für den ärztlichen Dienst die Namen von Tatgenossen oder die Straftaten des Gefangenen, für den Werkstattleiter Familienstand und Zahl der Kinder und für alle Bediensteten - außer den Anstaltspfarrer - das religiöse Bekenntnis des Gefangenen ohne Bedeutung sein. Erforderlich ist deshalb eine differenzierte Zugangsregelung, deren Einhaltung dadurch sichergestellt werden sollte, daß jede Einsichtnahme in Gefangenenpersonalakten von den einsichtnehmenden Bediensteten selbst kurz protokolliert wird. Zumindest sollten die Bediensteten, die von Ihrem Aufgabenzuschnitt her grundsätzlich nicht auf die Gefangenenpersonalakten zugreifen müssen, den Grund für die Einsichtnahme stichwortartig schriftlich festhalten.

Ich habe die weiteren Ergebnisse der Kontrolle in einem umfassenden Bericht zusammengefaßt. Wegen der Aufgeschlossenheit der Anstaltsleitung gegenüber den von mir aufgezeigten datenschutzrechtlichen Problemkreisen und der erfreulichen Tatsache, daß noch während meiner Kontrolle mehrere Mängel beseitigt wurden, gehe ich davon aus, daß noch bestehende - offenbar haushaltsbedingte - Defizite der Datensicherung (z. B. im Bereich des Anstaltsarztes) behoben werden.

8.2.2 Lichtbilder von Gefangenen

In Sachsen wie auch in anderen Bundesländern werden von allen Gefangenen - unabhängig von der Vollzugsdauer - bei der Erstaufnahme Lichtbilder angefertigt. Gegen diese Praxis habe ich nichts einzuwenden, weil sie einen verhältnismäßigen Eingriff in das Grundrecht auf informationelle Selbstbestimmung darstellt, der durch die Vorschrift des § 86 Abs. 1 Nr. 2 StVollzG gedeckt ist. Diese Maßnahme ist zur Sicherung des Vollzugs erforderlich, um Personenverwechslungen beim Gefangenentransport, bei Außenarbeitseinsätzen, Entlassungen etc. zu verhindern. Solche Verwechslungen kommen immer wieder vor. Sie sind wohl nicht nur bei Gefangenen mit einer langen Vollzugsdauer zu befürchten. Nicht entgegen steht die ermessensbindende Vorschrift Nr. 23 Abs. 2 der Vollzugsgeschäftsordnung, die die Pflicht begründet, von Gefangenen mit *mehr als einem Jahr* Dauer Freiheitsstrafe Lichtbilder anzufertigen. Hieraus kann nicht zwingend der Umkehrschluß gezogen werden, daß von den übrigen Gefangenen keine Lichtbilder angefertigt werden dürfen.

Hingegen halte ich es für zwingend geboten, daß die Gefangenen zum Zeitpunkt ihrer Entlassung ausdrücklich darüber belehrt werden, daß sie die Vernichtung der erkennungsdienstlichen Unterlagen verlangen können. Daß sie auf dieses Recht oftmals nur bei ihrer Aufnahme hingewiesen werden - mit der Folge des Vergessens bei der Entlassung -, ist nicht akzeptabel. Die Formulierung in § 86 Abs. 3 Satz 2 StVollzG,

die dazu verpflichtet, die Gefangenen über dieses Recht spätestens bei der Entlassung zu unterrichten, eröffnet der Justizvollzugsanstalt zwar einen Entscheidungsspielraum in bezug auf den Zeitpunkt, zu dem sie den Gefangenen über sein Recht belehrt. Das heißt aber nicht, daß die Justizvollzugsanstalt einen willkürlichen Zeitraum wählen kann. Weil der Gefangene erst bei seiner Entlassung die Vernichtung der Lichtbilder verlangen kann, ist dieser Zeitpunkt grundsätzlich auch der richtige, um den Gefangenen auf sein Antragsrecht hinzuweisen. Sofern keine Gründe entgegenstehen, hat die JVA die Pflicht, den Gefangenen zu diesem Zeitpunkt über sein Recht zu belehren. Das SMJus hat meine Vorschläge aufgegriffen und die Justizvollzugsanstalten angewiesen, die Gefangenen auch bei ihrer Entlassung ausdrücklich darüber zu belehren, daß sie die Vernichtung der erkennungsdienstlichen Unterlagen verlangen können.

Im übrigen sollte erwogen werden, die Lichtbilder auch ohne Antrag des Gefangenen nach dessen Entlassung von Amts wegen zu vernichten. Da die erkennungsdienstlichen Unterlagen nach der Entlassung des Gefangenen zur Aufgabenerfüllung der Justizvollzugsanstalt nicht mehr erforderlich sind (hierfür spricht § 86 Abs. 3 Satz 2 StVollzG) und die Vernichtung der Unterlagen jetzt schon von einer Entscheidung des Gefangenen abhängt, sollte eine Vereinfachung dieser Vorschrift angestrebt werden.

8.2.3 Briefkontrolle von Behördenpost

Aus einer Eingabe habe ich erfahren, daß in einer Justizvollzugsanstalt nicht nur die Privatpost, sondern auch die Behördenpost der Gefangenen zu Zwecken der Briefkontrolle von der Poststelle in Abwesenheit der Gefangenen geöffnet wird.

Nach § 29 Abs. 3 StVollzG kann der Schriftwechsel der Gefangenen aus Gründen der Behandlung oder der Sicherheit und Ordnung der Anstalt überwacht werden. Bei dieser Vorschrift handelt es sich aber um eine Ermessensvorschrift; es ist also Sache des Anstaltsleiters, Art und Umfang der Überwachung individuell festzulegen. Bei der Ausübung des Ermessens muß auch das Recht auf informationelle Selbstbestimmung beachtet werden. Dabei muß unter anderem berücksichtigt werden, daß die Briefüberwachung eine erhebliche Belastung der - für die Resozialisierung dringend notwendigen - Kommunikation des Gefangenen mit der Außenwelt darstellt. Aus diesem Grund sollte eine Inhaltskontrolle grundsätzlich nur im Einzelfall durchgeführt werden, wenn die eingangs genannten Voraussetzungen im konkreten Fall vorliegen. Bei Behördenbriefen kann ich mir keine Konstellation vorstellen, die es notwendig macht, aus Gründen der Behandlung oder der Sicherheit und Ordnung der Anstalt eine inhaltliche Kontrolle vorzunehmen. Hier sollte es genügen, wenn jeder Brief auf mögliche unerwünschte Gegenstände abgetastet wird bzw. geprüft wird, ob der Brief tatsächlich vom vermerkten Absender kommt (Sichtkontrolle). Diese Kontrolle sollte im Beisein des Gefangenen durchgeführt werden, damit dieser die Gewißheit erhält, daß seine Briefe nicht doch regelmäßig gelesen werden.

8.2.4 Informations- und Verwaltungssystem (IVS)

Dieses bei den Vollzugsgeschäftsstellen der Justizvollzugsanstalten eingerichtete System soll die Daten der Gefangenen automatisiert erfassen, verwalten und recherchierbar machen. In meinem 3. Tätigkeitsbericht (Nr. 8.6) habe ich die datenschutzrechtlichen Mängel aufgezeigt. Nach einer erneuten Kontrolle des inzwischen weiterentwickelten Systems ist deutlich geworden, daß die Zugriffberechtigung noch unzulänglich gestaltet ist. Weil das Programm im vergangenen Jahr nur im Bereich der Justizvollzugsgeschäftsstellen und des Anstaltsleiters eingesetzt wurde, habe ich eine differenzierte Zugriffsberechtigung zunächst für entbehrlich gehalten. Gleichzeitig habe ich aber auch deutlich gemacht, daß vor Erweiterung des Anwenderkreises eine solche differenzierte Zugriffsregelung programmtechnisch sichergestellt sein muß. Lesezugriff dürfen die Bediensteten nur auf solche Daten haben, die sie für ihre konkrete Aufgabenerfüllung benötigen. Leider enthält auch die überarbeitete Programmbeschreibung noch immer keine differenzierten Regelungen des Lesezugriffes.

Des weiteren habe ich angeregt, eine Löschungskomponente in das Programm einzuarbeiten, die dem Bearbeiter automatisch Löschfristen anzeigt oder bestimmte Daten selbsttätig löscht. Daneben müssen Protokollierungsregeln und Regeln für Löschungsfristen geschaffen werden, bevor dieses System endgültig in den Justizvollzugsanstalten eingesetzt wird. Dabei sollte unter anderem bedacht werden, daß die Protokollierungsdaten im Logbuch nur so lange vorgehalten werden dürfen, wie sie für Kontrollzwecke auch tatsächlich benötigt werden (etwa sechs Monate). Anschließend sind sie zu löschen. Schließlich sollten die Zugriffsmöglichkeiten des Systemadministrators so weit wie möglich eingeschränkt werden, oder es sollte auf andere Weise sichergestellt werden, daß dieser nicht unbefugt an personenbezogene Informationen gelangen kann.

8.2.5 Kontrolle der Post des Sächsischen Datenschutzbeauftragten an Gefangene

Wie jedermann hat auch der Gefangene das Recht nach § 22 SächsDSG, sich an den Sächsischen Datenschutzbeauftragten zu wenden. Dieses Recht wird dadurch besonders geschützt, daß das Sächsische Datenschutzgesetz es verbietet, daß der Betroffene wegen seiner Eingabe benachteiligt oder gemaßregelt wird. Für den Justizvollzug, der den vom Anstaltspersonal abhängigen Gefangenen ohnehin in seiner Entschlußfreiheit hemmt, bedeutet dies, daß der Schriftverkehr der Gefangenen mit dem Sächsischen Datenschutzbeauftragten nicht überwacht werden sollte. Ich habe daher dem SMJus empfohlen, entsprechend dem in Niedersachsen bereits praktizierten Verfahren meine Schreiben an Gefangene nicht zu überwachen, wenn ich den Anstaltsleiter in gesondertem Anschreiben um ungeöffnete Weiterleitung bitte.

Das SMJus hat meinem Anliegen durch Erlaß vollständig entsprochen.

Vgl. auch unter 10.1.10 und 10.1.11.

8.3 Staatsanwaltschaften

8.3.1 Verwaltungsvorschrift zur Zusammenarbeit von Staatsanwaltschaft und Polizeivollzugsdienst bei der Bekämpfung der Organisierten Kriminalität

Für die Strafverfolgungsbehörden ist die eindeutige Zuordnung kriminogener Erscheinungen zur - unscharf definierten - "Organisierten Kriminalität" (OK) ein großes Problem, weil im Einzelfall erst Indizien für die Annahme einer OK gesammelt werden müssen. Zu Beginn der Ermittlungen kann der OK-Bezug zunächst oft nur vermutet werden. So fällt es den Strafverfolgungsbehörden schwer, die Verhältnismäßigkeit von Ermittlungsmaßnahmen, die tief in das Persönlichkeitsrecht eingreifen, zu begründen. Gehört bei der OK die Begehung von Straftaten zu ihrer Organisationsstruktur, kann die Informationsgewinnung über die OK ein doppeltes Ziel verfolgen: die Aufklärung bereits begangener Straftaten (Repression) und die Zerstörung der Struktur (Prävention). Da im Bereich der OK außerdem Strafanzeigen - vor allem aus Angst - nur äußerst selten erstattet werden, wollen die Gefahrenabwehr- und Strafverfolgungsbehörden besondere Ermittlungsmethoden entwickeln. So sieht die Gemeinsame Verwaltungsvorschrift des SMJus und des SMI über die Zusammenarbeit von Staatsanwaltschaft und Polizeivollzugsdienst bei der Bekämpfung der OK Initiativermittlungen vor. Hierbei handelt es sich um Ermittlungen, die bereits im Vorfeld eines Verdachts zulässig sein sollen; somit um Ermittlungen, die ohne einen Anfangsverdacht i. S. v. § 152 Abs. 2 StPO und ohne eine Gefahr im Sinne des Polizeigesetzes vorgenommen werden dürfen. Sie sollen dazu dienen, diesen Verdacht erst einmal zu gewinnen. Bei solchen Ermittlungen im Vorfeld kommt jedoch dem Grundsatz der Verhältnismäßigkeit besondere Bedeutung zu: Es muß verhindert werden, daß Staatsanwaltschaft und Polizei unter Nennung des Zauberwortes "OK" heimlich und ohne konkrete Vorstellungen von dem, was geklärt werden soll, ermitteln. Je weiter im Vorfeld denkbarer Straftaten ermittelt wird, um so größer ist die Gefahr, daß Daten Unbeteiligter verarbeitet werden. Dieses Risiko muß minimiert werden.

Ungeachtet der zu beklagenden Tatsache, daß die für die Datenverarbeitung im Rahmen der Strafverfolgung maßgebende Strafprozeßordnung noch immer nicht den Vorgaben des Volkszählungsurteils des Bundesverfassungsgerichts genügt (so das Bundesverfassungsgericht in einem Beschluß vom 5. Juli 1995) und die polizeirechtlichen Verarbeitungsregeln des Sächsischen Polizeigesetzes weitgehend auf das als Auffanggesetz konzipierte Sächsische Datenschutzgesetz verweisen, sind an Initiativermittlungen folgende Mindestanforderungen zu stellen:

- Die Umstände, die das neue Instrumentarium rechtfertigen, sind so konkret wie

möglich zu bezeichnen. Die Verwaltungsvorschrift versucht dies ansatzweise, indem bestimmte Straftatbestände und Indizien genannt werden, bei denen ein Bezug zur OK vermutet werden kann.

- Konkrete Regelungen müssen die Behandlung der Daten regeln, deren Verarbeitung sich im nachhinein als nicht ergiebig und daher als nicht notwendig herausstellt. Hierunter fallen insbesondere Daten unbeteiligter Dritter. Aber auch Daten von Betroffenen, bei denen zwar der Bezug zur OK ausgeschlossen werden kann, nicht aber der Verdacht in bezug auf die Begehung einer anderen Verfehlung, dürfen nicht uneingeschränkt verarbeitet werden. Zumindest sofern sich aus den Initiativermittlungen kein Anfangsverdacht für die Begehung einer Straftat ergibt, sind Verwendungs- und Verwertungsverbote festzulegen. Wenn Initiativermittlungen im Bereich der OK schon ausnahmsweise zugelassen werden, müssen sie unter Beachtung des Zweckbindungsgrundsatzes auf diesen Bereich beschränkt bleiben.
- Unerläßlich ist die ausführliche Dokumentation des Umfanges der Initiativermittlungen und - soweit möglich - ihre spätere Offenlegung gegenüber allen Betroffenen.

8.3.2 Geplantes staatsanwaltschaftliches Registrierungs- und Informationssystem (STARIS) in Sachsen

Nach den Plänen des SMJus sollen alle sächsischen Staatsanwaltschaften mittels STARIS automatisiert auf Verfahrensdaten zugreifen können, um z. B. parallel laufende Ermittlungsverfahren, die von mehreren Staatsanwaltschaften gegen einen Beschuldigten geführt werden, konzentrieren zu können.

STARIS bedarf als automatisiertes Abrufverfahren nach § 8 Abs. 1 SächsDSG einer gesetzlichen Grundlage. Eine solche ist jedoch auf Landesebene nicht vorhanden. Es besteht lediglich für ein bundesweites, staatsanwaltschaftliches Verfahrensregister beim Bundeszentralregister mit den Vorschriften der §§ 474 ff. StPO eine gesetzliche Grundlage.

Weil die Einrichtung eines bundesweiten Registers aber zeitlich noch nicht abzusehen ist (nicht jede Verwaltung arbeitet so schnell wie die aufbaugewöhnte sächsische Verwaltung), denkt das SMJus daran, für einen Übergangszeitraum STARIS als (erste) Aufbaustufe des künftigen Bundessystems anzusehen; diesen Gedanken will ich im Interesse einer effektiven Verbrechensbekämpfung unterstützen, soweit die Rechtsordnung dies eben zuläßt.

Wenn folgende Fragen positiv beantwortet werden, kann ich dem Projekt daher zustimmen:

1. Ist STARIS in Aufbau und Technik identisch mit dem System, das für die künftige Teilhabe sächsischer Staatsanwaltschaften am Bundessystem Verwendung findet? Oder anders gefragt: Soll STARIS dereinst im Bundessystem aufgehen?

2. Sind die für die Einrichtung des Bundessystems zuständigen Stellen des Bundes über die Planung des SMJus informiert, STARIS als erste Stufe des Bundessystems zu betreiben?

3. Berücksichtigt STARIS im Laufe der Aufbauzeit jeweils die Vorgaben der nach § 476 Abs. 5 noch zu erwartenden Errichtungsanordnung des Bundessystems?

4. Eröffnet STARIS anderen öffentlichen Stellen (Polizei, Nachrichtendienste) keine Abfragemöglichkeiten?

Die Antwort des SMJus hat dazu noch keine vollkommene Klarheit gebracht; wir bleiben im kooperativen Dialog.

8.3.3 Mitteilung der Staatsanwaltschaften und Gerichte über den Ausgang von Ermittlungsverfahren

Um den Polizeidienststellen die Prüfung zu ermöglichen, ob die für polizeiliche Zwecke erhobenen personenbezogenen Daten auch nach einer Verfahrenseinstellung weiter bei der Polizei gespeichert werden dürfen, müssen die Staatsanwaltschaften und die Gerichte auf einem Formular den Verfahrensausgang der sachbearbeitenden Polizeidienststelle mitteilen. Insbesondere weil die Einstellung eines Verfahrens nicht zwangsläufig bedeutet, daß jeglicher Verdacht gegen die betreffende Person ausgeräumt ist - nur in diesem Fall werden die polizeilichen Daten nach den KpS-Richtlinien gelöscht - ist eine möglichst detaillierte Beschreibung der Einstellungsgründe erforderlich. Nur so kann die Polizei prüfen, ob die Daten zur polizeilichen Aufgabenerfüllung noch erforderlich sind. Erfolgt nur eine Mitteilung über die Einstellung des Verfahrens ohne Nennung der Gründe, werden die polizeilichen Daten im Zweifel von der Polizei nicht gelöscht. Das SMI hat mir gegenüber beklagt, daß in der Praxis oftmals keine ausreichenden Mitteilungen erfolgten. Dementgegen hat mir das SMJus nach einer Praxisbefragung geschrieben, die Staatsanwaltschaften kämen ihren Mitteilungspflichten "überwiegend" nach und seien vom SMJus außerdem auf diese Pflichten in geeigneter Weise hingewiesen worden.

Die Ressorts sollten über das Problem sprechen und mir ihre gemeinsame Auffassung mitteilen, wie die Praxis nun wirklich aussieht.

8.3.4 Einstellung des Ermittlungsverfahrens wegen Schuldunfähigkeit

Die Einstellung eines Verfahrens wegen Schuldunfähigkeit gemäß § 170 Abs. 2 StPO ist in der Regel bis zur Vollendung des 90. Lebensjahres des Betroffenen aus dem Bundeszentralregister ersichtlich (§ 11 Abs. 1 Nr. 1, §§ 20, 24 Abs. 2 BZRG). Auch in Führungszeugnisse für Behörden wird dieser Registereintrag aufgenommen (§ 32 Abs. 3 Nr. 3 BZRG). Von dieser Eintragung erfährt der Betroffene jedoch in der Regel nichts, da die Führungszeugnisse meist direkt an die Behörden übersandt werden (§ 31 Abs. 5 BZRG). Aus den im Volkszählungsurteil aufgeführten Grundsätzen zum Recht auf informationelle Selbstbestimmung ergibt sich jedoch, daß grundsätzlich jeder wissen können muß, wer was wann und bei welcher Gelegenheit über ihn weiß (BVerfGE 65, 1 [43]). Sofern demnach keine schutzwürdigen Interessen gefährdet werden, muß der Betroffene sowohl auf den Grund der Einstellung als auch auf sein Recht auf Entfernung der Eintragung nach § 25 BZRG aufmerksam gemacht werden. Vom Berliner Datenschutzbeauftragten habe ich erfahren, daß die dortige Generalstaatsanwaltschaft eine solche Regelung getroffen habe. Ein entsprechendes Vorgehen habe ich beim SMJus angeregt. Es hat mir mitgeteilt, das Bundesministerium erarbeite in diesem Zusammenhang einen Gesetzentwurf, der einen sachgerechten Ausgleich zwischen den berechtigten Schutzinteressen des Betroffenen und den Informationsinteressen von Rechtspflege und Verwaltung suche. Darüber hinaus hat das SMJus erfreulicherweise zugesagt, eine entsprechende Handhabung durch den Generalstaatsanwalt wie in Berlin anzuregen.

8.3.5 Staatsanwaltschaft ersucht Gesundheitsamt um Patientendaten

Eine Staatsanwaltschaft ersuchte ein Gesundheitsamt um Auskunft zu Erkrankungen, die möglicherweise im Zusammenhang mit verdorbener Schulspeisung stehen könnten. Der sieben Punkte umfassende Fragekatalog zielte auf beim Gesundheitsamt vorliegende patientenbezogene Einzelinformationen, die vom Arztgeheimnis geschützt sind. Dem auf § 161 StPO gestützten staatsanwaltschaftlichen Ersuchen in seiner jetzigen Form durfte das Gesundheitsamt nicht entsprechen, weil es ansonsten gegen § 203 Abs. 1 Nr. 1 StGB verstoßen hätte:

Das Arztgeheimnis (§ 2 der vorläufigen Berufsordnung für die Ärzte Sachsens; § 203 StGB) ist zentraler Bestandteil der Rechtsordnung. Ein "anvertrautes" Geheimnis i. S. d. § 203 Abs. 1 StGB sind nicht nur die Diagnose oder sonstige Lebensumstände des Patienten, sondern auch der bloße Umstand, daß sich ein bestimmter Patient in ärztliche Behandlung begeben hat. Das Arztgeheimnis darf nur nach einer wirksam erklärten Einwilligung des Patienten oder bei Vorliegen einer gesetzlichen Offenbarungsbefugnis (z. B. §§ 12, 13 Geschlechtskrankheitengesetz etc.) oder unter den Voraussetzungen eines rechtfertigenden Notstandes (§ 34 StGB) durchbrochen werden. Es ist ständige Rechtsprechung, daß das Strafverfolgungsinteresse bezüglich bereits begangener Delikte (anders als zur Verhinderung beabsichtigter Straftaten) die Verletzung der

Schweigepflicht im Regelfall nicht rechtfertigt. Nur bei besonders schweren und mit einer noch bestehenden, nachhaltigen Störung des Rechtsfriedens verbundenen Verbrechen (Wiederholungstäter schwerster Delikte; terroristische Gewalttaten) kann die Durchbrechung des Arztgeheimnisses zu Zwecken der Strafverfolgung gerechtfertigt sein.

In der vorliegenden Angelegenheit war es im gegenwärtigen Stadium des Ermittlungsverfahrens nicht erforderlich, die erkrankten Personen "namentlich aufzulisten" und die "bisherigen Erkenntnisse zum Krankheitsgeschehen" personenbezogen zu übermitteln: Zur Klärung der Frage, inwieweit die Schulspeisung für die Erkrankungen kausal war, war es ausreichend, zunächst nur die Gesamtzahl der erkrankten Personen, der stationären Behandlungen etc. mitzuteilen - mithin nur Daten ohne Personenbezug zu übermitteln.

Erst wenn anhand dieser Daten der vorbezeichnete Kausalzusammenhang als eindeutig indiziert erscheint, wäre der nächste Schritt zulässig - nämlich die Entbindung der Ärzte des Gesundheitsamtes von der Schweigepflicht durch die Patienten. Nur so könnte eine Offenbarung der nach § 203 StGB vom Arztgeheimnis geschützten Daten rechtmäßig sein. Nur in diesem Verfahrensstadium besteht dann eine Amtspflicht des Gesundheitsamtes bzw. des dortigen Arztes, sich um eine Befreiung von seiner Schweigepflicht zu bemühen.

Auf meine Intervention hin wurden die personenbezogenen Patientendaten nicht übermittelt.

8.3.6 Einsicht in Ermittlungsakten der Staatsanwaltschaft durch Dritte

Nach Auskunft einer sächsischen Staatsanwaltschaft erhalten auch nicht am Verfahren beteiligte Rechtsanwälte grundsätzlich Einsicht in die gesamte Ermittlungsakte, ohne daß hierbei nach dem Grund des Auskunftsbegehrens differenziert wird. Bei Vorgängen, in denen Ermittlungsverfahren miteinander verbunden wurden, ist es nach Meinung der Staatsanwaltschaft wegen des entstehenden Verwaltungsaufwandes nicht möglich, bestimmte Aktenteile von der Einsicht auszuschließen oder nur eine Aktenauskunft zu erteilen.

Diese Praxis halte ich für bedenklich. Die Gewährung von Einsicht in Ermittlungsakten an Dritte ist noch immer nicht gesetzlich geregelt. Nach den Richtlinien für das Straf- und Bußgeldverfahren (RiStBV) - die wegen fehlender Normqualität keine Rechtsgrundlage für einen Eingriff in das Grundrecht auf informationelle Selbstbestimmung sein können - kann Akteneinsicht gewährt werden, wenn der Antragsteller ein berechtigtes Interesse an der Einsichtnahme hat und wenn, wie es in Nr. 185 Abs. 4 RiStBV heißt, "sonst Bedenken nicht bestehen". Dabei ist eine Abwägung vorzunehmen, bei der insbesondere entgegenstehende schutzwürdige

Interessen des Betroffenen zu berücksichtigen sind. Deshalb muß das berechtigte Interesse des Antragstellers an der Akteneinsicht so dargelegt und begründet werden, daß erkennbar ist, welche in der Ermittlungsakte enthaltenen Informationen von dem berechtigten Interesse an der Übermittlung umfaßt werden.

Die Ermittlungsakte sollte anschließend nur dann zur Akteneinsicht übersandt werden, wenn eine Auskunft zur Wahrnehmung der berechtigten Interessen des Antragstellers nicht genügt. Sollte die Auskunft aus technischen Gründen nicht möglich sein, ist die Akteneinsicht grundsätzlich auf die Aktenteile zu beschränken, für deren Kenntnisnahme das berechtigte Interesse nachvollziehbar dargelegt wurde. Daraus folgt, daß insbesondere bei Akten, in denen Verfahren miteinander verbunden wurden, grundsätzlich nur die Aktenbestandteile an den Dritten herauszugeben sind, die er für die Wahrnehmung schutzwürdiger Interessen benötigt. Gerade Ermittlungsakten, die sensible Daten (auch über Dritte) enthalten, die zum Teil mit Zwang (z. B. Zeugenaussagen) oder aufgrund besonderer Befugnisse der Strafverfolgungsbehörden erhoben wurden, dürfen nicht pauschal und ohne Einzelfallabwägung Dritten zur Kenntnis gelangen. Der - von mir nicht verkannte - erhöhte Verwaltungsaufwand ist hinzunehmen, kann er doch gering gehalten werden: Wie bereits in Niedersachsen praktiziert, können bestimmte sensible Daten gesondert in der Ermittlungsakte abgeheftet und ohne großen Verwaltungsaufwand der Akte vor Gewährung der Akteneinsicht entnommen werden.

Auf meine Anregung hin hat das SMJus eine entsprechende Verfahrensweise angekündigt.

8.4 Sozialer Dienst der Justiz

Bewährungshilfe (EDV-System RESO)

Das EDV-System "RESO" beim Sozialen Dienst der Justiz des Freistaates Sachsen soll die bisher von den Bewährungshelfern manuell erledigten Aufgaben computergestützt erledigen helfen. Ich habe das System einer eingehenden Kontrolle unterzogen und dabei folgendes festgestellt:

Das Programmsystem ist auf Einzelplatz-PC der Bewährungshelfer installiert. Die Daten der Probanden werden nicht auf der Festplatte gespeichert, sondern nur auf der Diskette des sie betreuenden Bewährungshelfers. Die Abarbeitung von RESO setzt somit das Einlegen einer “Daten”-Diskette voraus. Programm und Daten sind also 'hardwaremäßig' getrennt. Hierdurch soll bei einem eventuellen Diebstahl eines PC der Schutz der personenbezogenen Daten gewährleistet werden. Folge einer solchen Verfahrensweise ist allerdings auch, daß die auf der Diskette gespeicherten (sensiblen) Probandendaten ohne großen Aufwand unauffällig transportiert und leicht kopiert werden können. Davon abgesehen besteht eine Mißbrauchsgefahr nicht nur durch

Externe. Auch die Beschäftigten des Sozialen Dienstes können sich einfach und nur schwer kontrollierbar Kopien der Disketten fertigen und so zum Beispiel auf die Probandendaten eines anderen Bewährungshelfers zugreifen. Ferner besteht die Gefahr, daß Kopien von Disketten aufbewahrt werden, deren Daten längst gelöscht sein müßten. Ich habe dem SMJus diese Mißbrauchsmöglichkeiten aufgezeigt und detaillierte Empfehlungen zur Mängelbeseitigung gegeben.

Weiterhin habe ich angeregt, die gespeicherten Probandendaten nach Ablauf eines Jahres zu löschen, weil sie danach zur Aufgabenerfüllung des Bewährungshelfers nicht mehr erforderlich sind (§ 19 SächsDSG). Auch die im Textprogramm erstellten Schreiben sollten grundsätzlich, sobald sie ausgedruckt und in der Akte abgeheftet sind, gelöscht oder gar nicht erst abgespeichert werden.

Gewissen datenschutzrechtlichen Bedenken begegnete die Durchführung des im System enthaltenen Schuldenregulierungsprogramms. Eine Schuldenregulierung soll nach der Programmbeschreibung zwar nur mit schriftlicher Einwilligung (gemäß § 4 SächsDSG) des Probanden durchgeführt werden. Problematisch ist dabei jedoch die Frage der Freiwilligkeit. Von einer freiwilligen Entscheidung kann nur bei Gleichgeordneten, nicht aber bei einem Probanden gegenüber seinem Bewährungshelfer gesprochen werden. Bei einer vom Bewährungshelfer lediglich angebotenen Schuldenregulierung besteht stets die Gefahr, daß der Proband der Schuldenregulierung zustimmt, um vom Bewährungshelfer eine günstige Sozialprognose gestellt zu bekommen. Von einer Freiwilligkeit kann daher in einem solchen Fall nicht die Rede sein. Ich habe deshalb angeregt, dem Probanden zunächst eine externe Schuldenregulierung anzubieten. Es gibt zahlreiche Schuldnerberatungsstellen der Kommunen, Wohlfahrtsverbände oder Verbraucherzentralen, die eine kostenlose Schuldenregulierung durchführen. Sofern der Proband im Einzelfall eine Schuldenregulierung wünscht, können ihm diese Stellen vom Bewährungshelfer genannt werden. Bei dieser Art der Schuldenregulierung ist sichergestellt, daß sie auf einem wirklich freien Entschluß des Probanden beruht und nicht unter dem Eindruck, sich mit seinem Bewährungshelfer gutstellen zu müssen. Wenn die Schuldenregulierung im Rahmen der Resozialisierungsbemühungen und als Maßnahme der Bewährungsaufsicht im Einzelfall nötig ist, muß sie vom Bewährungshelfer (evtl. mit dem Rückhalt des Gerichts) angeordnet werden. Verstößt der Proband gegen diese Anordnung und unterläuft er die Schuldenregulierung, indem er keine Angaben macht, so verstößt er gegen Bewährungsauflagen.

Falls es erforderlich ist, eine Schuldenregulierung vom Bewährungshelfer durchzuführen, werden auch Daten solcher Dritter (z. B. Gläubiger) gespeichert, die über diese Speicherung nicht informiert sind. Deshalb muß auf jeden Fall sichergestellt werden, daß nach erfolgter Schuldenregulierung unverzüglich sämtliche dabei verarbeiteten Daten gelöscht werden.

8.5 Rechtsanwaltskammer; Notarkammer

8.5.1 Offenbarung von Mandantendaten gegenüber der Sächsischen Rechtsanwaltskammer im Rahmen der Erteilung der Befugnis zum Führen einer Fachanwaltsbezeichnung

Wenn ein Rechtsanwalt eine Fachanwaltsbezeichnung führen will, prüft die Rechtsanwaltskammer gemäß § 43 c BRAO, ob der Rechtsanwalt besondere Kenntnisse und Erfahrungen auf dem Fachgebiet erworben hat. Dies hat der Rechtsanwalt gemäß § 43 c Abs. 2 BRAO i. V. m. dem Rechtsanwaltsfachbezeichnungsgesetz (RAFachBezG) nachzuweisen.

Für den Bereich Steuerrecht ist der Nachweis besonderer praktischer Erfahrungen gemäß § 9 RAFachBezG in der Regel erbracht, wenn der Bewerber 50 Fälle als Rechtsanwalt selbständig bearbeitet hat. Um dies nachzuprüfen, verlangte die Sächsische Rechtsanwaltskammer die Vorlage einer Liste von 50 Mandanten sowie deren Steuernummer, anhand deren dann wohl einzelne Akten stichprobenartig überprüft werden. Wie ich in meinem 3. Tätigkeitsbericht (Nr. 8.13) ausgeführt habe, ist dieses Verfahren unzulässig, weil zur Prüfung der Fachanwaltsbefähigung die Übermittlung anonymisierter Akten völlig ausreicht. Ferner kann eine Einwilligung des Mandanten zur Weitergabe seiner Daten an die Rechtsanwaltskammer eingeholt werden.

Hierauf habe ich die Rechtsanwaltskammer hingewiesen. Zwar hat sie daraufhin angekündigt, in künftigen Verfahren auf die Angabe der Steuernummer zu verzichten, zur Notwendigkeit einer Anonymisierung der Daten jedoch nicht mit der gebotenen Klarheit Stellung genommen.

Ich habe das SMJus gebeten, die Kammer zu einer eindeutigen Aussage aufzufordern.

8.5.2 Entwurf einer Verwaltungsvorschrift über gerichtliche Mitteilungen von Klagen, Vollstreckungsmaßnahmen u. ä. an öffentliche Stellen

Rechtsanwälte und Notare unterliegen der Aufsicht ihrer Standesvertretungen sowie der Landesjustizverwaltung. Den Gerichten und den Gerichtsvollziehern werden häufig Sachverhalte aus der Berufs- und Lebensführung von Rechtsanwälten und Notaren bekannt, die Anlaß zu berufsrechtlichen Maßnahmen geben.
Damit die Rechtsanwalts- und Notarkammern und die Justizverwaltung prüfen können, ob sie Verfahren einleiten, beabsichtigt das Sächsische Staatsministerium der Justiz den Erlaß einer Verwaltungsvorschrift, die auf der Grundlage des § 36 a BRAO den Gerichten und Gerichtsvollziehern eine Pflicht zur Übermittlung personenbezogener Daten an die zuständigen Stellen auferlegt. Dieses Ziel kann mit dem Mittel der Verwaltungsvorschrift nicht erreicht werden, weil nach dem Volkszählungsurteil des Bundesverfassungsgerichts (BVerfGE 65, 1 ff.) Einschränkungen des Grundrechts auf informationelle Selbstbestimmung einer gesetzlichen Grundlage bedürfen. Gesetzlich geregelt ist durch § 36 a BRAO lediglich die *Befugnis*, nach einer Interessenabwägung personenbezogene Informationen zu übermitteln; eine *Pflicht* zur Übermittlung wird durch diese Vorschrift ausdrücklich nicht normiert. In das Grundrecht auf informationelle Selbstbestimmung würde tiefer als vom Gesetz gewollt eingegriffen, wenn den Regelungsadressaten kein Ermessensspielraum mehr verbliebe und sie zur Meldung gezwungen würden.
Die Verwaltungsvorschrift also kann wegen fehlender Normqualität eine Pflicht zur Übermittlung personenbezogener Daten nicht begründen. Inhaltlich verstößt die Regelung zudem gegen den Grundsatz der Verhältnismäßigkeit, da z. B. Forderungsklagen gegen einen Notar persönlich ohne Feststellung ihrer Begründetheit zum Gegenstand von Datenübermittlungen gemacht werden sollen. Außerdem fehlen bereichsspezifische Vorschriften zur Relevanzprüfung sowie zur Löschung und Vernichtung der erhaltenen Daten.
Meine Bedenken habe ich dem SMJus mitgeteilt.

9 Wirtschaft und Arbeit

9.1 Straßenverkehrswesen

9.1.1 Änderung von § 52 Abs. 2 BZRG

Im 3. Tätigkeitsbericht (Nr. 9.1.1) habe ich dargelegt, daß diese Vorschrift, die eine zeitlich unbegrenzte Verwertungsmöglichkeit von Vorstrafen zum Nachteil des Betroffenen ermöglicht, meines Erachtens unverhältnismäßig ist und nicht mit den Vorschriften und Zielsetzungen der Straßenverkehrszulassungsordnung in Einklang

steht.

Der Entwurf eines Gesetzes zur Änderung des Straßenverkehrsgesetzes und anderer Gesetze sieht nunmehr vor, daß die Vorschrift an die zeitlich gestaffelten Verwertungsvorschriften, die für die im Verkehrszentralregister enthaltenen Verurteilungen gelten, angepaßt wird.

Hiergegen bestehen keine datenschutzrechtlichen Bedenken.

9.1.2 Vorlage des Gutachtens einer medizinisch-psychologischen Untersuchungsstelle (MPU-Gutachten) für die Verlängerung der Fahrerlaubnis zur Fahrgastbeförderung ab dem fünfzigsten Lebensjahr

Eine Fahrerlaubnisbehörde verlangte von über fünfzigjährigen Antragstellern für die Verlängerung der Fahrerlaubnis zur Fahrgastbeförderung *grundsätzlich* die Vorlage des Gutachtens einer medizinisch-psychologischen Untersuchungsstelle und wies lediglich auf die Möglichkeit hin, statt dessen ein fachärztliches Gutachten beizubringen.

Ich habe der Fahrerlaubnisbehörde und dem SMWA mitgeteilt, daß diese Praxis nicht in Einklang mit der Rechtsprechung des Bundesverfassungsgerichts (NJW 1993, 2365) steht. Die Rechtslage läßt sich wie folgt zusammenfassen:

Vor Anforderung eines MPU-Gutachtens ist stets zu prüfen, ob bestehende Eignungszweifel nicht durch einen "schonenderen Eingriff", z. B. durch Vorlage eines fachärztlichen Gutachtens, behoben werden können. Dieser aus dem verfassungsrechtlichen Grundsatz der Verhältnismäßigkeit folgenden Forderung entspricht auch die neueste Rechtsprechung des Bundesverwaltungsgerichts (Urteil vom 17. Mai 1995 - 11 C 2.94): Wenn die Eignungsbedenken allein auf dem fortgeschrittenen Alter der Antragsteller beruhen, ist keine umfassende medizinisch-psychologische Durchleuchtung und Beurteilung der Gesamtpersönlichkeit im Hinblick auf das künftige Verkehrsverhalten erforderlich. Vielmehr muß das Untersuchungsprogramm aus Gründen der Bestimmtheit und Verhältnismäßigkeit auf verkehrsrelevante Fähigkeiten beschränkt werden, also auf Aufmerksamkeitsleistung, Belastbarkeit, Reaktions- und Konzentrationsfähigkeit.
Hieraus folgt, daß MPU-Gutachten von Antragstellern ab dem fünfzigsten Lebensjahr nur bei Vorliegen *besonderer* Tatsachen, die Zweifel an der Eignung des Antragstellers begründen, verlangt werden dürfen.

Die Fahrerlaubnisbehörde hat mir zugesichert, die Rechtslage künftig zu beachten. Eine Stellungnahme des SMWA liegt mir noch nicht vor.

9.1.3 Kontrolle einer Führerscheinstelle / Kfz-Zulassungsstelle

Die Kontrolle einer Führerscheinstelle/Kfz-Zulassungsstelle ergab, daß die Datenverarbeitung überwiegend den gesetzlichen Vorschriften entsprach.

Zu beanstanden war lediglich, daß in der Führerscheinkartei teilweise das Personenkennzeichen der Fahrerlaubnisinhaber vermerkt war (nach dem Einigungsvertrag ist das Personenkennzeichen in Dateien zum frühestmöglichen Zeitpunkt zu löschen) und daß Halteranfragen beantwortet wurden, obwohl die Auskunftsbegehrenden keine konkreten Gründe hierfür dargelegt hatten (vgl. § 39 Abs. 1 StVG und Nr. 9.1.3 des 3. Tätigkeitsberichts).

Der Behördenleiter hat mir inzwischen mitgeteilt, daß die datenschutzrechtlichen Mängel behoben sind.

9.1.4 Inhalt einer Fahrtenbuchauflage

In einem Bußgeldverfahren wegen Geschwindigkeitsüberschreitung im Straßenverkehr ordnete die Bußgeldbehörde gegenüber dem Halter (der energisch bestritt, an dem fraglichen Tag selbst gefahren zu sein) das Führen eines Fahrtenbuches an. Neben den Daten
- Anschrift, Name und Vorname des Fahrzeugführers,
- amtliches Kennzeichen des Fahrzeugs sowie
- Datum und Uhrzeit des Fahrtbeginns und der Fahrtbeendigung

sollten zusätzlich die jeweiligen Abfahrts- und Zielorte eingetragen werden.

Ich habe die Behörde darauf hingewiesen, daß die Auflage rechtswidrig ist, soweit sie die Verpflichtung enthält, die Abfahrts- und Zielorte anzugeben.

Die Vorschrift des § 31 a Abs. 2 StVZO bestimmt nämlich *abschließend*, welche Daten in das Fahrtenbuch aufgenommen werden dürfen. "Abfahrts- und Zielorte" sind nicht erwähnt.
Abgesehen davon ist die Kenntnis dieser Daten für die Behörde auch nicht *erforderlich*. Die Anordnung zum Führen eines Fahrtenbuchs dient dazu, den verantwortlichen Fahrzeugführer etwaiger künftiger Verkehrsverstöße identifizieren zu können (vgl. BVerwG NJW 1989, 2704). Dies läßt sich mit den in § 31 a Abs. 2 StVZO vorgesehenen Eintragungen bereits erreichen.

Die Behörde hat die rechtswidrige Auflage zurückgenommen.

9.1.5 Weitergabe von Beschäftigtendaten durch eine Polizeidienststelle an eine Fahrerlaubnisbehörde

Ein Beschäftigter im polizeilichen Vollzugsdienst berichtete mir, daß sein Vorgesetzter die örtliche Führerscheinstelle über die Entziehung seiner dienstlichen Fahrerlaubnis sowie die Gründe dieser Maßnahme unterrichtet habe.

Ich habe dem Petenten mitgeteilt, daß diese Datenübermittlung von § 14 Abs. 4 Satz 2 StVZO gedeckt und daher zulässig sei. Nach dieser Vorschrift müssen die Polizeidienststellen die Fahrerlaubnisbehörden über eine erfolgte Entziehung einer Sonderfahrerlaubnis einschließlich der entscheidungserheblichen Gründe informieren, damit diese die *allgemeine* Fahreignung der Betroffenen überprüfen können. Die Übermittlung der Gründe ist nur dann unzulässig, wenn sich hieraus offensichtlich keine Zweifel an der allgemeinen Fahreignung ergeben.

9.1.6 Welche Daten dürfen Fahrerlaubnisbehörden im Rahmen der Eignungsprüfung bei Neuerteilung einer Fahrerlaubnis verarbeiten?

Eine Fahrerlaubnisbehörde verlangte im Rahmen der Eignungsprüfung bei Neuerteilung einer Fahrerlaubnis von allen Antragstellern Angaben zu strafrechtlichen Ermittlungsverfahren und zum Gesundheitszustand (z. B. "Sind bei Ihnen Beine/Rumpf gelähmt?"). Diese Datenerhebungen waren rechtswidrig, weil der Gesetzgeber die Datenverarbeitung im Verfahren zur Eignungsprüfung von Fahrerlaubnisbewerbern in der Straßenverkehrszulassungsordnung und im Straßenverkehrsgesetz *abschließend* geregelt hat und die o. g. Datenerhebungen dort nicht vorgesehen sind.
Nach den straßenverkehrsrechtlichen Vorschriften ist es zur Prüfung, ob Antragsteller strafrechtlich in Erscheinung getreten sind, nur zulässig, auf das Verkehrszentralregister zuzugreifen oder ein Führungszeugnis zu verlangen.
An gesundheitsrelevanten Daten dürfen die Fahrerlaubnisbehörden lediglich eine Sehtestbescheinigung und unter den *engen* Voraussetzungen des § 12 Satz 1 StVZO *im Einzelfall* ein in der Vorschrift näher bezeichnetes Gutachten fordern.
Das von mir unterrichtete Regierungspräsidium (Kommunalaufsicht) hat die Verwendung des Antragsformulars sofort unterbunden und die Löschung der aufgrund des Formulars erhobenen Daten verlangt. Ob die Löschung tatsächlich erfolgt ist, werde ich überprüfen.

9.2 Gewerberecht

9.2.1 Rechtliche Entwicklung

9.2.1.1 Gesetz zur Änderung der Gewerbeordnung und sonstiger gewerberechtlicher Vorschriften

Mit dem Bundesgesetz zur Änderung der Gewerbeordnung (GewO) und sonstiger gewerberechtlicher Vorschriften wurde mit Wirkung teils ab Februar, teils ab Dezember 1995 die Datenverarbeitung im gewerberechtlichen Verfahren endlich auf bereichsspezifische Grundlagen gestellt.

Die Vorschrift des § 11 regelt ausführlich insbesondere das Erheben und Nutzen personenbezogener Daten der Gewerbetreibenden durch Behörden. Berücksichtigt werden der Grundsatz der Datenerhebung beim Betroffenen und das Gebot, erhobene personenbezogene Daten nur zweckgebunden weiterzuverarbeiten.

In § 14 werden u. a. die Datenübermittlungen aus den Gewerbeanzeigen geregelt. Nach Abs. 8 ist die Übermittlung von Name, betrieblicher Anschrift und angezeigter Tätigkeit der Gewerbetreibenden an nicht-öffentliche Stellen nur zulässig, wenn der Auskunftsbegehrende ein *berechtigtes* Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft macht. Weitere Daten (erweiterte Auskunft) dürfen nur übermittelt werden, wenn er ein *rechtliches* Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft macht *und* kein Grund zu der Annahme besteht, daß das *schutzwürdige Interesse* des Gewerbetreibenden überwiegt.

Als datenschutzrechtliches Defizit ist es zu werten, daß der Betroffene vor der erweiterten Auskunft nicht anzuhören und nach erteilter Auskunft nicht zu unterrichten (etwa wie § 15 Abs. 3 SächsDSG es vorsieht) ist. Nach meiner Auffassung kann die Frage, ob schutzwürdige Interessen einer Auskunftserteilung entgegenstehen, nur nach Anhörung des Gewerbetreibenden ausreichend beantwortet werden. Außerdem hätte ich es begrüßt, wenn an die Zulässigkeit von *Gruppenauskünften* (das sind Auskünfte über eine Vielzahl namentlich nicht bestimmter Gewerbetreibender) besondere Anforderungen gestellt worden wären.

9.2.1.2 Verwaltungsvorschrift zur Durchführung der §§ 14, 15 und 55 c GewO

Die Änderung der Gewerbeordnung hatte zur Folge, daß das SMWA eine neue Verwaltungsvorschrift zur Durchführung der §§ 14, 15 und 55 c GewO erlassen hat. Bei meiner Stellungnahme zu dem Entwurf dieser Verwaltungsvorschrift habe ich angeregt klarzustellen, daß Führungszeugnisse im Rahmen der Zuverlässigkeitsprüfung nach § 31 BZRG grundsätzlich beim Betroffenen anzufordern sind. Außerdem habe ich angeregt, den in der Praxis zu Auslegungsschwierigkeiten führenden Begriff "rechtliches Interesse" (vgl. § 14 Abs. 8 GewO) in der Verwaltungsvorschrift wie folgt

zu definieren: "Ein rechtliches Interesse liegt z. B. vor, wenn der Auskunftssuchende die Daten des Gewerbetreibenden zur Geltendmachung von Rechtsansprüchen (z.B. vollstreckbarer Titel) benötigt."

Das SMWA hat meine Anregungen in die Verwaltungsvorschrift eingearbeitet.

9.2.2 Einholung unbeschränkter Auskünfte aus dem Bundeszentralregister über Beschäftigte bei einem Bewachungsunternehmen

Bei Beschäftigten in privaten Bewachungsunternehmen sind an die Zuverlässigkeitsprüfung strenge Anforderungen zu stellen. Daher erhalten die Gewerbeämter nach § 41 Abs. 1 Nr. 9 BZRG eine *unbeschränkte* Auskunft aus dem Bundeszentralregister für die Überprüfung des Überwachungspersonals. Ergibt sich aus der Auskunft, daß eine Wachperson unzuverlässig ist und daher nicht weiterbeschäftigt werden darf, teilen die Gewerbeämter dies in zu begründenden Auflagebescheiden den Bewachungsunternehmen mit. Auf diese Weise erlangt der Wachunternehmer z. B. Kenntnis darüber, daß der betroffene Mitarbeiter einschlägig vorbestraft ist.

Einige Landesdatenschutzbeauftragte vertreten die Auffassung, diese Datenübermittlungen seien wegen Fehlens einer Übermittlungsbefugnisnorm unzulässig. Dem vermag ich aus folgenden Gründen nicht zu folgen:

Der o. g. Auflagenbescheid ist ein Verwaltungsakt, der nach § 39 Abs. 1 VwVfG zu begründen ist. Gemäß § 39 Abs. 1 Satz 2 VwVfG umfaßt diese Begründung alle *wesentlichen* tatsächlichen und rechtlichen *Gründe* für die Entscheidung. Das Bundesverfassungsgericht (BVerfGE 6, 44) hat stets betont, daß die Begründung von belastenden Verwaltungsakten sehr ausführlich sein muß, damit der Empfänger die Erfolgsaussichten eines möglichen Widerspruchs abschätzen kann. Nur in diesem Fall sei er in der Lage, den durch Art. 19 Abs. 4 GG effektiv gewährleisteten Rechtsschutz wirksam zu erlangen.

Basiert die Annahme der Unzuverlässigkeit eines Beschäftigten bei einem Bewachungsunternehmen auf Eintragungen nach § 41 BZRG, *muß* dies daher dem Wachunternehmer mitgeteilt werden. Die Befugnis zum Eingriff in das Recht auf informationelle Selbstbestimmung des Betroffenen ergibt sich hier also unmittelbar aus § 39 Abs. 1 VwVfG.

Ich rege an, daß öffentliche Stellen, die private Wachgesellschaften beschäftigen, sich vertraglich das Recht sichern, über die (anonymen) Ergebnisse der Zuverlässigkeitsprüfung informiert zu werden.

9.2.3 Gewerberegisterauskunft über ausländische Gewerbetreibende

Die Frage eines Gewerbeamts, ob es einem "gemeinnützigen Verein" zur Förderung ausländischer Gewerbetreibender auf Anfrage Name, Anschrift und Tätigkeit sämtlicher *ausländischer* Gewerbetreibender aus dem Gewerberegister übermitteln darf, mußte ich verneinen. Zwar sind gemäß § 14 Abs. 8 GewO (bei Vorliegen eines berechtigten Interesses) einfache Gruppenauskünfte aus dem Gewerberegister über die Grunddaten "Name, betriebliche Anschrift und angezeigte Tätigkeit" der Gewerbetreibenden zulässig; wählt jedoch das Gewerbeamt die *Ausländereigenschaft* der Gewerbetreibenden als Auswahlkriterium für den zu bestimmenden Personenkreis, wird dieses personenbezogene Datum "zwangsläufig" (und entgegen § 14 Abs. 8 GewO) mitübermittelt.

9.2.4 Zum Begriff "Glaubhaftmachen"

Bei der Kontrolle einer Stadtverwaltung habe ich festgestellt, daß im Gewerbeamt Unsicherheiten herrschten, unter welchen Voraussetzungen die Übermittlung personenbezogener Daten aus den Gewerbeanzeigen zulässig ist. Beispielsweise wurde der Name und die betriebliche Anschrift eines Gewerbebetriebs an eine Anwaltskanzlei übermittelt, die lapidar in dem Anforderungsschreiben mitgeteilt hatte: "Das Vorliegen eines berechtigten Interesses wird anwaltlich versichert". So geht es nicht. Diese Datenübermittlung war nicht von § 14 Abs. 8 GewO gedeckt, wonach aus der Gewerbeanzeige an nicht-öffentliche Stellen "Name, betriebliche Anschrift und angezeigte Tätigkeit" des Gewerbetreibenden nur dann übermittelt werden dürfen, wenn der Auskunftsbegehrende ein berechtigtes Interesse an der Kenntnis der Daten *glaubhaft macht.*

"Glaubhaftmachen" bedeutet, daß der Auskunftsbegehrende einen nachprüfbaren *Sachverhalt* schildern muß, der ein berechtigtes Interesse begründet, und zwar für jedes einzelne Datum. Eine "Versicherung" (mag es auch eine "anwaltliche" sein) reicht also keinesfalls aus.

Das Gewerbeamt hat zugesichert, die Rechtslage künftig zu beachten.

9.3 Handwerkskammern, Industrie- und Handelskammern

9.3.1 Einrichtung von "Warndateien" über säumige Schuldnerfirmen

Wiederholt wurde gefragt, ob zentrale "Warndateien" eingerichtet werden dürfen, um die "schwarzen Schafe" unter den Gewerbetreibenden herauszufiltern.

Mit den Staatsministerien des Innern sowie für Wirtschaft und Arbeit stimme ich

überein, daß solche Dateien kaum eine zusätzliche Wettbewerbssicherheit bringen würden, zumal es bereits gut eingeführte Einrichtungen dieser Art gibt.

Im öffentlichen Bereich mangelt es im übrigen an Rechtsgrundlagen, so daß die Errichtung einer "Warndatei" rechtswidrig wäre.

9.3.2 Lebenslauferstellung bei Fortbildungsveranstaltungen

Der Teilnehmer einer beruflichen Fortbildungsveranstaltung berichtete, daß die Kursteilnehmer der Anmeldung zur Prüfung einen (tabellarischen) Lebenslauf beizufügen hätten.

Tatsächlich sehen vom SMWA genehmigte Prüfungsordnungen der Kammern u. a. die Erstellung tabellarischer Lebensläufe als Prüfungsvoraussetzung vor.

Das SMWA hat sich meiner Auffassung angeschlossen, daß Lebensläufe als Prüfungsvoraussetzung nicht erforderlich sind. Es läßt gegenwärtig bei allen sächsischen Kammern sämtliche Prüfungsordnungen im Hinblick auf evtl. verlangte Lebensläufe überprüfen, was nicht zuletzt das Verdienst des kritischen Petenten ist.

9.3.3 Bekanntgabe von Prüfungsergebnissen durch die Kammern an den Ausbildungsbetrieb

Die Frage, ob die zuständigen Stellen (Kammern) den Ausbildungsbetrieben die Ergebnisse, die ihre Auszubildenden in den Prüfungen erzielt haben, mitteilen dürfen, habe ich wie folgt beurteilt:

Nach dem Volkszählungsurteil des Bundesverfassungsgerichts vom 15. Dezember 1983 (NJW 1984, 419 ff.) gewährleistet das aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG als Konkretisierung des allgemeinen Persönlichkeitsrechts abgeleitete Recht auf informationelle Selbstbestimmung die Befugnis des Einzelnen, grundsätzlich selbst über die Erhebung, Verwendung und Weitergabe seiner personenbezogenen Daten zu bestimmen (Art. 33 SächsVerf). Sie dürfen ohne freiwillige und ausdrückliche Zustimmung der berechtigten Person nicht erhoben, gespeichert, verwendet und weitergegeben werden. In dieses Recht darf nur durch Gesetz oder aufgrund eines Gesetzes eingegriffen werden. Eine solche gesetzliche Regelung muß dem Gebot der Normenklarheit entsprechen und verhältnismäßig sein.

§ 45 Abs. 1 Satz 1 BBiG erfüllt diese Voraussetzungen für sich allein genommen nicht. Die Pflicht der Kammern, die Berufsausbildung durch Beratung der Ausbildenden und der Auszubildenden zu fördern, läßt keineswegs den Schluß zu, daß die Übermittlung der Prüfungsergebnisse an die Ausbildenden durch diese nicht normenklare Bestimmung erlaubt oder gar vorgeschrieben sei.

Allerdings verkenne ich nicht, daß eine Mitteilung sowohl über das Bestehen als auch über das Nichtbestehen der Abschlußprüfung im Hinblick auf die Beendigung des Ausbildungsverhältnisses oder die Weiterbeschäftigung bzw. auf die Verlängerung der Ausbildungszeit in der Gesamtschau der §§ 14, 17, 45 BBiG von Bedeutung ist.

Ohne die wünschenswerte Schaffung einer normenklaren Übermittlungsregelung im BBiG selbst (z. B. in § 45) kann jedoch zur Legitimation solcher Datenübermittlungen auf die nach § 41 BBiG zu erlassenden Prüfungsordnungen zurückgegriffen werden (z. B. enthält § 23 Abs. 1 der Prüfungsordnung Nordrhein-Westfalen zumindest eine Regelung bei Nichtbestehen). Eine solche Prüfungsordnung besitzt jedoch m. E. keine Rechtsnormqualität. Deshalb muß auf die §§ 13 und 15 SächsDSG als Auffanggesetz zurückgegriffen werden: Die Übermittlung ist für den Ausbildenden nicht nur zur gänzlichen Erfüllung des Ausbildungsvertrages erforderlich, sondern sie entspricht auch der gesetzlichen Beratungspflicht der Kammern. In der Prüfungsordnung, die jedem Auszubildenden auszuhändigen ist, muß der Hinweis gemäß § 15 Abs. 3 SächsDSG enthalten sein, daß die Übermittlung der nachstehenden Daten erfolgt.

Erforderlich könnten außer Namen, Vornamen und Betriebszugehörigkeit des Auszubildenden sein:
- Bei Nichtbestehen Angaben, in welchen Prüfungsteilen keine ausreichenden Leistungen erbracht worden sind und welche Prüfungsleistungen in einer Wiederholungsprüfung nicht mehr wiederholt zu werden brauchen, um den Ausbildenden in die Lage zu versetzen, bis zur Wiederholungsprüfung gezielt Leistungsdefizite des Auszubildenden zu beseitigen;
- bei bestandener Prüfung nur die Tatsache, daß der Auszubildende bestanden hat (nicht also mit welchen Noten), damit der Ausbildende rechtzeitig erfährt, daß das Ausbildungsverhältnis gemäß § 14 Abs. 1 oder Abs. 2 BBiG beendet ist und er die notwendigen Maßnahmen zu einer eventuellen Weiterbeschäftigung einleiten kann.

Die Übermittlung weiterer Daten dürfte weder mit noch ohne Einwilligung des Auszubildenden mangels Erforderlichkeit erlaubt sein.

Das SMWK hat mir mitgeteilt, daß sich der Bund-Länder-Ausschuß "Berufliche Bildung" in seiner Frühjahrssitzung mit diesem Thema befassen wird.

9.3.4 Verpflichtung zur Vorlage des Arbeitsvertrages zwischen Gewerbetreibendem und Betriebsleiter bei der Handwerkskammer

In einer Eingabe wird durch einen Rechtsanwalt der Datenschutz strapaziert, weil die Handwerkskammer den Arbeitsvertrag zwischen dem Gewerbetreibenden und seinem Betriebsleiter verlangt habe. Es wurde befürchtet, daß "durch Bekanntgabe von Firmendaten ein Wettbewerbsnachteil entsteht".

Dabei wurde übersehen, daß nach § 17 Abs. 1 HwO Gewerbetreibende verpflichtet

sind, der Handwerkskammer u. a. Auskunft über die *vertragliche* und praktische Ausgestaltung des Betriebsleiterverhältnisses zu erteilen. Der Arbeitsvertrag ist ein Indiz dafür, daß kein "Strohmann" als Betriebsleiter eingesetzt wird.

Entgegen dem Vorbringen des Rechtsanwaltes konnte ich mir nicht vorstellen, daß seiner Mandantin durch Vorlage des Arbeitsvertrages Wettbewerbsnachteile entstehen. Die Handwerkskammer ist schließlich als Körperschaft des öffentlichen Rechts (§ 90 Abs. 1 HwO) gemäß Art. 20 Abs. 3 GG, 3 Abs. 3 SächsVerf an gesetzmäßiges Verwaltungshandeln gebunden und wird Firmendaten nicht rechtswidrig bekanntgegeben.

9.4 Offene Vermögensfragen

9.4.1 Bekanntgabe des Investitionsvorrangbescheides

Die Geltung des Investitionsvorranggesetzes wurde bis Ende 1998 verlängert. Verfahren nach diesem Gesetz sind nicht einfach, nicht zuletzt auch deswegen, weil an dem Verwaltungsverfahren neben der entscheidenden Behörde drei Private (oder doch wie Private zu Behandelnde) beteiligt sind. Dies wirft Fragen für den Datenschutz auf, bei denen für die Betroffenen wirtschaftlich Wesentliches auf dem Spiel steht (vgl. schon im 2. Tätigkeitsbericht unter 9.2.2). Enthalten doch die Begründungen von Investitionsvorrangbescheiden (IVBen) notwendigerweise in der Regel Angaben zur Vermögenslage (Finanzierungsplan, namentlich Art und Umfang vorhandener Eigenmittel und konkrete Zusagen bestimmter Kreditgeber) bzw. zur persönlichen geschäftlichen Qualifikation (insbesondere Erfüllung spezieller Zulassungsvoraussetzungen zu bestimmten Berufen, vgl. Kimme-Frantzen Rdnrn. 10 f. zu § 4 InVorG) des Vorhabenträgers oder auch des Anmelders (wenn dieser seinerseits investive Maßnahmen zusagt, indem auch er einen eigenen Vorhabenplan einreicht, vgl. § 5 Abs. 1 bis 3 InVorG). Die Vorhabenpläne können auch die geschäftlichen Daten Dritter enthalten, die der Vorhabenträger oder auch der Anmelder als Vertragspartner (namentlich Mieter oder Pächter) schon an der Hand haben muß, um sein Vorhaben, etwa ein zu vermietendes Gebäude mit Werkstätten, Läden, Büroräumen oder Praxen, betreiben zu können. Denn es ist nach der Rechtsprechung zum Investitionsvorranggesetz zulässig, daß der Vorhabenträger, wie auch der Anmelder, zur Durchführung des Vorhabens und insbesondere zu dessen Finanzierung Dritte einschalten darf. Allerdings hat dies einen 'datenschutzrechtlichen Preis', nämlich den, daß der Vertragspartner des Verfügungsberechtigten (also der Vorhabenträger) oder auch der Anmelder belegen muß, daß der Dritte, der das Vorhaben für ihn ausführen soll, vertraglich zur Durchführung der entsprechenden Maßnahmen verpflichtet ist und daß die Gewähr besteht, daß diese Verpflichtung auch durchsetzbar ist (vgl. Keil-Pée-Scheidmann, Rechtsprobleme und praktische Fragen der Anwendung des Investitionsvorranggesetzes, RWS-Skript 266, 1994 S. 25 f. unter Berufung auf VG Berlin VIZ 1994, 37).

In den Verfahrensakten befinden sich dann ggf. auch die Nachweise, also die konkreten Verträge oder Zusagen der Dritten.

Beteiligte im Verwaltungsverfahren sind der Verfügungsberechtigte i. S. d. Vermögensgesetzes (§ 2 Abs. 3 VermG) als Antragsteller und der Anmelder eines vermögensrechtlichen Anspruches (vgl. § 5 Abs. 1 Satz 1 InVorG 9), beide als notwendige Verfahrensbeteiligte gemäß § 13 Abs. 1 Nr. 1 und 2 VwVfG (der letztere deswegen, weil nach § 9 Abs. 1 InVorG der IVB ihm bekannt zu machen und damit an ihn zu richten ist).

Dabei ist der Verfügungsberechtigte der hauptsächliche Verfahrensbeteiligte, nicht jedoch der Vorhabenträger, also der Investor (vgl. BVerwG, Entscheidung vom 13. Oktober 1994 - 7 C 15.94 -, SächsVBl. 1995, 182; Kimme-Frantzen Rdnr. 6 zu § 4 InVorG). Deswegen muß der gesamte IVB, einschließlich der vollständigen Begründung, dem Verfügungsberechtigten kundgegeben werden, und zwar auch in dem Falle, daß der Verwaltungsakt zu seinen Gunsten ergangen ist. Denn der Verfügungsberechtigte muß als Verfahrensbeteiligter auch Gelegenheit erhalten, sich darauf einzurichten, wenn die Begründung der günstigen Bescheidung des von ihm gestellten Antrages Schwächen aufweist oder wenn sie ihm bis dahin unbekannte Gründe aufführt.

Es besteht die Gefahr, daß die Vertragspartner des Vorhabenträgers oder auch Dritte vom Verfügungsberechtigten mehr über die wirtschaftlichen Verhältnisse des Vorhabenträgers erfahren, als diesem lieb sein kann, etwa mit der Folge, daß die Vertragspartner abspringen bzw. abgeworben werden. Möglicherweise entstehen in solchen Fällen zivilrechtliche Unterlassungs- und Schadensersatzansprüche; datenschutzrechtlich lassen sich Vorkehrungen gegen solche Vorgänge nicht treffen.

Übersendung des IVB an das Belegenheits-ARoV:

§ 9 Abs. 1 Satz 2 InVorG verpflichtet die InVorG-Behörde ausdrücklich, demjenigen ARoV, in dessen Zuständigkeitsbereich das Grundstück bzw. Gebäude belegen ist, eine Abschrift des IVB zukommen zu lassen. Verfassungsrechtlich ist dies nicht ganz frei von Bedenken, weil zur Unterrichtung des ARoV die Übermittlung des Tenors des IVB in aller Regel ausreichen müßte. Eine verfassungskonforme restriktive Auslegung in dem Sinne, daß eine Abschrift nicht des gesamten IVB, sondern nur seines Tenors zu übermitteln wäre (auch im Falle des § 9 Abs. 1 Satz 3 InVorG), dürfte ausscheiden.
Die Beeinträchtigung des Grundrechts auf informationelle Selbstbestimmung, die von einer solchen Übermittlung an das ARoV und ggf. an den Entschädigungsfonds ausgeht, ist gering. Akteneinsicht haben dort der Anmelder und der Verfügungsberechtigte, die ohnehin im Rahmen des InVorG-Verfahrens Kenntnis des IVB zu erhalten haben.

Einer Behörde, die sich insoweit an den klaren Gesetzeswortlaut hält, ist kein Vorwurf

zu machen.

Bekanntgabe des IVB an den Anmelder:
Die Pflicht der InVorG-Behörde, dem durch den positiven IVB belasteten Anmelder (eines Rückübertragungsanspruches) den Bescheid zukommen zu lassen, ergibt sich aus § 41 Abs. 1 Satz 1 VwVfG. Aufgrund des Anspruches auf rechtliches Gehör hat der Anmelder auch einen Anspruch darauf, daß das geschieht.

Es handelt sich um Daten mit Doppel- bzw. mit Mehrfachbezug. Im Rahmen rechtsstaatlicher Verfahren müssen diese grundsätzlich allen Verfahrensbeteiligten zur Verfügung stehen. Die Rechtsstaatlichkeit des Verfahrens verbietet es, daß die betreffenden Daten ausschließlich der entscheidenden Behörde oder dem entscheidenden Gericht zur Verfügung stehen. Es handelt sich um dieselbe Problematik wie bei der beamtenrechtlichen Konkurrentenklage oder beim Nachweis der richtigen Sozialauswahl im Kündigungsschutzverfahren vor den Arbeitsgerichten.

9.4.2 Anspruch auf Auskunft über Verträge, mit denen Kommunen Immobilien aus Volkseigentum veräußert haben

Jemand, der einen Anspruch auf Rückübertragung eines Grundstückes nach dem Vermögensgesetz gestellt hatte, wandte sich an mich, weil eine Stadtverwaltung unter - wie in solchen Fällen üblich pauschaler - Berufung auf den Datenschutz sich geweigert hatte, ihm den Text der Verträge zur Verfügung zu stellen, mittels deren städtische Stellen aus Volkseigentum das Haus und dann 1990 auch das Grundstück an den Verfügungsberechtigten (derzeitigen Eigentümer) veräußert hatten. Nur dem ARoV, so hatte die Stadt erklärt, werde sie auf Antrag (!) im Wege der Amtshilfe (!) die Verträge vorlegen.

Die Stadt hatte den Datenschutz anscheinend nur vorgeschoben. Sofern die Stadt darauf spekuliert haben sollte, daß das ARoV unter Verstoß gegen den Amtsermittlungsgrundsatz (§ 31 Abs. 1 Satz 1 VermG) es unterlassen würde, die Verträge im Hinblick auf die Frage des redlichen Erwerbes gemäß § 4 Abs. 2 Satz 1 VermG beizuziehen, hatte sie sich nicht verrechnet. (Der Verdacht läßt sich nicht ganz unterdrücken: Eine Entscheidung zu Lasten des Entschädigungsfonds, also des Bundes, fällt leichter als eine Entscheidung zu Lasten einer Gemeinde, die dem Landkreis angehört, der Träger des betreffenden ARoV ist.)

Die Stadt war sehr wohl verpflichtet, die Vertragstexte 'herauszurücken'. Der Antragsteller hatte nämlich einen nur durch Überlassung des Textes der Verträge zu erfüllenden Auskunftsanspruch nach Archivrecht (§ 6 Abs. 3 SächsArchG), ersatzweise den allgemeinen Auskunftsanspruch nach § 17 Abs. 1 SächsDSG.

Denn das Auskunftsersuchen war von einer Person gestellt, welche einen Rückübertragungsanspruch nach dem Vermögensgesetz geltend gemacht hatte (vgl. §

30 Abs. 1 Satz 1 VermG). Zur Begründung dieses Anspruches machte sie geltend, die Verträge, in die sie Einsicht begehrte, könnten Aufschluß darüber geben, ob der Erwerber ("Verfügungsberechtigter" im Sinne von § 2 Abs. 3 VermG) die Einwendung des redlichen Erwerbes gemäß § 4 Abs. 2 VermG geltend machen könne. Somit kann sich der Antragsteller darauf berufen, daß die Vertragsunterlagen Daten darstellen, welche sich auch auf seine Person beziehen.

Die Verträge, mit welchen die Stadt als Rechtsträger des Volkseigentums Grundstücksrechte an Private veräußert hat, haben nämlich einen - wenn auch gewissermaßen latenten - Bezug auf die Person des Antragstellers. Dieser Bezug wird dadurch hergestellt, daß der Antragsteller möglicherweise einen Rechtsanspruch auf Übertragung des Grundstückes (Hauses) hat, auf welches sich die Verträge beziehen; wobei sogar noch hinzukommt, daß der Inhalt der Unterlagen, in die Einsicht verlangt wird, den entscheidenden Aufschluß darüber geben kann, ob der Anspruch besteht oder ob ihm die Einwendung des redlichen Erwerbes gemäß § 4 Abs. 2 Satz 1 VermG entgegensteht.
Im übrigen zeigt auch § 2 Abs. 3 SächsArchG mit der Erwähnung des "Dritten", daß das Archivrecht auch die Belange nicht in den Unterlagen namentlich genannter Personen zu berücksichtigen hat.

Sofern für die Vertragsunterlagen noch nicht sämtliche Vorraussetzungen einer Anwendbarkeit des Sächsischen Archivgesetzes (vgl. dazu meinen 3. Tätigkeitsbericht unter 5.8.2) erfüllt waren, war das Einsichtsbegehren durch den nach § 17 Abs. 1 SächsDSG bestehenden allgemeinen datenschutzrechtlichen Auskunftsanspruch begründet: Der Bezug des Inhaltes der Vertragsunterlagen auf die Person des Antragstellers ergibt sich aus den vorstehend zu § 6 Abs. 3 SächsArchG genannten Gründen durch das Vermögensgesetz.

Zugleich enthalten die von der Stadt verwahrten Unterlagen freilich Daten Dritter, vor allem solche der privaten Vertragspartner, die seinerzeit die Grundstücksrechte erworben haben. Es sind Daten mit *Mehrfachbezug*.

Daraus ergibt sich jedoch keine Pflicht und kein Recht der Stadt, dem Antragsteller die Einsicht in diese Unterlagen vorzuenthalten. Denn das Interesse der Erwerber bzw. des Verfügungsberechtigten im Sinne des Vermögensgesetzes überwiegt keineswegs das Interesse der Antragsteller nach dem Vermögensgesetz; nur in solchen Fällen ist ja bei Daten mit Mehrfachbezug der Auskunftsanspruch ausgeschlossen (vgl. § 17 Abs. 5 SächsDSG; § 19 Abs. 4 Nr. 3 BDSG). Daß die Interessen so zu werten sind, läßt sich wiederum dem Vermögensgesetz entnehmen, welches die Prüfung der Voraussetzungen des Bestehens eines Rückübertragungsanspruches und die Ermittlung des diesbezüglichen Sachverhaltes zur Pflicht der Vermögensämter macht (§ 31 Abs. 1 Satz 1 VermG) und damit die Unterlagen einem uneingeschränkten Akteneinsichtsrecht des Antragstellers unterwirft (§ 31 Abs. 3 Satz 1 VermG), sofern dieser seinen Anspruch glaubhaft macht (§ 31 Abs. 3 Satz 2 VermG).
Im Falle des Antragstellers lag inzwischen ein Bescheid des ARoV vor, wonach die

Anspruchsgrundlage des § 1 Abs. 2 VermG erfüllt war, der Vermögenswert also einer Maßnahme im Sinne des § 1 VermG unterlegen hatte (vgl. § 3 Abs. 1 Satz 1 VermG).

Der Antragsteller konnte auch nicht etwa auf eine durch das Vermögensamt vermittelte Akteneinsicht verwiesen werden. Die Bearbeitung der vermögensrechtlichen Ansprüche zieht sich in den verschiedenen Verwaltungs- und gerichtlichen Instanzen hin. Vielfach sind Anträge in den Vermögensämtern noch nicht einmal 'angearbeitet' oder hat es die untere Verwaltungsinstanz unterlassen, zur Amtsermittlung die Unterlagen beizuziehen. Es ist daher im Bereich des Vermögensrechtes in ganz besonderem Maße geboten, dem Rechtsuchenden es durch möglichst frühzeitige Akteneinsicht zu ermöglichen, in einem frühzeitigen Verfahrensstadium seine Erfolgsaussichten - ggf. mit Hilfe eines zur Rechtsberatung Berufenen - zu beurteilen und sich entsprechend zu verhalten.

Ein Mißbrauch des Datenschutz-Gedankens, wie er im vorliegenden Fall der Stadtverwaltung vorzuwerfen war, ist geeignet, den Schutz des Grundrechts auf informationelle Selbstbestimmung gemäß Art. 33, 57 SächsVerf in Mißkredit zu bringen und damit zu beeinträchtigen.

9.4.3 Datenübermittlung von den Vermögensämtern an Notare für das Vermittlungsverfahren nach dem Sachenrechtsbereinigungsgesetz?

Das Sachenrechtsbereinigungsgesetz soll langfristig dafür sorgen, daß im Beitrittsgebiet das Eigentum an Grund und Boden und an dem auf dem Grundstück stehenden Gebäude zusammengeführt wird (und auch für andere Fälle der Aufspaltung grundstücksbezogener Rechte die Überführung in einem dem Sachenrecht des BGB entsprechenden Rechtszustand ermöglichen).
Vor eine gerichtliche Auseinandersetzung der Beteiligten hat das Gesetz ein obligatorisches Vermittlungsverfahren geschaltet, das vor einem Notar durchzuführen ist. Es soll schon vor einer Inanspruchnahme der Gerichte eine Einigung zwischen den Beteiligten herbeiführen (§§ 87 ff. SachenRBerG).

Unterstützt von einer Ausarbeitung der Notarkammer Sachsen machten Notare gegenüber sächsischen Vermögensämtern geltend, sie hätten gemäß § 91 Satz 1 SachenRBerG einen Auskunftsanspruch, der die Behörde verpflichte, ihnen bezogen auf Grundstücke, für die sie das Vermittlungsverfahren durchführen, die Namen und Anschriften derjenigen bekanntzugeben, die einen Rückübertragungsantrag gestellt haben.

Bei systematischer und verfassungskonformer, nämlich auf den Grundsatz der Erforderlichkeit der Datenverarbeitung abstellender Auslegung der Vorschriften über das notarielle Vermittlungsverfahren ergibt sich, daß dem betreibenden Notar über das Datum des Ob einer Anmeldung (§ 91 Satz 2 SachenRBerG) hinaus eine Befugnis, das Datum der Person des Anspruchmelders bei dem Vermögensamt zu erheben, nicht

eingeräumt wird. Genausowenig schreibt das SachenRBerG dem Vermögensamt eine diesbezügliche Datenübermittlung an den Notar vor. (Die Einzelheiten der Begründung müßten an dieser Stelle zu weit führen.)

Hinzu kommt: Schon die Anwendung des Adreßmittlungsverfahrens macht die begehrte Datenübermittlung entbehrlich. Der Notar kann (im Hinblick auf § 92 Abs. 3 SachenRBerG) denjenigen, der einen Rückübertragungsanspruch auf das Grundstück angemeldet hat, dadurch unterrichten, daß er die Mitteilung über den von ihm anberaumten Termin dem Vermögensamt übersendet mit der Bitte um Weiterleitung an einen der Behörde ggf. bekannten Anmelder (Amtshilfe). Darüber hinaus könnte in den meisten Fällen die Adreßmittlung sogar der Eigentümer (=Verfügungsberechtigte im Sinne des Vermögensgesetzes) leisten; denn gemäß § 31 Abs. 1 Satz 2 VermG muß der Eigentümer/Verfügungsberechtigte ohnehin über die Person (Name, Anschrift) des Anspruchsanmelders unterrichtet sein. Er muß diese Angaben ohne weiteres vom Vermögensamt auf Anfrage erhalten. (Allerdings läßt der Bearbeitungszustand vieler vermögensrechtlicher Verfahren, so jedenfalls der Stand in Sachsen Januar 1996, eine solche Auskunft noch nicht zu.) Selbstverständlich ist der Eigentümer (Verfügungsberechtigte) auch nicht gehindert, die ihm bekanntgegebenen Angaben dem Notar weiterzugeben, so daß dieser unmittelbar den Anmelder anschreiben kann.

Schreibt der Notar im Wege des Adreßmittlungsverfahrens den Anspruchsanmelder gemäß § 92 Abs. 3 SachenRBerG an, so hat er den Adressaten in einer § 4 Abs. 2 und 3 SächsDSG entsprechenden Form darauf hinzuweisen, daß dieser in keiner Weise verpflichtet ist, dem Notar das Schreiben zu beantworten.

Was eine Anwendung des Adreßmittlungsverfahrens durch das vom Notar angegangene Vermögensamt betrifft, ist keineswegs gesichert, daß dieses insoweit zur Amtshilfe verpflichtet ist. Die Vermögensämter dürfen den Notar darauf verweisen, daß die Amtshilfe (Adreßmittlungsverfahren) nicht erforderlich sei, weil dem Notar, oder besser gesagt den Parteien des vor ihm betriebenen Vermittlungsverfahrens, die Möglichkeit der Adreßmittlung durch den Eigentümer (Verfügungsberechtigten; im Falle des § 16 Abs. 3 VermG auch den Nutzer) selbst zur Verfügung steht.

Für den Fall, daß die Vermögensämter sich als Adreßmittler zur Verfügung stellen, ist dem von ihnen weitergeleiteten Schreiben des Notars ein Begleitschreiben hinzuzufügen, aus dem für den Adressaten deutlich hervorgeht, daß dieser zum Adressaten des Notar-Schreibens geworden ist, ohne daß das Vermögensamt dem Notar Daten übermittelt hat. Zusätzlich sollte das Vermögensamt sich von dem Notar im vorhinein amtlich versichern lassen, daß dieser den genannten Hinweis auf die Freiwilligkeit der Beantwortung in sein Schreiben aufgenommen hat, und das Amt sollte in sein Begleitschreiben die Mitteilung aufnehmen, daß das Schreiben des Notars diesen Hinweis enthalte.

Das LARoV Sachsen habe ich, soweit mir bekannt, von der Richtigkeit dieses Standpunktes überzeugt. Eine Antwort der Notarkammer Sachsen ist mir nicht bekannt.

9.5 Sonstiges

Planfeststellung: Auslegung von Planungsunterlagen

Nicht nur in Sachsen wird bei der Planveröffentlichung gemäß § 73 Abs. 3 VwVfG auch ein Grundstücksverzeichnis mit Namen, Vornamen und Anschrift der aus dem Plan ersichtlichen Grundstückseigentümer ausgelegt.

Ich habe dem SMWA mitgeteilt, daß ich diese Verhaltensweise für rechtswidrig halte.

Nach § 4 Abs. 1 Nr. 1 SächsDSG dürfen personenbezogene Daten ohne Einwilligung des Betroffenen nur verarbeitet (hier übermittelt, vgl. § 3 Abs.1 Nr. 5 Buchst. b SächsDSG) werden, wenn das Sächsische Datenschutzgesetz oder eine andere Rechtsvorschrift dies erlaubt. Diese Voraussetzung ist nicht erfüllt:

1. Das Auslegen der personenbezogenen Verzeichnisse ist nicht durch § 73 Abs. 3 VwVfG gerechtfertigt. Die Vorschrift muß nämlich unter Beachtung des *Grundsatzes der Verhältnismäßigkeit* so interpretiert werden, daß nur die für die Betroffenen *erforderlichen* Planunterlagen zur Einsicht bereit gehalten werden. Die Planauslegung dient den durch das geplante Vorhaben (potentiell) Betroffenen zur Prüfung, ob sie im Anhörungsverfahren erfolgreich Einwendungen erheben können. Hierzu brauchen Sie die Eigentumsverhältnisse an sämtlichen Grundstücken nicht zu kennen.
2. Auch § 15 SächsDSG kommt als mögliche Befugnisnorm für die Auslegung der Grundstücksverzeichnisse nicht in Betracht. Weder ist die Datenübermittlung zur Aufgabenerfüllung der Kommune erforderlich noch ist ein berechtigtes Interesse der Bürger an der Kenntnisnahme der Eigentümerdaten ersichtlich.

Dieses Ergebnis wird durch eine Entscheidung des Bundesverfassungsgerichts (Beschl. vom 24. Juli 1990 - 1 BvR 1244/87, NVwZ 1990, 1162) gestützt.

Das SMWA teilt meine Auffassung und hat die Planfeststellungsbehörden angewiesen, künftig auf die Grundstückseigentümerdaten in den Grundstücksverzeichnissen zu verzichten.

10 Soziales und Gesundheit

10.1. Gesundheitswesen

10.1.1 Sächsisches Ausführungsgesetz zum Krebsregistergesetz des Bundes

Das SMS hat mich im Berichtszeitraum ständig an der Erarbeitung des Entwurfes eines Sächsischen Ausführungsgesetzes zum Krebsregistergesetz des Bundes beteiligt. Mit der Vorlage des Gesetzentwurfs im Kabinett und im Landtag ist in absehbarer Zeit zu rechnen. Der Entwurf enthält, wie von mir in Übereinstimmung mit dem SMS seit langem gefordert (vgl. zuletzt in meinem 3. Tätigkeitsbericht unter 10.1.2), Regelungen über eine widerspruchsunabhängige Meldepflicht der Ärzte. Angesichts der teilweise dagegen erhobenen pauschalen Vorbehalte (vgl. Stellungnahme der Staatsregierung zum 3. Tätigkeitsbericht, S. 24 f.) muß ich mich wiederholen:

Belehrungen über Zustimmungs- und Widerspruchsrechte stören die vertrauliche Sphäre zwischen Arzt und Patient, die tunlich frei von staatlichem Einfluß bleiben muß. Denn ob und wie weit der Arzt seinen Patienten aufklärt, muß zum Schutz der Persönlichkeit des Patienten der ärztlich zu verantwortenden Entscheidung überlassen bleiben. Keinesfalls dürfen Unterrichtungspflichten über Widerspruchsrechte diese Entscheidung beeinflussen. Datenschutz ist nicht der einzige Inhalt des Schutzes des Persönlichkeitsrechts! Es ist nicht verantwortbar, einen Patienten, der Krebs hat und der die Mitteilung darüber nach ärztlichem Urteil nicht verkraften kann, nur deshalb aufzuklären, weil die Meldung an die Vertrauensstelle eine (vorherige oder nachträgliche) Aufklärung voraussetzt.

Die Daten eines Krebsregisters sind nur dann für eine epidemiologische Auswertung geeignet, wenn sie einen hohen Vollständigkeitsgrad erreichen. Weltweit halten die führenden Wissenschaftler nur eine Meldequote von mindestens 95 % für wissenschaftlich tragfähig. Zustimmungs- und Widerspruchsrechte der Patienten stellen daher die Eignung des Registers insgesamt in Frage. Ein Widerspruchsrecht ist nicht akzeptabel, weil damit zu rechnen ist, daß es so häufig ausgeübt wird, daß das Krebsregister seine wissenschaftliche Eignung verliert. Die Einrichtung der von der Registerstelle getrennten ärztlich geleiteten Vertrauensstelle kompensiert den Eingriff in die informationelle Selbstbestimmung; ein Eingriff ist überdies in bezug auf die Registerstelle nicht ersichtlich, weil die Daten dort nur anonymisiert vorliegen. Jeder spätere wissenschaftliche Umgang mit Klardaten wird von der verantwortlichen Einwilligung des Patienten getragen.

Die vom Normprüfungsausschuß geäußerte Kritik, wonach eine widerspruchsunabhängige Meldepflicht unverhältnismäßig sei, halte ich daher für nicht stichhaltig. Eine solche Regelung entspricht auch herkömmlichen, ebenfalls widerspruchsunabhängigen Meldepflichten, wie sie in §§ 12, 13 GeschlKrG, §§ 3 f.

BSeuchG oder § 5 Berufskrankheiten-Verordnung vom 20. Juni 1968 (BGBl. I S. 721) begründet werden.
Genausowenig kann der Einwand überzeugen, die widerspruchsunabhängige Meldepflicht verstoße gegen maßgebliche Vorgaben des KRG des Bundes. Denn dieser hat mit § 13 Abs. 5 Nr. 1 KRG von seinem Modell (widerspruchsabhängiges Melderecht des Arztes) abweichende landesrechtliche Bestimmungen ausdrücklich zugelassen, nicht anders als in der Vorgängerregelung des § 6 Abs. 5 des Krebsregistersicherungsgesetzes vom 21. Dezember 1992 (BGBl. I S. 2335), in dessen Ausführungen das Sächsische Krebsregistergesetz vom 19. Juli 1993 (SächsGVBl. S. 589) für den Freistaat eine widerspruchsunabhängige Meldepflicht eingeführt hat, deren Beibehaltung bei Ausarbeitung des KRG nach dem Willen der Beteiligten möglich bleiben sollte.

Ohne die widerspruchsunabhängige Meldepflicht könnte ich den Gesetzentwurf nicht mittragen, weil ich sonst mitursächlich für ein wissenschaftlich ungeeignetes Register würde.

10.1.2 Meldeordnung der Sächsischen Landesapothekerkammer

Gemäß § 3 Abs. 2 des Sächsischen Heilberufekammergesetzes kann die Landesapothekerkammer in einer Meldeordnung das Nähere über das Meldeverfahren regeln und die zur Überwachung der Berufspflichten erforderlichen Angaben und Nachweise, die Gegenstand der Meldung seien sollen, festlegen. Der Umfang der Meldepflicht wird also beschränkt durch die gesetzliche Aufgabe der Landesapothekerkammer, die Einhaltung der Berufspflichten zu überwachen.

Die Meldeordnung der Sächsischen Landesapothekerkammer vom 16. Oktober 1991 beruhte noch auf dem "Gesetz über die Berufsvertretung und die Berufsausübung der Ärzte, Zahnärzte und Apotheker (Kammergesetz)" vom 13. Juli 1990. Eine Angleichung an die neue Rechtslage war also dringend geboten.

Die Landesapothekerkammer hat mich frühzeitig an den Überlegungen zur Novellierung beteiligt.

Schnell wurde Einigkeit erzielt, welche Daten des Apothekers die Landesapothekerkammer benötigt. Unterschiedliche Auffassungen bestanden jedoch zunächst über die in § 2 der früheren und auch im Entwurf der novellierten Meldeordnung vorgesehene Meldung der Mitarbeiter der Apotheke durch den Leiter. Sie erfolgte auf einem bundesweit verwendeten Vordruck des Deutschen Apotheker Verlags. Gemeldet wurden nicht nur Berufsabschluß und Name, Vorname, Geburtsdatum der Mitarbeiter, sondern z. B. auch Staatsangehörigkeit, Familienstand und sogar Zahl der Kinder.

Die Landesapothekerkammer wies zur Begründung auf die Bemühungen der

Sächsischen Staatsregierung hin, alle Lehrstellen in Sachsen zuverlässig zu erfassen. Die Landesapothekerkammer könne sich auf Grund des Vordrucks einen Überblick über die Stellensituation der Apotheken verschaffen, Apotheker gezielt darauf ansprechen, ob sie zur Ausbildung bereit seien, und Lehrstellenbewerber auf freie Stellen hinweisen.

Die Bemühungen um ein möglichst breites und zutreffend registriertes Lehrstellenangebot sind sicherlich zu begrüßen. Fraglich ist jedoch, ob es zu den gesetzlichen Aufgaben der Sächsischen Landesapothekerkammer gehört, etwa gemäß § 5 Abs. 1 Nr. 7 SächsHKaG, als Lehrstellenvermittler tätig zu werden; in diesem Zusammenhang ist auch die Zuständigkeit der Bundesanstalt für Arbeit nach dem Arbeitsförderungsgesetz zu beachten.

Auch wenn man eine solche Aufgabe bejaht, ist festzustellen, daß der Vordruck für diesen Zweck nicht geeignet ist. Fraglich ist bereits, ob Angaben zu den Mitarbeitern und deren Ausbildung sichere Rückschlüsse auf die Ausbildungskapazität einer Apotheke zulassen. Bei der Entscheidung auszubilden, spielen zahlreiche Faktoren eine Rolle, z.B. der Umsatz oder die Arbeitsbelastung des Apothekers. Auf keinen Fall sind jedoch Angaben im vorgesehenen Umfang erforderlich. Die Erhebungsmerkmale "Verheiratet, Anzahl der Kinder, Staatsangehörigkeit" haben keinerlei Bezug zur Einschätzung der Stellensituation, ebenso das Geburtsdatum, der Geburtsname, die bisherige Beschäftigung.

Keine Einwände habe ich, wenn die Apotheker gebeten werden, Ausbildungsplätze an die Landesapothekerkammer zu melden, die solche Angebote weitergibt (vorausgesetzt, die der Landesapothekerkammer zugewiesenen Aufgaben erlauben die Vermittlung und das Arbeitsförderungsgesetz steht nicht entgegen).

Sinnvoll ist darüber hinaus möglicherweise ein gezieltes Ansprechen der Apotheken, die als Ausbildungsstätte in Betracht kommen. Ich habe angeboten, gemeinsam mit der Landesapothekerkammer nach Möglichkeiten zu suchen, wie sie sich die erforderlichen Angaben beschafft.

Als weiteres Argument nannte die Landesapothekerkammer, sie müsse die Möglichkeit haben, zu überprüfen, ob, wie von § 21 Abs. 1 Nr. 2 BBiG gefordert, die Zahl der Auszubildenden in einem angemessenen Verhältnis zur Zahl der beschäftigten Fachkräfte stehe. Zuständig für diese Überwachung ist jedoch nicht die Landesapothekerkammer, sondern gemäß §§ 23, 91 Abs. 2 BBiG das SMS. Es muß die Möglichkeit haben, die erforderlichen Daten zu erheben.

Die Apothekerkammer eines anderen Bundeslandes teilte mir mit, die Bögen seien auch Grundlage für Meldungen an die Bundesvereinigung der Deutschen Apothekerverbände (ABDA), vermutlich für Statistikzwecke. Hier allerdings muß sich die ABDA fragen lassen, worauf sie die Führung einer solchen "Privatstatistik" stützt.

Nach meiner Auffassung darf nach dem Sächsischen Heilberufekammergesetz die Meldeordnung nur vorschreiben, welche Angaben das Mitglied in der Anmeldung zu machen hat. Diese Angaben müssen für die Überwachung der Berufspflichten erforderlich sein (§ 3 Abs. 2 SächsHKAG). Mitteilungspflichten des Apothekers, etwa auf Grund des Berufsbildungsgesetzes, haben keinen Platz in der Meldeordnung, was nichts daran ändert, daß die in der jeweiligen Rechtsvorschrift genannten Übermittlungspflichten zu erfüllen sind.

Meine Einwände gegen den Vordruck bedeuten nicht, daß die Sächsische Landesapothekerkammer keines der in ihm enthaltenen Daten verarbeiten darf. Soweit sich eine Befugnis zur Verarbeitung einzelner Angaben aus einem speziellen Gesetz oder subsidiär aus dem Sächsischen Datenschutzzgesetz ergibt, darf sie diese verwenden. Nicht erforderlich jedoch ist dafür der Vordruck.

Eine Pflicht zur Meldung der Mitarbeiter ist daher nicht in die novellierte Meldeordnung aufgenommen worden.

10.1.3 Datenschutz bei der Sächsischen Landesärztekammer

Ein niedergelassener Arzt bat um Auskunft,
- ob bei der Sächsischen Landesärztekammer personenbezogene Daten dem Datenschutz unterliegen und
- ob die Sächsische Landesärztekammer berechtigt ist, im Zusammenhang mit der Festsetzung des Kammerbeitrags Berufseinnahmen aus ärztlicher Tätigkeit zu erfragen und entsprechende Nachweise zu verlangen.

Die Fragen habe ich wie folgt beantwortet:

Die Sächsische Landesärztekammer ist als Körperschaft des öffentlichen Rechts eine sonstige öffentliche Stelle des Freistaates Sachsen und hat damit bei der Datenverarbeitung die Vorschriften des Heilberufekammergesetzes und des Sächsischen Datenschutzgesetzes zu beachten. Das bedeutet insbesondere, daß die im Zusammenhang mit der Festsetzung des Kammerbeitrags erhobenen und gespeicherten Daten einer strengen Zweckbindung unterliegen und nur unter den strengen Voraussetzungen des Sächsischen Datenschutzgesetzes an Dritte weitergegeben werden dürfen. Zur Gewährleistung der Datensicherheit hat die öffentliche Stelle die in § 9 SächsDSG aufgeführten Maßnahmen zu treffen.

Das Verfahren zur Beitragsfestsetzung ergibt sich aus der *Beitragsordnung der Sächsischen Landesärztekammer*. Diese hat ihre gesetzliche Grundlage in § 14 Abs. 1 und 2 SächsHKaG, das die Kammern berechtigt, zur Erfüllung ihrer Aufgaben von den Mitgliedern Beiträge zu erheben und zur Beitragsfestsetzung Auskünfte und Nachweise zu verlangen. Näheres dürfen sie in einer Beitragsordnung festlegen.

Nach der o. g. Beitragsordnung bemißt sich der Kammerbeitrag nach dem Berufseinkommen aus ärztlicher Tätigkeit. Bei *niedergelassenen* Ärzten ist dies der Bruttoumsatz, ggf. abzüglich gezahlter Gehälter an andere in der Praxis beschäftigte Ärzte. Datenschutzrechtlich bestehen daher keine Bedenken, wenn im Zusammenhang mit der Beitragsfestsetzung eine Bestätigung des Steuerberaters gefordert wird. Da nach der Beitragsordnung auch ein *Auszug* aus dem Steuerbescheid als Nachweis ausreicht, obwohl die steuerlichen Einkünfte aus selbständiger Arbeit wegen der abgesetzten Betriebsausgaben regelmäßig niedriger ausfallen, ist datenschutzrechtlich

dagegen nichts einzuwenden.

10.1.4 Einführung eines automatisierten Datenübermittlungsverfahrens zwischen der Sächsischen Ärzteversorgung und dem Landesamt für Finanzen (LfF)

Angestellte Ärzte, die gemäß § 6 Abs. 1 Nr. 1 SGB VI von der Versicherungspflicht in der gesetzlichen Rentenversicherung befreit sind, haben an die Sächsische Ärzteversorgung einen Beitrag in der Höhe zu entrichten, der ohne diese Befreiung an die gesetzliche Rentenversicherung zu zahlen wäre. Den beim Freistaat beschäftigten Ärzten zahlt das LfF dafür zusammen mit dem Gehalt einen steuerfreien Zuschuß, als Arbeitgeberbeitrag zur Rentenversicherung. Der Monatsbeitrag bemißt sich im Rahmen von Höchst- und Mindestgrenzen nach dem Monatseinkommen und ist vom Arzt am Monatsende an die Ärzteversorgung zu entrichten. Da Bereitschafts-, Nacht-, Not- und Wochenenddienste besonders vergütet werden und nicht jeden Monat im selben Umfang anfallen, erzielen die Ärzte kein gleichbleibendes Monatseinkommen. Dies hat zur Folge, daß auch die an die Ärzteversorgung zu entrichtenden Monatsbeträge schwanken können. Ob eingegangene Zahlungen dem Monatseinkommen entsprechen, wird während des laufenden Kalenderjahres nicht geprüft.

Nach Ablauf eines Kalenderjahres setzt die Ärzteversorgung auf der Grundlage entsprechender Einkommensnachweise den endgültigen Jahresbeitrag fest, erstattet Differenzbeträge oder fordert sie nach. Außerdem erhält der Arzt eine Bescheinigung für das LfF, damit hier die zweckgerichtete Verwendung der Zuschüsse für die Zukunftssicherung geprüft und ggf. eine Nachversteuerung veranlaßt werden kann. Das Verfahren verursacht erheblichen Verwaltungsaufwand.

Ärzteversorgung und LfF strebten deshalb folgende Verfahrensverbesserung an:
Das LfF teilt der Sächsischen Ärzteversorgung in einem automatisierten Verfahren monatlich die Zuschüsse zur Rentenversicherung mit, damit die Ärzteversorgung die entsprechenden Beträge zum Soll stellen, eingehende Zahlungen kontrollieren und Fehlbeträge zeitnah anfordern kann. Außerdem kann die Ärzteversorgung auf Einkommensnachweise für die Jahresfestsetzung verzichten, weil sich bereits aus den vom LfF mitgeteilten Beträgen der festzusetzende Jahresbeitrag ermitteln läßt. Das LfF wiederum kann von der zweckgerichteten Verwendung der gewährten Zuschüsse ausgehen und auf entsprechende Nachweise durch die Ärzte verzichten.

Die Ärzteversorgung ging zutreffend davon aus, daß die Datenerhebung beim LfF nur mit Einwilligung der Ärzte zulässig ist. Um jedoch diejenigen Ärzte zu ermitteln, die ihre Bezüge über das LfF erhalten, sollte dem Verfahren ein Bestandsabgleich zwischen LfF und Ärzteversorgung vorangehen.

Das SMF bat mich um eine datenschutzrechtliche Beurteilung.

Gegen die monatlichen Datenübermittlungen des LfF habe ich keine datenschutzrechtlichen Bedenken erhoben, da sie mit Einwilligung der betroffenen Ärzte erfolgen sollte. Den beabsichtigten Bestandsabgleich habe ich jedoch als unzulässig angesehen. Zwar dienen die mit ihm verbundenen Datenübermittlungen beiden öffentlichen Stellen zur Aufgabenerfüllung, die Daten würden jedoch einer unzulässigen Zweckänderung unterworfen, denn das LfF hat die Daten der Ärzte für Bezügezahlungen, die Ärzteversorgung für Versorgungsangelegenheiten gespeichert. Der Ärzteversorgung bleibt deshalb nur die Möglichkeit, alle Ärzte anzuschreiben, bei denen sie aufgrund eigener Bestandsdaten von einer Beschäftigung im Landesdienst ausgehen kann; ich denke, sie werden die Einwilligung nicht versagen.

10.1.5 Dienstanweisung für den Datenschutz in einem Krankenhaus

Ein städtisches Krankenhaus hat mir den Entwurf seiner "Dienstanweisung für den Datenschutz" zur Stellungnahme vorgelegt. Da in einigen Punkten die datenschutzrechtlichen Anforderungen zu knapp dargestellt und die vorgesehenen Regelungen zur Einsicht des Patienten in seine Krankenakte mit § 33 Abs. 5 Nr. 2 SächsKHG nicht zu vereinbaren waren, habe ich eigene Textvorschläge gemacht.

Nach meinen Feststellungen existieren nur in wenigen Krankenhäusern Dienstanweisungen für den Datenschutz, obwohl gerade dieser Bereich im großen Umfang Zugang zu besonders schutzwürdigen Daten hat. Die Dienstanweisung sollte mindestens folgendes enthalten:

Patientendaten

Patientendaten sind alle Einzelangaben über persönliche oder sachliche Verhältnisse bestimmter oder bestimmbarer Patienten aus dem Bereich der Krankenhäuser. Außer den in Dateien gespeicherten oder in Akten aufgezeichneten Angaben gehören auch die auf andere Weise festgehaltenen Informationen über den Betroffenen zu den Patientendaten (z. B. Röntgenaufnahmen, graphische Aufzeichnungen wie EKG, Blut-, Gewebeproben usw.). Patientendaten sind auch die personenbezogenen Daten von Angehörigen, anderen Bezugspersonen des Patienten sowie sonstiger Dritter, die dem Krankenhaus im Zusammenhang mit der Behandlung bekannt werden.

Im Krankenhaus (zur Übermittlung an Stellen außerhalb des Krankenhauses s. u.) *dürfen Patientendaten nur erhoben, verarbeitet oder sonst genutzt werden, soweit*

- *dies im Rahmen des Behandlungsverhältnisses auf vertraglicher Grundlage erforderlich ist,*

- *dies zur Ausbildung oder Fortbildung erforderlich ist und dieser Zweck nicht in vertretbarer Weise mit anonymisierten Daten erreichbar ist,*
- *eine Rechtsvorschrift es erlaubt oder*
- *der Patient eingewilligt hat.*

Die Erhebung umfaßt jede Form der Informationsgewinnung, also nicht nur die Befragung des Patienten, sondern z. B. auch Untersuchungen, die Fertigung von Röntgen- oder Ultraschallbildern, EKG usw. Verarbeiten ist das Speichern, Verändern, Anonymisieren, Sperren, Löschen von Patientendaten, sonstiges Nutzen jede andere Form der Datenverwendung; für die Definitionen im einzelnen ist § 3 Abs. 2 SächsDSG maßgebend. Erforderlich ist die Erhebung, Verarbeitung und Nutzung nur dann, wenn ohne sie die Aufgaben des Krankenhauses nicht, nicht rechtzeitig oder nicht ordnungsgemäß erfüllt werden können. Es genügt also nicht, daß die Daten nur praktisch und nützlich sind.

Die Einwilligung des Patienten als Ersatz für die sonstigen Erhebungs-, Verarbeitungs- und Nutzungserlaubnisgründe ist die Ausnahme. Sie muß im Rahmen des Behandlungsverhältnisses erforderlich sein und darf nicht zu einer beliebigen Erweiterung der o. g. Zulässigkeitsvoraussetzungen führen. Die Einwilligung bedarf der Schriftform. Der Patient ist über die Bedeutung der Einwilligung sowie über den Zweck der Erhebung und die vorgesehene Verarbeitung der Daten aufzuklären; er ist darauf hinzuweisen, daß ihm wegen einer Verweigerung der Einwilligung keine Nachteile entstehen. Wegen besonderer Umstände kann die Einwilligung auch in anderer Form erteilt werden. Erfolgt sie mündlich, ist dies aufzuzeichnen. Soweit ein Patient rechtlich nicht in der Lage ist, eine aufgeklärte und verantwortliche Einwilligung zu erklären, kann sie nur von Personensorgeberechtigten, gesetzlichen Vertretern oder Betreuern abgegeben werden

Im Notfall dürfen Patientendaten auch ohne ausdrückliche Einwilligung verarbeitet werden, um Gefahren für Leben oder Gesundheit des Patienten abzuwenden.

Übermittlung von Patientendaten

Ohne Einwilligung des Patienten dürfen Patientendaten in den Fällen des § 33 Abs. 3 Nr. 1 bis 8 SächsKHG an Personen oder Stellen außerhalb des Krankenhauses übermittelt werden. Da insoweit eine Befugnis zur Offenbarung des Patientengeheimnisses besteht, liegt kein Verstoß gegen § 203 StGB vor, der die Schweigepflicht des Arztes und des sonstigen medizinischen Personals regelt.

Im einzelnen ist die Übermittlung zulässig
1. zur Erfüllung einer gesetzlich vorgeschriebenen Behandlungs- oder Mitteilungspflicht,
2. bis 7... (Wiedergabe des Gesetzestextes) ...
8. oder wenn sie in einem anderen Gesetz geregelt ist.

In anderen Fällen ist die Übermittlung von Daten nur mit Einwilligung des Patienten zulässig. Das gilt auch für die Übermittlung von Patientendaten nach Abschluß der Behandlung an anderen Fachabteilungen innerhalb des Krankenhauses (§ 33 Abs. 7 SächsKHG).

Forschungsvorhaben

Übermittlung, Verarbeitung und sonstige Nutzung von Patientendaten im Rahmen von Forschungsvorhaben sind in § 34 SächsKHG geregelt.

Ärztliche Schweigepflicht

Die Berufsordnung der Ärzte und § 203 StGB verpflichten Ärzte und ärztliches Hilfspersonal zur Geheimhaltung von Patientendaten über den Tod des Betroffenen hinaus.

Löschung von Patientendaten

Patientendaten sind zu löschen, wenn sie für das Behandlungsverhältnis, für Ausbildungs- und Fortbildungszwecke oder für die Verarbeitung und Nutzung aufgrund besonderer Rechtsvorschriften nicht mehr erforderlich sind und vorgeschriebene Aufbewahrungsfristen abgelaufen sind. Die Löschung darf nur erfolgen, wenn kein Grund zu der Annahme besteht, daß dadurch schutzwürdige Belange des Betroffenen beeinträchtigt werden und wenn das zuständige Archiv die Übernahme abgelehnt hat.
(Anmerkung: Gemäß § 5 SächsArchG haben die Landeskrankenhäuser Patientenunterlagen dem zuständigen staatlichen Archiv anzubieten, für kommunale Krankenhäuser regelt die jeweilige kommunale Archivsatzung die Anbietungspflicht.)

Andere personenbezogene Daten

Die Verarbeitung personenbezogener Daten, die keine Patientendaten sind (z. B. Personaldaten, Daten von Lieferanten, Handwerkern usw.), richtet sich nicht nach dem Sächsischen Krankenhausgesetz. Sie ist zulässig, wenn das Sächsische Datenschutzgesetz oder eine andere Rechtsvorschrift sie erlaubt oder soweit der Betroffene eingewilligt hat.
Wer die Einwilligung einholt, hat den Betroffenen zuvor auf den Zweck der Datenverarbeitung, die Empfänger einer vorgesehenen Datenübermittlung sowie auf sein Recht zur Verweigerung der Einwilligung hinzuweisen. Rechtsnachteile dürfen dem Betroffenen durch die Verweigerung der Einwilligung nicht entstehen.

Einsicht in die Krankenakte

Dem Patienten ist gemäß § 33 Abs. 5 Nr. 2 SächsKHG auf Antrag kostenfrei Einsicht in seine Krankenakte zu gewähren. Die Auskunfts- und Einsichtsansprüche können im Interesse der Gesundheit des Patienten eingeschränkt werden. Die Einschränkung ist unter Bezugnahme auf die Krankheit konkret nach Art und Richtung zu begründen, ohne ins Detail zu gehen.

Durch berechtigte Geheimhaltungsinteressen Dritter wird das Auskunfts- und

Einsichtsrecht eingeschränkt. Der behandelnde Arzt und das Krankenhauspersonal sind im Verhältnis zum Patienten keine Dritten.

Soweit Auskunfts- und Einsichtsansprüche medizinische Daten betreffen, darf sie nur der behandelnde Arzt erfüllen.

Zu den Auskunfts- und Einsichtsrechten auch nachstehend unter 10.1.7.

10.1.6 Öffnen und Weiterleiten von Post in einem Krankenhaus

In einem Landeskrankenhaus war die Behandlung von Post umstritten, die im Adreßfeld an erster Stelle das Krankenhaus nennt und an weiterer Stelle den Zusatz "zu Händen" enthält, jedoch ohne Hinweise wie "vertraulich", "persönlich", "Arztsache" o. ä. Derart adressierte Sendungen wurden in der Poststelle geöffnet und der Krankenhausleitung vorgelegt. Die ärztliche Leitung bestand auf einer Änderung dieser "Behördenpraxis", da sie vielen Absendern unbekannt sei und dazu führe, daß der Krankenhausleitung auch Korrespondenz von Ärzten in Patientenangelegenheiten sowie Privatpost an Patienten und Mitarbeiter vorgelegt würde.

Nach ausführlicher Diskussion wurde gemeinsam folgende Lösung gefunden:

1. *Ergibt sich aus der Anschrift oder dem Absender, daß es sich um Post für einen Patienten oder von einem Patienten an einen Arzt, Psychologen oder Sozialarbeiter handelt, wird - unabhängig von der Stellung des Namens in der Anschrift - die Postsendung stets ungeöffnet an die genannte Person weitergeleitet.*

2. *Sobald sich nach dem berechtigten Öffnen (weil der Umschlag z. B. keinen Absender enthält) aus dem Briefinhalt ergibt, daß es sich um Patientenpost oder Privatpost eines Beschäftigten handelt, ist der Umschlag wieder zu verschließen und dem Betroffenen direkt zuzuleiten.*

Diese Lösung sehe ich als datenschutzgerecht an, weil unabhängig von der formalen Adressierung Patientenpost nicht geöffnet wird, wenn eine Verletzung des dem Schutz des § 203 StGB unterliegenden Bereichs vermutet werden muß. Damit ist sichergestellt, daß ein formell an das Krankenhaus (erste Stelle der Anschrift), aber "zu Händen" eines Arztes, Psychologen oder Sozialarbeiters gerichtetes Schreiben ungeöffnet weitergeleitet wird. Zugunsten des Datenschutzes sollte hingenommen werden, daß auch eine solche Handhabung nicht unproblematisch ist. Wollte ein Patient das Krankenhaus anschreiben und hat deshalb *bewußt* "zu Händen" adressiert, können seine Rechte durch die Nichtweitergabe eines solchen Schreibens an die Krankenhausleitung beeinträchtigt werden, weil der Mitarbeiter z. B. nicht erkennt, daß deren Belange betroffen sind. Dieses (Rest-)Risiko kann aber durch entsprechende Hinweise an die Mitarbeiter gering gehalten werden.

Bei anderen Absendern läßt sich diese Handhabung nicht rechtfertigen; denn sie könnte bei der Krankenhausleitung zu Informationsverlusten mit unvorhersehbaren Folgen führen. So adressieren öffentliche Stellen nach "Behördengepflogenheit" und müssen sich darauf verlassen können, daß ihre Post entsprechend behandelt wird. Dies ist nicht nur Voraussetzung für eine funktionierende Verwaltung, sondern hat auch rechtliche Konsequenzen. Denn die Art der Adressierung ist mehr als "Behördengepflogenheit". Von ihr hängt u. a. ab, ob ein Schriftstück wirksam zugestellt worden ist. Und nur eine wirksame Zustellung hat im Rechtsverkehr die vom Absender beabsichtigten rechtlichen Folgen.

Von Absendern, die ihrerseits ein Geheimnis i. S. v. § 203 StGB zu wahren haben (z. B. Ärzte, Apotheker, Anwälte, Notare, Psychologen) *muß* aufgrund von Bildungsstand und qualifizierter Ausbildung erwartet werden, daß sie durch entsprechende Adressierung (Name an erster Stelle *oder* Zusätze wie "persönlich" oder "vertrauliche Arztsache") eine unbefugte Offenbarung ausschließen.

10.1.7 Einsicht des Patienten in seine Krankenakte

Wünscht ein Patient Einsicht in seine Krankenunterlagen, ergeben sich häufig Probleme, obwohl § 33 Abs. 3 SächsKHG dazu eindeutige Regelungen enthält (vgl. oben 10.1.5).

Ein städtisches Krankenhaus fragte, ob einem Patienten im Hinblick auf ein Urteil des Bundesgerichtshof vom 23. November 1982 (NJW 1983, 328) Einsicht in seine vollständige Krankenakte gewährt werden müsse, also auch in solche Unterlagen, die über objektive physische Befunde und Berichte über Behandlungsmaßnahmen hinausgehen.

Ich habe dem Krankenhaus mitgeteilt, daß das Urteil hier ohne Bedeutung ist: Es stammt aus dem Jahre 1982, also aus der Zeit vor dem Volkszählungsurteil, mit dem das Bundesverfassungsgericht Grundsätze formuliert hat, die der Gesetzgeber bei dem Erlaß von Rechtsvorschriften über den Umgang mit personenbezogenen Daten zu beachten hat. Einer dieser Grundsätze lautet, daß der Betroffene grundsätzlich die Möglichkeit haben müsse, sich darüber zu informieren, wer was über ihn weiß und woher die Angaben stammen. Diesen Grundsatz hat der sächsische Gesetzgeber in § 33 Abs. 5 SächsKHG umgesetzt. Danach ist dem Patienten Einsicht in seine Krankenakte zu gewähren. Dieser Anspruch kann nur im Interesse der Gesundheit des Patienten begrenzt werden; durch berechtigte Geheimhaltungsinteressen Dritter wird er eingeschränkt. Eine Beschränkung auf *objektive* Daten dagegen hat der Gesetzgeber nicht vorgesehen.
Ein anderer Patient bat ein Landeskrankenhaus, ihm die über seine psychotherapeutische Behandlung gefertigten Therapieberichte sowie seinen Lebenslauf und von ihm beantwortete Fragebogen in Kopie zu übersenden. Das Krankenhaus hat dies aus "therapeutischen Gründen" sowie im Interesse der

behandelnden Ärzte abgelehnt und statt dessen ein Gespräch angeboten.

Dies war mit § 33 Abs. 5 Nr. 2 SächsKHG nicht zu vereinbaren: Die Übersendung von Kopien ist eine mögliche Form der Akteneinsicht und darf nur *im Interesse der Gesundheit des Patienten* oder *wegen berechtigter Geheimhaltungsinteressen Dritter* eingeschränkt werden.

Ob es aus medizinischer Sicht gerechtfertigt war, die Akteneinsicht durch ein ärztliches Gespräch zu ersetzen, konnte ich nicht beurteilen. Ich habe jedoch die schlichte Angabe, eine gesundheitliche Schädigung sei möglich, nicht als Ablehnungsgrund akzeptiert. Zu Gunsten des Betroffenen darf das "Recht auf Selbstgefährdung" nur in Ausnahmesituationen eingeschränkt werden. Deshalb müssen die maßgeblichen Bedenken nach Art und Richtung erläutert werden, ohne ins Detail zu gehen. (Rechtsprechung zu therapeutischen Vorbehalten als Grenzen des Selbstbestimmungsrechts: Urteil des BGH vom 6. 12. 1988 - NJW 1989, 764; bestätigt durch Beschluß des BVerfG vom 17. 11. 92 - MedR 1993, 232 - und des BVerwG vom 27. 4. 1989 - NJW 1989, 2960)

Auch die Einlassung des Krankenhauses, durch die Akteneinsicht würden die "Interessen Dritter verletzt", nämlich der behandelnden Ärzte, ist kein Grund. Dies wäre nur bei berechtigten Geheimhaltungsinteressen *Dritter* möglich. Weder ist der behandelnde Arzt im Verhältnis zum Patienten Dritter (Dritte wären z. B. Verwandte und Freunde des Patienten), noch erfährt der Patient durch die Aushändigung des eigenen Lebenslaufs, eigener Lebensziele und von ihm beantworteter Fragebögen Geheimnisse anderer Personen. Dagegen kann die Aushändigung des Therapieberichts berechtigte Geheimhaltungsinteressen Dritter beeinträchtigen. Hinsichtlich solcher Passagen ist die Einsichtnahme eingeschränkt, so daß die betreffenden Textstellen ggf. in der Kopie geschwärzt werden müßten. Nicht medizinisch begründete Interessen von Ärzten haben stets zurückzustehen.

Einem wiederum anderen Patienten hatte ein städtisches Krankenhaus für die Einweisung in ein Fachkrankenhaus das Laborergebnis einer zytologischen Untersuchung im *verschlossenen* Umschlag mitgegeben. Der Patient fragte, ob das Ergebnis der ärztlichen Schweigepflicht unterläge. Dazu habe ich ihm erläutert:

Die *ärztliche Schweigepflicht* schützt das Vertrauen des Patienten in den Arzt durch das sogenannte "Patientengeheimnis". Es verbietet dem Arzt und dem an der Behandlung beteiligten Hilfspersonal wie z. B. Krankenschwestern, Pflegern, Laborkräften, Röntgenassistenten usw. einem Außenstehenden etwas über einen Patienten zu offenbaren, was sie im Rahmen der Behandlung erfahren haben. Die Verletzung der Schweigepflicht ist strafbar (§ 203 Abs. 1 StGB).

Der Patient selbst gehört nicht zu den Außenstehenden. Er steht als unmittelbar Betroffener im Mittelpunkt der Behandlung und hat ein Recht auf Information. Deshalb gewährt das Sächsische Krankenhausgesetz ihm Einsicht in seine

Krankenakten. Laborbefunde sind deren Bestandteil und dürfen deshalb eingesehen werden; da es sich insoweit um medizinische Daten handelt, jedoch nur im Beisein des behandelnden Arztes.

10.1.8 Offene Lagerung von Patientenunterlagen

Ich erhielt den Hinweis, in einem städtischen Krankenhaus lagerten seit längerem paketweise Patientenunterlagen offen vor der Eingangstür. In der Stellungnahme des Krankenhauses hieß es, es habe sich um mit Namen, Vornamen, Geburtsdaten und krankenhausspezifischer Kennung versehene EEG-Kurven gehandelt, die zur Vernichtung bereitgestellt, aber nicht abgeholt worden seien. Um Vorkommnisse dieser Art künftig zu vermeiden, sei eine erneute Belehrung der Krankenhausmitarbeiter vorgesehen.

Ich habe dem Krankenhaus mitgeteilt, daß dies nicht ausreiche, denn es gehe um Patientendaten, von denen Personen und Stellen außerhalb des Krankenhauses nur unter den strengen Voraussetzungen des § 33 Abs. 3 SächsKHG Kenntnis erhalten dürften. Zudem stünden sie unter dem besonderen Schutz des § 203 StGB. Eine Belehrung schaffe keine Datensicherheit, deshalb müsse das zur Vernichtung vorgesehene Material mit Patientendaten (Akten, Röntgen- und Ultraschallbilder, Disketten usw.) bis zur datenschutzgerechten Löschung verschlossen aufbewahrt werden - größere Mengen in einem separaten Raum.

Das Krankenhaus hat daraufhin für jeden Fachbereich Zwischenlager eingerichtet. Ein Mitarbeiter übergibt die Unterlagen nach vorheriger telefonischer Absprache persönlich den mit der Vernichtung beauftragten Personen. Außerdem wurde eine Dienstanweisung für den Datenschutz erstellt. Danach ist das Krankenhauspersonal halbjährlich über datenschutzrechtliche Belange zu informieren.

Aufgrund des aktiven Bemühens um eine datenschutzgerechte Lösung habe ich keine Beanstandung ausgesprochen.

10.1.9 Einsichtnahme in Todesbescheinigungen durch Doktoranden

Noch nicht alle Gesundheitsämter haben sich mit den Voraussetzungen vertraut gemacht, unter denen seit dem 30. Juli 1994 (Inkrafttreten des SächsBestG) Einsicht in Todesbescheinigungen genommen werden darf. So wurde einer Medizinstudentin, die sich in ihrer Doktorarbeit mit Todesursachen beschäftigt, die Einsichtnahme mit der Begründung verweigert, daß hierfür eine Genehmigung durch das SMS erforderlich sei.

Tatsächlich bedarf es zur Einsichtnahme in Todesbescheinigungen keiner Genehmigung durch das SMS. Gemäß § 14 Abs. 5 Satz 3 Nr. 2 SächsBestG können z. B. Doktoranden im Fach Medizin Einsicht in Todesbescheinigungen nehmen, wenn

- ihr Professor oder der Institutsleiter, sinnvollerweise schriftlich, einen Antrag auf Einsichtnahme gestellt und darin Angaben zur Erforderlichkeit der Einsichtnahme für das Forschungsvorhaben sowie zu dessen wissenschaftlicher Bedeutung gemacht hat und
- das Gesundheitsamt aufgrund dieser Angaben, für deren Ergänzung es nötigenfalls sorgen muß, nach sorgfältiger Prüfung zu dem Ergebnis gekommen ist, daß den Belangen des Verstorbenen oder seiner Hinterbliebenen weniger Gewicht als dem wissenschaftlichen Interesse an der Durchführung des Forschungsvorhabens beizumessen ist.

Es ist eine Abwägung im Einzelfall erforderlich, für die sich allgemeine Regeln kaum aufstellen lassen. Als Belange des Verstorbenen oder seiner Hinterbliebenen kommen der sogenannte postmortale Persönlichkeitsschutz des Toten und das Grundrecht der Hinterbliebenen auf informationelle Selbstbestimmung in Frage. Beide sind nur berührt, wenn die erhobene Todesursache eine als ehrenrührig geltende (z. B. in Teilen der Öffentlichkeit Aids oder Selbstmord) oder eine vererbbare Krankheit ist.

Das Gesundheitsamt hat, insbesondere im Schriftverkehr mit der Hochschule (Professor oder Institut), klarzustellen, daß die Daten, die durch Gewährung von Einsicht in die Unterlagen übermittelt werden, nicht dem Doktoranden als Person, sondern dem Doktoranden als Hilfskraft der Hochschule, also der Hochschule (Institut oder Lehrstuhl) übermittelt werden, so daß die Verantwortung für den rechtmäßigen Umgang mit den Daten bei der Hochschule liegt. § 14 Abs. 5 Satz 3 Nr. 2 SächsBestG erlaubt nämlich nur die Übermittlung an mit wissenschaftlicher Forschung befaßte *Stellen*; eine frei forschende Einzelperson als solche hat nicht die mit dem Begriff "Stelle" vorausgesetzte organisatorische Verfestigung. Die Hochschule muß also intern ihre "Datenherrschaft" und ihre Verantwortlichkeit sicherstellen. Ergänzend sollte das Gesundheitsamt die Hochschule (Professor oder Institutsleiter) darauf hinweisen, daß für den Umgang mit den betreffenden Daten gemäß § 14 Abs. 5 Satz 3 Nr. 2, 2. Satz SächsBestG die Vorschriften des § 30 Abs. 2 bis 5 SächsDSG entsprechend gelten. Weil es sich um die Übermittlung personenbezogener Daten an die Hochschule und somit an eine öffentliche Stelle im Sinne von § 30 Abs. 2 SächsDSG handelt, braucht sich das Gesundheitsamt die in dieser Vorschrift vorgesehene Verpflichtungs-Erklärung nicht abgeben zu lassen.

10.1.10 Datenschutz im Maßregelvollzug

Aufgrund strafgerichtlicher Entscheidung können psychisch kranke Straftäter zum Maßregelvollzug in einem Fachkrankenhaus für Psychiatrie (Landeskrankenhaus) untergebracht werden. Ein solcher Patient vermutete die Verletzung der ärztlichen Schweigepflicht durch Ärzte und andere Krankenhausmitarbeiter. Er gab an, Außenstehende und nicht an seiner Behandlung Beteiligte seien über Einzelheiten seines Verhaltens sowie über bestimmte Äußerungen informiert worden. Dies führte er u. a. auf die engen verwandtschaftlichen Beziehungen zwischen den Beschäftigten

zurück. Außerdem sah er sein Persönlichkeitsrecht durch Kontrollen beeinträchtigt, dieim Zusammenhang mit seinen Aufenthalten außerhalb des Krankenhauses durchgeführt wurden.

Die rechtlichen Rahmenbedingungen:

Datenweitergabe innerhalb des Krankenhauses
Bei der Datenverarbeitung für Patienten im Maßregelvollzug gelten gemäß § 33 Abs. 2 Nr. 3 SächsKHG bereichsspezifische Rechtsvorschriften, hier das Strafvollzugsgesetz in Verbindung mit dem Sächsischen Gesetz über die Hilfen und die Unterbringung bei psychischen Krankheiten (SächsPsychKG). Danach hat die Behandlung eines psychisch kranken Straftäters nach ärztlichen Gesichtspunkten zu erfolgen, wobei ihm die nötige Aufsicht, Betreuung und Pflege zuteil werden muß. Die Behandlung ist nach einem Behandlungsplan durchzuführen, zu dem auch Schulbesuche, Berufsausübung und Arbeit - ggf. außerhalb des Krankenhauses - gehören können (§ 38 Abs. 2 SächsPsychKG).

Zwischen dem an der *Behandlung* beteiligten Krankenhauspersonal (z. B. Ärzte, Pfleger, Therapeuten; im Rahmen der Arbeitstherapie einbezogene Gärtner, Handwerker sowie Küchen- und Wäschereipersonal) dürfen die erforderlichen Informationen weitergegeben werden. Werden jedoch aus diesem "zum Wissen berufenen" Kreis Daten an nicht in das Behandlungsgeschehen einbezogene Dritte weitergegeben, so verstößt dies nicht nur gegen Datenschutzbestimmungen, weil die Weitergabe der Daten nicht erforderlich ist, sondern auch gegen das Patientengeheimnis, selbst wenn die Dritten Angehörige des Krankenhauses sind und ihrerseits das Patientengeheimnis zu wahren haben.

Datenweitergabe an Personen und Stellen außerhalb des Krankenhauses
Jeder Aufenthalt des Patienten außerhalb des Krankenhausgeländes ohne Beaufsichtigung ist eine Vollzugslockerung. Da der Vollzug auch während der Dauer der Inanspruchnahme von Vollzugslockerungen erfolgt (§ 38 Abs. 3 letzter Satz SächsPsychKG), unterliegt der Patient auch in dieser Zeit gemäß § 136 StVollzG der *nötigen* Aufsicht. Wenn seitens des Krankenhauses im Rahmen dieser Aufsicht Kontakt zu Personen außerhalb des Krankenhauses aufgenommen wird und in diesem Zusammenhang Patientendaten mitgeteilt werden, ist dies datenschutzrechtlich nicht zu beanstanden. Entsprechendes gilt, wenn die Entlassung des Patienten bevorsteht und das Krankenhaus i. S. v. § 38 Abs. 4 SächsPsychKG mit Personen und Institutionen zusammenarbeitet, die den Patienten künftig betreuen oder ihm beistehen werden.

Bei meinem Besuch im Fachkrankenhaus hat sich bestätigt, daß das Krankenhauspersonal über datenschutzrechtliche Belange unzureichend unterrichtet war. So fehlte eine Dienstanweisung bzw. Hausverfügung o. ä. zum Datenschutz. Die datenschutzrechtlichen Regelungen im Sächsischen Krankenhausgesetz waren unbekannt, ebenso § 6 SächsDSG, so daß Verpflichtungen auf das Datengeheimnis nicht vorgenommen wurden. Noch bis *Ende 1994* wurde ein Vordruck verwendet, der

über die Schweigepflicht nach *§ 136 des Strafgesetzbuches der DDR* - Verletzung des Berufsgeheimnisses durch Rechtsanwälte, Notare, Ärzte, Psychologen, Hebammen, Apotheker oder deren Mitarbeiter - belehrte.

Ich habe dem Patienten mitgeteilt, daß die im Rahmen der Vollzugslockerungen vorgenommenen Kontrollen datenschutzrechtlich nicht zu beanstanden seien, daß jedoch das Klinikpersonal offensichtlich nicht ausreichend über datenschutzrechtliche Belange informiert sei und ich mich für die Beseitigung dieses Defizits einsetzen würde.
Die Belehrung über die Schweigepflicht ist inzwischen überarbeitet und mir vorgelegt worden. Darüber hinaus halte ich es jedoch für unerläßlich, auch eine Dienstanweisung zum Datenschutz zu erstellen.

10.1.11 Ärztliche Bescheinigung zur Haft- und Gewahrsamsfähigkeit

Die Kassenärztliche Vereinigung Sachsen bat mich um eine datenschutzrechtliche Prüfung der ärztlichen Bescheinigungen zur Haft- und Gewahrsamsfähigkeit.

1. Ärztliche Bescheinigung zur Gewahrsamsfähigkeit

Zu den zunächst bestehenden datenschutzrechtlichen Problemen konnte mit dem SMI weitgehende Übereinstimmung erzielt werden. Das SMI hat die Polizeidienststellen zur Aktualisierung der *Verwaltungsvorschrift zur Durchführung des Gewahrsams* vom 4. Juni 1993 zu deren Punkt 3.3 aufgrund von mir gemachter Vorschläge auf folgendes hingewiesen:

Der Befund des untersuchenden Arztes zur Beurteilung der Gewahrsamsfähigkeit ist künftig in einem verschlossenen Umschlag bei den polizeilichen Akten aufzubewahren. Auf dem Kuvert wird dann nur das Ergebnis der Untersuchung zur Gewahrsamsfähigkeit vermerkt.

Die Angabe des Arbeitgebers ist nicht erforderlich. Daher ist auf die Erhebung dieses Datums zu verzichten. In den Formularen wird dieses Datum gestrichen. Ich habe darauf hingewiesen, daß die bisher erhobenen Arbeitgeberdaten gemäß § 49 SächsPolG i. V. m. §§ 19, 20 SächsDSG zu löschen bzw. zu sperren sind.

Die Angabe der Krankenkasse ist notwendig, da während des Gewahrsams gemäß § 22 SächsPolG der Anspruch auf Sachleistungen der Krankenkasse ohne Unterbrechung fortbesteht. § 16 Abs. 1 Nr. 4 SGB V (Ruhen des Anspruchs) greift hier nicht ein.

Die Einwilligung des Betroffenen in die Offenbarung seiner Patientendaten durch den behandelnden Arzt wird vor der Untersuchung schriftlich (unter Hinweis auf die Bedeutung und die Freiwilligkeit der Erklärung) eingeholt. Rechtliche Folgen hat die Verweigerung der Einwilligung nicht. Jedoch könnten fehlende medizinische Daten eine Gefahr für Gesundheit und Leben für den Betroffenen entstehen lassen; das muß er

wissen.

Bei einem Notfall, beispielsweise bei Bewußtlosigkeit, wird man in der Regel die mutmaßliche Einwilligung in die Offenbarung annehmen können.

Nicht erforderlich ist die Einwilligung, wenn die Offenbarung in Ausnahmefällen zum Schutze höherwertiger Rechtsgüter erforderlich ist oder gesetzliche Anzeige- und Mitteilungspflichten bestehen.

2. Ärztliche Bescheinigung zur Haftfähigkeit

Ebenfalls legte mir die Kassenärztliche Vereinigung Sachsen ein Formular zur datenschutzrechtlichen Prüfung vor, das der Feststellung der Haftfähigkeit dient. Nach Auskunft des SMJus, das die Justizvollzugsanstalten und die Justizvollzugskrankenhäuser befragt hat, wird das Formular jedoch von der Justizverwaltung des Freistaates nicht verwendet. Das Ergebnis der Aufnahmeuntersuchung und die Entscheidung, ob der Gefangene nach ärztlicher Auffassung vollzugstauglich ist, wird vielmehr auf einem anderen, bundeseinheitlichen Vordruck festgehalten.

10.2 Sozialwesen

10.2.1 Verwaltungsvorschrift zur Durchführung des Wohngeldverfahrens

Die Wohngeldstellen haben in Sachsen ein vom SMI vorgeschriebenes Verfahren anzuwenden (siehe auch unter 10.2.6). Einzelheiten sollten durch eine Verwaltungsvorschrift konkretisiert und festgeschrieben werden. An dem Entwurf wurde ich beteiligt.

Mein grundsätzlicher Einwand war, daß ein landeseinheitliches Wohngeldverfahren für die Kommunen einen unzulässigen Eingriff in deren Organisationshoheit bedeutet. Diese beruht auf der kommunalen Selbstverwaltung und ist verfassungsrechtlich garantiert; sie fördert eine ortsnahe und damit für den Betroffenen überschaubare dezentrale Datenverarbeitung. Inzwischen konnte ich das SMI überzeugen, daß dieses Recht nicht nur zu achten, sondern aktiv zu fördern ist. Deshalb soll an die Stelle des jetzigen landeseinheitlichen Verfahrens bis spätestens 1999 ein Verfahren treten, das den Kommunen Raum für dezentrale Lösungen läßt.

Den beabsichtigten generellen Datenabgleich zwischen Sozialamt und Wohngeldstelle habe ich als unzulässig angesehen. Er sollte den gleichzeitigen Bezug von pauschaliertem Wohngeld und Tabellenwohngeld bei Leistungsempfängern verhindern. Auch wenn die Feststellung des Doppelbezugs wünschenswert ist, fehlt für einen generellen Datenabgleich die gesetzliche Grundlage. Diese läßt derzeit den Abgleich

nur im Einzelfall zu. Das SMI hat die vorgesehene Regelung gestrichen und wird stattdessen eine Gesetzesinitiative beim Bundesministerium für Bauangelegenheiten anregen.
Auch in einer Reihe weiterer Fragen wurde Einigkeit erzielt.
Aufgrund meiner Hinweise wurden die Regelungen zur Wohngeldstatistik mit dem geltenden Recht in Übereinstimmung gebracht und bei der Mikroverfilmung von Wohngeld-Unterlagen auf die in § 80 SGB X geregelte Datenverarbeitung im Auftrag Bezug genommen.

10.2.2 Führung eines Dateien- und Geräteverzeichnisses durch Sozialleistungsträger

Die LVA Sachsen bat mich um Stellungnahme, mit welchem Inhalt das Dateien- und Geräteverzeichnis zu erstellen sei und ob eine Pflicht bestehe, dieses Verzeichnis dem Sächsischen Datenschutzbeauftragten zuzuleiten.
Gemäß § 81 Abs. 4 Satz 1 SGB X gilt für Sozialleistungsträger § 18 Abs. 2 und 3 BDSG. Die Sozialleistungsträger haben demnach ein Dateien- und Geräteverzeichnis mit dem Inhalt des § 18 Abs. 2 und 3 BDSG zu führen.

Diese Regelung gilt jedoch nicht für die Sozialleistungsträger der Länder, die das jeweilige Landesrecht anzuwenden haben. Davon ausgenommen sind wiederum die Sozial*versicherungs*-träger und ihre Verbände (§ 81 Abs. 4 Satz 4, 1. Halbs. SGB X).

Im Klartext bedeutet diese Regelung, daß z. B. die Sozialämter, Jugendämter und Wohngeldstellen ein Dateien- und Geräteverzeichnis nach § 10 SächsDSG, die landesunmittel-baren Krankenkassen (Allgemeine Ortskrankenkassen, Innungskrankenkassen, Betriebs-krankenkassen, Landwirtschaftliche Krankenkassen), aber auch z. B. die Landesversicherungs-anstalt und der Sächsische Gemeindeunfallversicherungsverband § 18 Abs. 2 und 3 BDSG anzuwenden haben.

Insoweit ist die Rechtslage - trotz der verwirrenden Formulierung - eindeutig.
Gestritten wird hingegen um die Auslegung des zweiten Halbsatzes von § 84 Abs. 1 Satz 4 SGB X ("Im übrigen bleiben landesrechtliche Vorschriften über Verzeichnisse der eingesetzten Datenverarbeitungsanlage und Dateien sowie über behördliche Datenschutzbeauftragte unberührt"). Aus dieser Formulierung wird zum Teil die Schlußfolgerung gezogen, daß die landesunmittelbaren Sozial*versicherungs*träger neben einem Dateien- und Geräteverzeichnis nach § 18 Abs. 2 und 3 BDSG zusätzlich ein weiteres Verzeichnis nach Landesrecht zu führen haben.
Für mich ist nicht erkennbar, welchen Sinn ein solches doppeltes Verzeichnis haben sollte, zumal die Angaben nach § 18 BDSG und nach § 10 SächsDSG weitgehend übereinstimmen. Eine solche Bürokratisierung ist (selbst) dem Sozialdatenschutz fremd.

Der zweite Halbsatz könnte vielmehr so auszulegen sein, daß auch für die

Sozialversicherungsträger Landesrecht gilt, soweit es hinsichtlich der Verzeichnisse und der behördlichen Datenschutzbeauftragten Regelungen trifft, die über § 81 Abs. 4 Satz 1 bis 3 SGB X hinausgehen. Damit ist allerdings nicht die unterschiedliche Meldepflicht für die Verzeichnisse nach dem Bundesdatenschutzgesetz und den Landesdatenschutzgesetzen gemeint, weil diese bereits in Absatz 2 geregelt ist. Eine über die Sätze 1 bis 3 hinausgehende Regelung kennt zumindest das Sächsische Datenschutzgesetz nicht (zur Meldepflicht siehe unten).

Der nicht eindeutig formulierte zweite Halbsatz läßt sich am ehesten sinnvoll auslegen, wenn man ihn als Öffnungsklausel betrachtet. Die Verarbeitung von Sozialdaten ist abschließend im Zweiten Kapitel des Zehnten Buches geregelt (§ 35 Abs. 2 SGB I). Mit einer Öffnungsklausel hat der Gesetzgeber für die Sozialleistungsträger mit Ausnahme der Sozialversicherungsträger den Weg freigegeben für die Anwendung des durch § 35 Abs. 2 SGB X versperrten Landesrechts. Er will darüber hinaus klarstellen, daß auch für die Sozialversicherungsträger das Landesrecht gilt, wenn sie nicht Sozialdaten, sondern etwa Beschäftigtendaten verarbeiten.

Zusammenfassend ist also festzustellen, daß die Sozialleistungsträger mit Ausnahme der Sozialversicherungsträger ein Dateien- und Geräteverzeichnis nach § 10 SächsDSG, die Sozialversicherungsträger ausschließlich nach § 18 Abs. 2 und 3 BDSG führen.

Ob die so erstellten Verzeichnisse an den Landesdatenschutzbeauftragten zu melden sind, richtet sich nach § 81 Abs. 2 SGB X. Die Vorschrift unterscheidet nicht zwischen Sozialversicherungsträgern und sonstigen Sozialleistungsträgern, sondern verweist einheitlich auf das Landesrecht. Das Sächsische Datenschutzgesetz kennt keine Pflicht zur Anzeige oder Meldung des Dateien- und Geräteverzeichnisses. Es ist vielmehr dem Sächsischen Datenschutbeauftragten nur auf dessen Aufforderung zuzuleiten (§ 28 Abs. 1 SächsDSG).

Hinzuzufügen ist noch, daß nur die Sozialversicherungsträger einen behördlichen Datenschutzbeauftragten bestellen müssen, dessen Rechte und Pflichten sich nach den §§ 36 und 37 Abs. 1 BDSG richten.

10.2.3 Übermittlung von Sozialdaten aufgrund einer landesrechtlichen Regelung

Gemäß § 1 Abs. 1 SächsLErzGG besteht ein Anspruch auf Leistungen nur dann, wenn das Kind nicht gleichzeitig eine mit staatlichen Mitteln geförderte Kindertageseinrichtung besucht.

Nach einer Feststellung des SMS nehmen jedoch ca. 15 % der Familien beide Leistungen in Anspruch, obwohl in den Antragsformularen und Bescheiden auf den Ausschluß eines gleichzeitigen Bezuges hingewiesen wird. Das Ministerium bat mich daher um Prüfung, ob im Landeserziehungsgeldgesetz angeordnet werden dürfe, daß

die Jugendämter zweimal jährlich den Ämtern für Familie und Soziales, die das Landeserziehungsgeldgesetz ausführen, Namen und Anschrift der Erziehungsberechtigten mitteilen müssen, deren Kinder eine Kindertageseinrichtung besuchen.

Die Jugendämter übermitteln, wenn sie die Namen der Erziehungsberechtigten mitteilen, Sozialdaten. Eine Erhebung, Verarbeitung und Nutzung von Sozialdaten ist nur unter den Voraussetzungen des Zweiten Kapitels des Zehnten Buches zulässig (§ 35 Abs. 2 SGB I).

Gemäß § 67 d Abs. 1, 2. Fall SGB X ist die Übermittlung zulässig, soweit eine gesetzliche Übermittlungsbefugnis nach einer Rechtsvorschrift "in diesem Gesetzbuch" vorliegt. "Dieses Gesetzbuch" ist zu verstehen als das Sozialgesetzbuch mit seinen verschiedenen Büchern bzw. besonderen Teilen.

Die Gesetze, die als besondere Teile gelten, sind in Artikel II § 1 SGB I aufgeführt. In Nr. 20 wird der Erste Abschnitt des Bundeserziehungsgeldgesetzes genannt. Dieser Erste Abschnitt gilt also als Teil des Sozialgesetzbuchs. Eine darin geregelte Übermittlungsbefugnis ist eine Rechtsvorschrift im Sinne von § 67 d Abs. 1 SGB X.

Das Landeserziehungsgeldgesetz gehört nicht zu diesem Katalog, der im übrigen ausschließlich Bundesgesetze nennt.
Dieser Gesichtspunkt spricht dafür, daß der Landesgesetzgeber eine eigenständige Übermittlungsbefugnis nicht schaffen kann, weil andernfalls entgegen § 67 d Abs. 1, 2. Fall SGB X eine Übermittlungsbefugnis "außerhalb dieses Gesetzbuches" entstehen würde. Etwas anderes ergibt sich auch nicht aus § 67 Abs. 2 Nr. 4 SGB X ("Aufgaben nach diesem Gesetzbuch sind, soweit dieses Kapitel angewandt wird, auch Aufgaben, soweit sie den in § 35 des ersten Buches genannten Stellen durch Gesetz zugewiesen sind"). Diese Vorschrift räumt dem Landesgesetzgeber keine Regelungsbefugnis ein, sondern erweitert den in § 67 Abs. 1 SGB X definierten Begriff der Sozialdaten. Sozialdaten sind danach Einzelangaben, die von einer in § 35 SGB I genannten Stelle "im Hinblick auf ihre Aufgaben nach diesem Gesetzbuch" erhoben, verarbeitet und genutzt werden. Aufgaben sind also auch solche, die den Leistungsträgern nicht durch das Sozialgesetzbuch, sondern durch ein anderes Gesetz zugewiesen sind, etwa Aufgaben der Bundesanstalt für Arbeit nach § 17 des Arbeitnehmerüberlassungsgesetzes.
Zur Klärung dieser Auslegungsfragen habe ich den Bundesbeauftragten für den Datenschutz und das Bundesministerium für Arbeit und Sozialordnung um Auslegungshilfe gebeten (zu einem weiteren Auslegungsproblem bei § 67 Abs. 2 Nr. 4 SGB X nachstehend unter 10.2.12). Die Überlegungen sind noch nicht abgeschlossen.
In Anbetracht dieser Unsicherheiten hat das Sächsische Staatsministerium für Soziales, Gesundheit und Familie darauf verzichtet, in den Gesetzentwurf eine Übermittlungspflicht der Jugendämter aufzunehmen. Eine Übermittlung durch sie erfolgt also nur dann, wenn die Voraussetzungen der §§ 64, 65 SGB VIII, §§ 67 b, 67 d ff. SGB X erfüllt sind.

Allerdings findet nun eine verstärkte Information und Kontrolle bereits bei Antragstellung auf Erziehungsgeld statt. Eine bessere Information ist schon deshalb sinnvoll, weil es für die Betroffenen nicht auf der Hand liegt, daß sich die beiden Leistungen ausschließen. Der Antragsteller bestätigt, daß das Kind im Bezugszeitraum keinen staatlich geförderten Platz in einer Kindertageseinrichtung in Anspruch nehmen wird. Weil zwischen Antragstellung und Bescheiderteilung ein längerer Zwischenraum liegt, wird vor Bescheiderteilung erneut nach einer Inanspruchnahme eines Platzes in einer Kindertageseinrichtung gefragt und im Bescheid ein weiteres Mal auf die Mitteilungspflicht hingewiesen.

Ich habe dieses Verfahren begrüßt.

10.2.4 Weitergabe des Prüfberichts durch das Landesprüfungsamt für Sozialversicherung

Das Landesprüfungsamt für Sozialversicherung führt gemäß § 274 SGB V mindestens alle fünf Jahre die Geschäfts-, Rechnungs- und Betriebsprüfung der seiner Aufsicht unterstehenden Krankenkassen durch.

Neben dieser Prüfung steht ein weiteres, selbständiges Kontrollverfahren. Aufgabe der Krankenkassen ist es nämlich nicht nur, die Beiträge zur Krankenversicherung einzuziehen und ordnungsgemäß zu verwalten. Zugleich sind sie Einzugstelle für den Gesamtsozialversicherungsbeitrag, der auch die Beiträge zur Renten-, Pflege- und zur Arbeitslosenversicherung umfaßt (§§ 28 d, 28 h SGB IV). Die Träger der Rentenversicherung und die Bundesanstalt für Arbeit prüfen daher bei den Einzugsstellen Eingang, Verwaltung, Weiterleitung, Abrechnung und Abstimmung der ihnen zustehenden Beiträge (§ 28 q SGB IV).

Die Krankenkassen werden also regelmäßig sowohl vom Landesprüfungsamt für Sozialversicherung als auch von den Rentenversicherungsträgern und der Bundesanstalt für Arbeit aufgesucht.

Eine Krankenkasse teilte mir mit, das Landesprüfungsamt stelle den Prüfbericht den anderen Beteiligten vollständig zur Verfügung. Bei einer Prüfung durch das Landesarbeitsamt und die Landesversicherungsanstalt Sachsen habe einer der Prüfer wörtlich aus dem Prüfbericht des Landesprüfungsamts zitiert. Auf Nachfrage habe er angegeben, es gebe im Hause des Landesprüfungsamtes sogar eine Kontaktperson für den Austausch der Berichte. Als Begründung für diese Praxis sei genannt worden, das Landesprüfungsamt sehe es zur Bestätigung der eigenen Feststellungen gerne, wenn sie auch in den Prüfberichten der anderen Sozialleistungsträger erschienen.

Das von mir um Stellungnahme gebetene Landesprüfungsamt teilte mit, hier sei im Einzelfall dem Landesarbeitsamt ein Prüfbericht zur Verfügung gestellt worden. Eine

Kontaktperson, die für den regelmäßigen Austausch der Berichte zuständig sei, gebe es im Landesprüfungsamt jedoch nicht. Auch treffe die Annahme koordinierter Feststellungen zur Bestätigung der Rechtsauffassung des Landesprüfungsamts nicht zu. Es halte jedoch "bei Beachtung der einschlägigen Vorschriften des SGB X" die Überlassung bestimmter Prüfungsteile "im Rahmen der Amtshilfe" für zulässig. Wenn darüber hinaus durch einen "zulässigen Datenaustausch" die wirtschaftliche Erbringung von Dienstleistungen bei den beteiligten Stellen noch gefördert werden könne, so sei dieser Gesichtspunkt ebenfalls beachtenswert. Zulässig sei die Übermittlung der Sozialdaten gemäß § 69 Abs. 1 Nr. 1 SGB X.

Die Amtshilfe kommt als Grundlage für eine Datenerhebung, -übermittlung und -nutzung nicht in Betracht, da jeder Umgang mit personenbezogenen Daten, wie das Bundesverfassungsgericht im Volkszählungsurteil (BVerfGE 65, 1 ff.) klargestellt hat, einer - möglichst spezifischen - Rechtsgrundlage bedarf. Kurz: Datenschutz ist amtshilfefest.

Das Landesprüfungsamt übermittelt personenbezogene Daten, weil in seinem Prüfbericht Einzelfälle mit Betriebsnummer oder Krankenversichertennummer aufgeführt werden, so daß Betriebe, Betriebsinhaber und Versicherte zumindest bestimmbar sind.

Das Landesprüfungsamt ist zwar kein Sozialleistungsträger, es erfüllt jedoch Aufgaben im Sinne von § 67 c Abs. 3 SGB X, da es Kontrollbefugnisse wahrnimmt. Daher hat es das Sozialgeheimnis wie ein Sozialleistungsträger zu wahren (§ 35 Abs. 1 Satz 4 SGB I). Eine Erhebung, Verarbeitung und Nutzung ist nur unter den Voraussetzungen des Zweiten Kapitels des Zehnten Buches zulässig (§ 35 Abs. 2 SGB I).

Das Landesprüfungsamt will die Übermittlung auf § 69 Abs. 1 Nr. 1 SGB X stützen. Nach allen drei in dieser Vorschrift vorgesehenen Möglichkeiten ist die Übermittlung von Sozialdaten nur zulässig, soweit sie erforderlich ist für die im einzelnen genannten Zwecke. Der Prüfauftrag der LVA Sachsen und des Landesarbeitsamts gemäß § 28 q SGB IV ist sehr viel enger als die Aufgabe des Landesprüfungsamts. Während sich die Prüfung der LVA Sachsen und des Landesarbeitsamts auf den Einzug, die Verwaltung, Weiterleitung, Abrechnung und Abstimmung der ihnen zustehenden Beitragsansprüche sowie das Meldeverfahren beschränkt, muß das Landesprüfungsamt die gesamte Geschäfts- Rechnungs- und Betriebsführung kontrollieren.
Ein Teil der im Bericht des Landesprüfungsamtes enthaltenen Sozialdaten hat einen Bezug auch zu den Aufgaben der anderen an der Prüfung beteiligten Stellen. Bei anderen Sozialdaten fehlt er. Aber selbst bei den zuerst genannten ist die Übermittlung nicht erforderlich. Erforderlich heißt, daß der Empfänger ohne diese Daten seine Aufgaben nicht, nicht ordnungsgemäß oder nicht rechtzeitig erfüllen könnte. Die LVA Sachsen und das Landesarbeitsamt sind in diesem Sinne keineswegs auf die Daten des Landesprüfungsamts angewiesen, weil sie sich diese Daten ohne weiteres selbst verschaffen können. Der Gesetzgeber hat verschiedene Einrichtungen mit der Prüfung beauftragt, nicht aber den Aufsichtsbehörden der Länder eine Generalkompetenz

zugewiesen.
Die Übermittlung würde also zu einer gewissen Arbeitserleichterung führen, die jedoch nicht den Anforderungen an eine Erforderlichkeit im oben dargelegten Sinne entspricht. Zudem besteht die Gefahr, daß LVA Sachsen und Landesarbeitsamt ohne ausreichende eigene Prüfung Feststellungen des Landesprüfungsamt übernehmen und damit der Intention des Gesetzgebers zuwiderhandeln.

Die Diskussion mit dem Landesprüfungsamt ist noch nicht abgeschlossen.

10.2.5 Wie wird der überwiegende Teil des gesamten Datenbestands bei der Auftragsdatenverarbeitung von Sozialdaten bestimmt?

Soll eine private Stelle Sozialdaten im Auftrag verarbeiten, ist dies nach § 80 Abs. 5 Nr. 2 SGB X nur zulässig, wenn der überwiegende Teil der Speicherung des gesamten Datenbestands beim Auftraggeber verbleibt. Die Frage, woraus sich der gesamte Datenbestand eines Auftraggebers zusammensetzt, ist mir wiederholt gestellt worden (dazu auch unter 10.2.6 und 10.2.13). Entschieden ist sie noch nicht. Das Zehnte Buch des Sozialgesetzbuches enthält keine Definition des Gesamtbestands, selbst die Gesetzesbegründung gibt keinen Aufschluß. Auch die mir bekannte Literatur und Rechtsprechung hat sich mit dieser Frage nicht im einzelnen auseinandergesetzt. Für die Entscheidung, ob ein Privatunternehmen mit der Datenverarbeitung beauftragt werden darf, ist sie jedoch von zentraler Bedeutung.

Einen Lösungsansatz habe ich in Antworten auf folgende Fragen - konkretisiert auf den Beispielfall einer automatisierten Verarbeitung von Wohngelddaten - gesucht:
1. Sind mit "Gesamtbestand" die Daten des Einzelnen oder aller Betroffenen gemeint?
2. Wie beurteilt sich der überwiegende Teil, wenn identische Daten sowohl in Akten als auch auf Datenträgern gespeichert sind, die nur durch automatisierte Verfahren ausgewertet werden können?
3. Sind in den Gesamtbestand außer den aktuellen auch abgeschlossene Fälle einzubeziehen?

Zu Frage 1:
Nach der Begriffsbestimmung in § 67 Abs. 1 SGB X sind Sozialdaten "Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person ...". Diese Definition stellt den Einzelnen als Betroffenen in den Mittelpunkt des Datenschutzes und legt den Gedanken nahe, den Gesamtbestand der Daten auf den jeweiligen Betroffenen zu beziehen. Denn die Möglichkeit einer Persönlichkeitsverletzung ist um so größer, je mehr Daten über ihn in fremde Hände gelangen. Ausgehend von diesem Gedanken dürften z. B. die Anschriftendaten aller Wohngeldempfänger im Auftrag verarbeitet werden, nicht aber ein einziger kompletter Fall.

Gegen eine solche Auslegung spricht aber das allgemeine Sprachverständnis, wonach unter "Datenbestand" zunächst die Gesamtheit der Daten für eine Vielzahl von Fällen

verstanden wird.

Zu Frage 2:
§ 67 Abs. 1 SGB X definiert die Sozialdaten unabhängig von dem Datenträger, auf dem sie gespeichert sind. Sind identische Daten gleichzeitig mehrfach in einem (Sozial-)Datenbestand - etwa in einer automatisierten Datei (sowie i. a. zusätzlich in einer Sicherheitskopie derselben) und in einer Akte - vorhanden (Fall der "Informationsredundanz"), kann mit "Gesamtdatenbestand" nur der redundanzfreie Datenbestand gemeint sein. Anders ausgedrückt: Sind identische Daten auf verschiedenen Datenträgern gespeichert, bildet die logische Informationsmenge den Datenbestand, unabhängig davon, wie oft, in welcher Form und in welchem Zusammenhang die Einzelinformationen gespeichert sind. Erhält der Auftragnehmer z. B. auf Diskette alle Daten aus allen Wohngeldanträgen, so wird ihm der gesamte Datenbestand übergeben und nicht nur deshalb die Hälfte, weil das Antragsformular mit denselben Daten beim Auftraggeber verbleibt.

Im allgemeinen ist davon auszugehen, daß die beim Auftraggeber in Akten vorhanden Daten umfassender sind als die einem Auftragnehmer zur automatisierten Weiterverarbeitung zur Verfügung gestellten. In der Praxis dürfte eine Quantifizierung nur im Schätzwege möglich sein, wobei der tatsächliche Datenbestand keine geeignete Ausgangsbasis ist, ganz abgesehen davon, daß er sich vermutlich wegen der unterschiedlichen Fallkonstellationen nicht einmal näherungsweise feststellen ließe. Zur Bestimmung des überwiegenden Teils könnte es ein Weg sein, auf den "typischen Einzelfall" abzustellen. Dabei wären die Daten, die der Auftragnehmer zur Weiterverarbeitung erhält, den vom Auftraggeber erhobenen Daten gegenüberzustellen. Bezogen auf das Wohngeldverfahren müßten die personenbezogenen Daten aus der Datensatzbeschreibung für die automatisierte Verarbeitung zu den im Wohngeldantrag vorgesehenen Angaben ins Verhältnis gesetzt werden.

Dieses Ergebnis würde eine weitere Diskussion der Frage 1 erübrigen, weil vom Prinzip her auf den Einzelnen abgestellt würde.

Zu Frage 3:
Nach § 84 Abs. 2 SGB X sind Sozialdaten u. a. zu löschen, wenn ihre Kenntnis für die speichernde Stelle zur rechtmäßigen Aufgabenerfüllung nicht mehr erforderlich ist. Ausgehend von dieser Regelung müßten in den Gesamtbestand deshalb auch abgeschlossene Fälle einbezogen werden. Allerdings ist bei abgeschlossenen Fällen der zu Frage 2 aufgezeigte Lösungsansatz für eine "typisierende Betrachtungsweise" am Einzelfall nicht möglich. Vielmehr müßte auf Fallzahlen abgestellt werden, indem die beim Auftraggeber und Auftragnehmer jeweils gespeicherten (gleichartigen) Fälle ins Verhältnis gesetzt würden. Derartige Fallzahlen unterliegen jedoch einem dynamischen Prozeß mit sich verändernden Anteilen.

So hat ein Auftraggeber in der Regel bereits vor der Auftragserteilung Sozialdaten aus (laufenden und) abgeschlossenen Fälle gespeichert. In der Anfangsphase dürften die

Zulässigkeitsvoraussetzungen meist erfüllt sein, weil der überwiegende Teil des Datenbestands beim Auftraggeber verbleibt (vorausgesetzt, abgeschlossene Fälle sind nicht Auftragsgegenstand). Dieses Verhältnis kann sich mit zunehmender Dauer des Auftragsverhältnisses in Richtung Unzulässigkeit verschieben.

Dem hätte ein Auftraggeber im Wohngeldbereich dadurch entgegenzuwirken, daß er nach § 80 Abs. 4 SGB X kurze Speicherungsfristen für abgeschlossene Fälle vereinbart und im Bedarfsfall die Daten nicht im Dialogbetrieb beim Auftragnehmer abruft, sondern auf seine Akten zurückgreift.

Vorstehende Antworten sollen ein Lösungsansatz für eine weiterführende Diskussion sein.

10.2.6 Datenverarbeitung im Auftrag zur Wohngeldberechnung

In meinem 2. Tätigkeitsbericht habe ich mich unter Nr. 5.5.1 ausführlich mit der Entwicklung der kommunalen Datenverarbeitung in Sachsen auseinandergesetzt und dabei die Aufgaben der Zweckverbände kritisch beleuchtet. Trotz meiner grundsätzlichen Bedenken hat das SMI die Wohngeldberechnung nicht von dem bis zum 31. Dezember 1995 beauftragten Privatunternehmen auf die Kommunen übertragen, sondern im Rahmen einer Kooperationsvereinbarung den dazu neu gegründeten Zweckverbänden die Gesamtabwicklung des Wohngeldverfahrens ab 1. Januar 1996 übertragen.

Der Freistaat Sachsen ist allerdings Inhaber der Rechte an den zur Zeit von fast allen Wohngeldstellen in Sachsen verwendeten Wohngeld-Programmen, er hat das alleinige Verfügungsrecht.

Nunmehr haben sich die Kommunen an dem Verfahren zu beteiligen, selbst wenn sie die Wohngeldberechnung im eigenen Rechenzentrum kostengünstiger gestalten können. Ausnahmen müssen beantragt werden und sind nur zulässig, wenn es die wirtschaftliche Leistungsfähigkeit der *Zweckverbände* nicht beeinträchtigt. Darin habe ich einen unzulässigen Eingriff in die Organisationshoheit der Kommunen gesehen, die auf ihrer verfassungsrechtlich garantierten Selbstverwaltung beruht und von der staatlichen Verwaltung nicht nur zu respektieren, sondern aktiv zu fördern ist.
Inzwischen habe ich das SMI davon überzeugt, daß den Wohngeldstellen die Wahl des Verfahrens grundsätzlich offenstehen muß. Bis zum Auslaufen der Kooperationsvereinbarung im Jahre 1999 sollen die Voraussetzungen für ein dezentrales Verfahren geschaffen werden, das die Wohngeldstellen auf freiwilliger Grundlage einführen können.

Nicht nur das zentrale Wohngeldverfahren forderte meine Kritik heraus.

Mehrere Gemeinden traten mit Zweifelsfragen zu den Vertragstexten an mich heran,

die ihnen die Zweckverbände zur Auftragserteilung übersandt hatten. Tatsächlich waren die Verträge stark überarbeitungsbedürftig, weil fälschlicherweise von § 7 SächsDSG als Grundlage für die Datenverarbeitung im Auftrag ausgegangen worden war. Wohngelddaten sind jedoch Sozialdaten, so daß § 80 Abs. 1 und 2 SGB X mit seinen differenzierten Anforderungen zu beachten ist.

Im einzelnen bestanden folgende Defizite:

- Nach § 80 Abs. 1 SGB X bleibt der Auftraggeber für die Einhaltung der Vorschriften nach dem Sozialgesetzbuch sowie anderer Vorschriften über den Datenschutz verantwortlich. Dies verpflichtet ihn nach § 80 Abs. 2 Satz 3 SGB X, dem Auftragnehmer erforderlichenfalls Weisungen zur Ergänzung von technischen und organisatorischen Maßnahmen zur Gewährleistung der Datensicherheit zu erteilen. Diese sind bei Auftragserteilung *festzulegen*.
  Dazu ist ein Auftraggeber jedoch nur in der Lage, wenn er die Sicherheitsmaßnahmen des Auftragnehmers kennt. Notwendiger Vertragsbestandteil muß deshalb ein Sicherheitskonzept für Auftragnehmer und Unterauftragnehmer sein. Der darin beschriebene Standard ist vertraglich zu garantieren. Außerdem hat sich der Auftragnehmer zu verpflichten, Weisungen des Auftraggebers zur Ergänzung der vorhandenen technischen und organisatorischen Datensicherheitsmaßnahmen umzusetzen und bei den Unterauftragnehmern das Erforderliche zur Umsetzung zu veranlassen.
  Die mir zuvor auf Anforderung als Sicherheitskonzept vorgelegte "Sicherheitsrichtlinie" habe ich nicht akzeptiert, weil sie lediglich ein Soll-Konzept war, dessen Maßnahmen noch nicht realisiert waren.

- Bereits bei Vertragsabschluß sind etwaige Unterauftragsverhältnisse festzulegen (§ 80 Abs. 2 Satz 2 SGB X).

- Bei der Verarbeitung von Sozialdaten sind sowohl Auftraggeber als auch Auftragnehmer verpflichtet, ein Dateien- und Geräteverzeichnis nach den landesrechtlichen Vorschriften, also § 10 SächsDSG, zu führen. Dies ergibt sich für den Auftraggeber aus § 81 Abs. 2 und 4 SGB X, für den Auftraggeber aus § 80 Abs. 6 Satz 5 SGB X. Die Wohngeldstellen können ihr Verzeichnis nur vervollständigen, wenn ihnen die Zweckverbände die notwendigen Angaben zur Verfügung stellen und die Aktualität garantieren, indem sie Änderungen unaufgefordert mitteilen. Dies ist vertraglich zu vereinbaren.

- Die Aufbewahrungsdauer für Daten *abgeschlossener* Wohngeldfälle, die Auftragnehmer oder Unterauftragnehmer zuvor verarbeitet haben, sind festzulegen.

Ohne meinen Hinweis wären zudem die nach § 80 Abs. 3 SGB X erforderlichen Anzeigen bei den zuständigen Aufsichtsbehörden unterblieben.
In einer gemeinsamen Besprechung zwischen den Zweckverbänden, dem SMI und mir wurde vereinbart, die aufgezeigten Mängel durch Zusatzvereinbarungen zu den bestehenden Verträgen zu beseitigen und ein aussagefähiges Sicherheitskonzept zu

erstellen.

Für mich bleibt es problematisch, die Zweckverbände als Auftragnehmer anzusehen, weil die wesentlichen Leistungen von dritter Seite erbracht werden (z. B. die automatisierte Datenverarbeitung durch ein externes Rechenzentrum, Verteilung und Transport der Druckergebnisse durch Privatunternehmen). Ihre Tätigkeit reduziert sich auf eine Beraterfunktion. Ich habe die Zweckverbände letztlich deshalb als Auftragnehmer angesehen, weil sie den Wohngeldstellen die Datenverarbeitung der Wohngeldfälle vertragsgemäß schulden. Insofern sind das externe Rechenzentrum sowie alle von diesem oder einem Zweckverband beauftragten Dienstleister Unterauftragnehmer.

(Zur Auftragsdatenverarbeitung im BAföG-Bereich unten 10.2.13).

10.2.7 Vorlage des Steuerbescheids bei einem Wohngeldantrag

Ein Petent, der ein Gewerbe betreibt, fragte nach der Berechtigung der Wohngeldstellen, den Einkommensteuerbescheid für das zurückliegende Jahr 1994 zu verlangen, obwohl er Wohngeldleistungen erst ab Mai 1995 beantragt hatte, weil sich seit diesem Zeitpunkt seine geschäftliche Situation erheblich verschlechtert hatte.

Ich habe ihm mitgeteilt, daß ein Steuerbescheid keine geeignete Grundlage für die Ermittlung des Jahreseinkommens nach den Vorschriften des WoGSoG ist, weil sich die einkommensteuerliche und wohngeldrechtliche Ermittlung der Einkünfte grundlegend voneinander unterscheiden. Die steuerlichen Einkünfte werden nach den komplexen und in ihrer Anwendung umfangreiches Fachwissen voraussetzenden §§ 3 bis 23 des Einkommensteuergesetzes ermittelt. Dagegen werden die Einkünfte nach § 10 WoGSoG pauschal berechnet, indem von den *zu erwartenden Einnahmen* ein bestimmter Prozentsatz abgezogen wird - nämlich 25 v. H. der Einnahmen aus nichtselbständiger Arbeit und 6,5 v. H. der Einnahmen aus anderen Einkunftsarten. Auch wenn die Bezeichnung der Einkunftsarten in § 9 WoGSoG mit der steuerlichen übereinstimmt, ist das nicht mehr als eine identische Terminologie bei der Aufzählung der für Wohngeldzwecke maßgebenden Einkunftsquellen. Eine Verbindung zum Steuerrecht läßt sich daraus nicht ableiten.

Dagegen kann die Wohngeldstelle eine Erklärung der *zu erwartenden Einnahmen* und ggf. entsprechende Nachweise verlangen, wobei die Einnahmen zu erwarten sind, "die auf der Grundlage der im Zeitpunkt der Antragstellung bekannten Daten verläßlich ermittelt werden können" (§ 10 Abs. 1 WoGSoG). Bei Arbeitnehmern reicht eine aktuelle Gehaltsbescheinigung, bei Selbständigen eine Bestätigung des Steuerberaters über Umsätze (soweit sie den Einnahmen entsprechen) oder ein Auszug aus einer vorläufigen Gewinn- und Verlustrechnung. Maßgebend sind stets die Verhältnisse im Bewilligungszeitraum. Und dieser liegt stets in der Zukunft, weil das Wohngeld (längstens für ein Jahr) im voraus bewilligt wird.

Die Eingabe war für mich Anlaß, beim SMI auf eine Änderung des Wohngeldantrags (Mietzuschuß) hinzuwirken. Künftig werden keine *bestimmten* Nachweise mehr verlangt. Dem Antragsteller wird freigestellt, durch welche Unterlagen er seine Angaben belegt.

10.2.8 Antrag auf Eingliederungshilfe für ein körperbehindertes Kind

Ein Elternpaar sah es als unverhältnismäßig an, einen eng bedruckten, sechs Seiten umfassenden Sozialhilfeantrag für die Unterbringung seines gehörlosen Kindes in einer Schule für Gehörlose mit Ganztagsbetreuung auszufüllen. Hierbei handelt es sich um eine teilstationäre Maßnahme, die als erweiterte Form der Hilfe nach § 43 Abs. 2 BSHG gewährt wird, wobei die Eltern nur für die Kosten des Lebensunterhalts aufzukommen haben. Obwohl als Kostenpauschale lediglich 2,- DM pro Tag für das eingesparte häusliche Mittagessen zu entrichten waren, sah der Antrag detaillierte Angaben zu den persönlichen Verhältnissen der Eltern, ihren Einkommens- und Vermögensverhältnissen sowie der des Kindes und auch Dritter vor.

Auf meine Initiative hin hat der Sozialhilfeträger einen erheblich gekürzten Antrag erarbeitet und mit mir abgestimmt. Er besteht nunmehr aus zwei Teilen. Der erste umfaßt den eigentlichen Antrag, der zweite Angaben zur Familie und zum Einkommen. Den zweiten Teil brauchen die Eltern nur auszufüllen, wenn sie erklären, den Kostenbeitrag nicht aufbringen zu können. Alle Fragen zum Vermögen wurden gestrichen, da es für diese Art der Hilfe nicht eingesetzt werden muß.

Folgende Punkte der zur Frage der Erforderlichkeit von Angaben geführten Diskussion möchte ich hervorheben:

Geburtsort/Kreis des Hilfesuchenden und seiner Eltern - nicht erforderlich

Der Sozialhilfeträger meinte, ein Geburtsort außerhalb Deutschlands sei ein möglicher Hinweis auf einen Übertritt aus dem Ausland, Abweichungen zwischen Geburts- und Wohnort innerhalb Deutschland könnten dagegen auf einen Zuzug aus dem Bereich eines anderen Sozialhilfeträgers hindeuten. In beiden Fällen hätten andere Sozialhilfeträger dem jetzigen Sozialhilfeträger die für die Hilfe aufgewendeten Kosten zu erstatten (§§ 107, 108 BSHG).
Es wurde Übereinstimmung erzielt, daß der Geburtsort ein für diese Zwecke ungeeignetes Kriterium ist und allein die vorangegangenen Aufenthaltsverhältnisse des Hilfesuchenden maßgebend sind.

Staatsangehörigkeit des Hilfesuchenden - erforderlich, die der Eltern - nicht erforderlich

Sozialhilfe wird uneingeschränkt nur Deutschen und Gleichgestellten gewährt. Insofern ist die Staatsangehörigkeit entscheidungsrelevant, allerdings nur die des Hilfesuchenden und nicht - wie ursprünglich vorgesehen - die der Eltern.

Krankenversicherung des Hilfesuchenden und seiner Eltern - nicht erforderlich

Statt des Namens der Krankenkasse ist nur die Tatsache der Krankenversicherung zur Prüfung der (Vor-)Leistungspflicht des Sozialhilfeträgers für benötigte Hilfsmittel von Bedeutung. Nunmehr ist nur noch die Frage "krankenversichert" mit den Antworten "ja" oder "nein" vorgesehen, und auch nur für den Hilfesuchenden.

Beamtenverhältnis von Vater und Mutter - erforderlich

Unabhängig vom tatsächlichen Bestehen einer privaten Krankenversicherung haben Beamtenkinder nach Beihilferecht stets Anspruch auf eine heilpädagogische Behandlung. Die Frage dient der Überleitung von Beihilfeansprüchen.

Aufenthaltsverhältnisse des Hilfesuchenden - nur mit zeitlicher Begrenzung erforderlich

Es ist nicht erforderlich, die Aufenthaltsverhältnisse vor der Antragstellung ohne zeitliche Begrenzung zu erfragen. Da es für die Kostenerstattung durch einen anderen Träger (§§ 107, 108 BSHG) nur auf die Verhältnisse des letzten Monats ankommt, wurde dies im Antragsformular entsprechend berücksichtigt.

Name der Versicherung, wenn ein Unfall die Behinderung verursacht hat - erforderlich

Bei einem Unfall geht der Anspruch kraft Gesetzes auf den Sozialhilfeträger über (§ 116 SGB X). In diesen Fällen macht der Sozialhilfeträger die von ihm aufgewendeten Kosten für die Hilfe unmittelbar bei der angegebenen Versicherung geltend.

Familien- und Einkommensverhältnisse der Personen, die mit dem Hilfesuchenden und seinen Eltern in häuslicher Gemeinschaft leben - erforderlich

Die Fragen dienen der Feststellung, ob den Eltern ein gesetzlich garantierter Mindestbetrag verbleibt, wenn sie den Kostenbeitrag entrichten, und sind nur zu beantworten, wenn sie eine Kostenbeteiligung ablehnen (s. o.). Der Mindestbetrag erhöht sich, wenn im Haushalt Personen mit Unterhaltsansprüchen gegen die Eltern des Hilfesuchenden leben (§ 79 BSHG). Aus *Verwandtschaftsgrad, Familienstand* und *Nettoeinkünften* der angegebenen Personen lassen sich Unterhaltsverpflichtungen bzw. Unterhaltsberechtigungen ableiten. Die *Berufsangabe* ist dagegen ebensowenig erforderlich wie die *Anschrift des Arbeitgebers*.

10.2.9 Antrag auf Eingliederungshilfe für seelisch behinderte Kinder und Jugendliche

Kinder und Jugendliche, die seelisch behindert oder von einer solchen Behinderung

bedroht sind, haben Anspruch auf Eingliederungshilfe. Die Hilfe ist beim Jugendamt zu beantragen und wird bedarfsgerecht in ambulanter Form, in Kindertageseinrichtungen oder anderen teilstationären Einrichtungen gewährt. Auch Pflegepersonen, Heime oder betreute Wohnformen kommen in Betracht. An den Kosten haben sich der Betroffene und dessen Eltern zu beteiligen.

Das Jugendamt einer größeren Stadt übersandte mir das neu erarbeitete Antragsformular zur datenschutzrechtlichen Beurteilung. Offenbar handelte es sich dabei nur um den "Grundantrag", denn Angaben zu Vermögens- und Einkommensverhältnissen wurden nicht gefordert, obwohl sie zur Feststellung der Kostenbeteiligung benötigt werden. Da Einkommens- und Vermögensverhältnisse vermutlich separat erhoben werden, habe ich für eine datenschutzrechtliche Gesamtbeurteilung den betreffenden Vordruck angefordert. Noch liegt er mir nicht vor.

Aus der Diskussion um die Erforderlichkeit einiger Angaben greife ich folgende heraus:

- Angaben zum *Geburtsort* und zur *Staatsangehörigkeit* des Betroffenen scheinen mir nicht erforderlich zu sein.

- Nach Auskunft des Jugendamtes wird der Name der *Krankenkasse* für eine eventuelle Notfallbehandlung erhoben. Diese Begründung kann die Datenerhebung nicht rechtfertigen, weil ein Notfall glücklicherweise ein seltenes Ereignis ist und Ärzte zur Notfallbehandlung verpflichtet sind. Die vom Arzt benötigten Angaben können nachgereicht werden. Zudem besteht die Gefahr, daß durch einen - in Zukunft häufigeren - Wechsel der Krankenkasse die erhobenen Daten nicht aktuell sind.
  Auch das Argument, das Jugendamt habe für ein nicht (familien-)versichertes Kind Krankenhilfe zu leisten, hat mich nicht überzeugt: Gesetzlich wird Krankenhilfe nur bei Inanspruchnahme einer Pflegeperson oder eines Heimplatzes gewährt. Da Krankenhilfe bei anderen Formen der Eingliederungshilfe nicht in Betracht kommt, habe ich eine entsprechende Differenzierung gefordert.

- Der Fragenkomplex zu "*Personalien der Eltern bzw. der/des Sorgeberechtigten*" war überarbeitungsbedürftig, weil die geforderten Angaben keinen Sinn ergeben hätten, wenn der Antrag von Sorgeberechtigten gestellt worden wäre, die nicht die Eltern sind (z. B. Krankenkasse und Geburtsdatum des Vormunds). Da mit den Fragen lediglich eine Kontaktadresse für den Schriftverkehr und eine Telefonnummer für Rückfragen sowie die Kostenbeitragspflichtigen festgestellt werden sollen, muß dies in der Vordruckgestaltung klar zum Ausdruck kommen.

- Das Jugendamt hält es für notwendig, Daten zur *Arbeitsstelle der Eltern* im Hinblick auf eine eventuelle Zwangsvollstreckung zu erfragen. Dem habe ich widersprochen. Die Angabe darf erst im Zusammenhang mit konkreten Vollstreckungsmaßnahmen gefordert werden; ob sie dann beantwortet werden muß, lasse ich hier offen.
- Die Angabe eines *Adoptivkindschaftsverhältnisses* habe ich als rechtswidrig

angesehen, weil sie mit dem Adoptionsgeheimnis nach § 1758 BGB unvereinbar ist.

- Auch die *Angabe von Geschwistern* in Kindertageseinrichtungen ist nur von Bedeutung, wenn die Eingliederungshilfe für einen Platz in einer Tageseinrichtung beansprucht wird, weil dann eine Beitragsminderung geltend gemacht werden kann. Ich habe einen entsprechenden Hinweis im Antrag angeregt.

- Gegen die Vorlage des *amtsärztlichen Gutachtens* habe ich keine datenschutzrechtlichen Bedenken erhoben. Ich habe jedoch gebeten, sicherzustellen, daß das Gutachten innerhalb des Jugendamtes nur an die Stellen weitergegeben wird, die das Gutachten als Entscheidungsgrundlage benötigen.

10.2.10 Bescheinigung für Zwecke der Arbeitsbefreiung bei Erkrankung von Kindern

Bei Erkrankung eines Kindes haben Beschäftigte im öffentlichen Dienst für eine bestimmte Anzahl von Tagen Anspruch auf Freistellung vom Dienst. Arbeiter und Angestellte erhalten in dieser Zeit statt der Monatsbezüge Krankengeld von ihrer Krankenkasse. Für diese Zwecke stellt der Arzt eine Bescheinigung nach einem vorgeschriebenen Muster aus. Dazu wurde mir folgendes Problem vorgetragen:

Auf der Bescheinigung ist u. a. die Diagnose anzugeben. Da für den Arbeitgeber keine gesonderte Bescheinigung vorgesehen ist, legen die Beschäftigten der Personalstelle das Original vor. Davon wird eine Kopie für die Personalakte als Nachweis für die Freistellung gefertigt, eine weitere Kopie erhält das Landesamt für Finanzen zur Änderung der Bezüge.

Wie sich herausstellte, hätten die Ärzte bereits ab 1. Januar 1995 die Bescheinigung nach einem neuen Muster ausstellen müssen, das keine Angabe zur Diagnose mehr enthält. Auf meine Bitte hin hat die Kassenärztliche Vereinigung Sachsens (KVS) die sächsischen Vertragsärzte darüber informiert, daß Altbestände der Vordrucke nicht mehr verwendet werden dürfen.

Doch auch der geänderte Vordruck ist noch keine optimale Lösung. Sein grundlegender Mangel besteht darin, daß er auf die Belange der Krankenkassen zugeschnitten ist und im Gegensatz zur Arbeitsunfähigkeitsbescheinigung des Beschäftigten keine Durchschrift für den Arbeitgeber vorsieht. Bei Vorlage der Originalbescheinigung erhält dieser somit zwangsläufig Kenntnis von Daten, die er nicht benötigt. Die von mir dazu angeregten Vordruckkorrekturen sind nur durch Änderung der "Vordruckvereinbarung" auf Spitzenverbandsebene möglich. Dankenswerterweise unterstützt die KVS bei der Kassenärztlichen Bundesvereinigung mein Anliegen. Das Ergebnis bleibt abzuwarten. Deshalb habe ich es begrüßt, daß die KVS den Ärzten als Zwischenlösung die Ausfertigung eines Attests empfohlen hat, das nur die für den Arbeitgeber relevanten Daten enthält.

10.2.11 Angabe ausländischen Einkommens und Vermögens bei Anträgen auf Sozialhilfe

Ein Petent hatte nach § 11 Abs. 1 BSHG Hilfe zum Lebensunterhalt beantragt, die demjenigen gewährt wird, der seinen notwendigen Lebensunterhalt nicht oder nicht ausreichend aus eigenen Kräften und Mitteln, vor allem aus eigenem *Einkommen* und *Vermögen*, beschaffen kann. Als das Sozialamt im Zuge der Antragsbearbeitung "firmeninterne Zahlen" über das ausländische Unternehmen des Petenten verlangte, bat er mich um Auskunft über die Rechtmäßigkeit. Dazu habe ich ihm mitgeteilt:

§ 76 Abs. 1 BSHG in Verbindung mit § 1 der Verordnung zur Durchführung des § 76 BSHG besagt, daß zum Einkommen *alle* Einkünfte in Geld oder Geldeswert gehören, ohne Rücksicht auf ihre Herkunft und Rechtsnatur sowie ohne Rücksicht darauf, ob sie zu den Einkunftsarten im Sinne des Einkommensteuergesetzes gehören und ob sie der Steuerpflicht unterliegen. Folglich sind auch im Ausland oder durch im Ausland ansässige Unternehmen erzielte Einkünfte in die Einkommensermittlung einzubeziehen. Entsprechendes gilt für das Vermögen, da nach § 88 Abs. 1 BSHG zum Vermögen das *gesamte* verwertbare Vermögen gehört, also grundsätzlich auch der Wert eines ausländischen Unternehmens.

Zur Feststellung des Einkommens und Vermögens darf das Sozialamt nach § 67 a SGB X beim Betroffenem die Daten erheben, deren Kenntnis zur Aufgabenerfüllung erforderlich ist. Dies können durchaus "firmeninterne Zahlen" sein, z. B. Bilanzen sowie Gewinn- und Verlustrechnungen.

10.2.12 Befreiung von der Rundfunkgebührenpflicht

Gemäß § 6 Abs. 1 des Rundfunkgebührenstaatsvertrags können die Landesregierungen durch Rechtsverordnung die Voraussetzungen für die Befreiung von der Rundfunkgebührenpflicht u. a. aus sozialen Gründen bestimmen. Das Nähere regelt auf dieser Grundlage die "Verordnung der Sächsischen Staatsregierung über die Voraussetzungen für die Befreiung von der Rundfunkgebührenpflicht (Rundfunkgebührenbefreiungsverordnung)". Ähnliche Befreiungsverordnungen bestehen in den anderen Bundesländern. Auf Antrag werden u. a. Empfänger von Hilfe zur Pflege und von laufender Hilfe zum Lebensunterhalt nach dem Bundessozialhilfegesetz von der Rundfunkgebührenpflicht befreit.

Der Antrag ist gemäß § 5 Abs. 2 der Rundfunkgebührenbefreiungsverordnung beim örtlichen Träger der Sozialhilfe zu stellen. Über den Antrag entscheidet jedoch nicht das Sozialamt, sondern die Rundfunkanstalt auf dessen Vorschlag. Sie kann das Sozialamt allerdings "zur Aushändigung des Bescheids ermächtigen".

Der Mitteldeutsche Rundfunk (MDR) hat den Sozialämtern diese Ermächtigung erteilt.

Sie entscheiden über den Antrag und händigen, wenn sie einen Anspruch auf Gebührenbefreiung bejahen, den Bescheid auf dem bundesweit einheitlichen Vordruck 7410 aus und senden jeweils eine Durchschrift an die Gebühreneinzugszentrale (GEZ) und den MDR. Allerdings übergeben die Sozialämter zusätzlich noch die Antragsunterlagen zur Prüfung an den MDR. Wenn er zu der Auffassung gelangt, daß kein Anspruch auf Befreiung besteht, hebt er den Bescheid auf. Nach Auskunft des MDR betrifft dies ungefähr 2 % der Befreiungen.
Die Ablehnung des Antrags erfolgt nicht durch das Sozialamt, sondern durch den MDR, der auch in diesem Falle alle Antragsunterlagen erhält.

Dieses Verfahren gilt für die meisten Rundfunkanstalten. Es wirft jedoch eine Reihe von Fragen auf.

Das Sozialamt erhebt und verarbeitet personenbezogene Daten, ohne für die Entscheidung zuständig zu sein. Andererseits händigt es den "Bescheid des MDR" aus, ohne daß dieser den Vorgang auch nur zur Kenntnis genommen hat, und der den Bescheid anschließend, wenn er anderer Auffassung ist als das Sozialamt, wieder aufhebt. Abgesehen von allgemeinen verfahrensrechtlichen Problemen (Rücknahmevoraussetzungen nach § 48 Abs. 2 VwVfG; Formgültigkeit des "Bescheids" gemäß § 37 Abs. 3 VwVfG) ist einzuwenden, daß zwei Stellen zum Teil sensible Daten wie Angaben zu Behinderungen und zu Einkommensverhältnissen verarbeiten, obwohl die Beteiligung von zwei Stellen nicht zwingend geboten ist. Daher haben die Landesbeauftragten für den Datenschutz von Sachsen-Anhalt, Thüringen und Sachsen die jeweils zuständige Staatskanzlei zu einer Änderung des Verfahrens aufgerufen. § 6 Abs. 4 Rundfunkgebührenstaatsvertrag eröffnet nämlich die Möglichkeit, daß eine andere Behörde als die Rundfunkanstalt über den Antrag entscheidet. In diesem Falle ist durch Rechtsverordnung auch zu bestimmen, welche personenbezogenen Daten die für die Entscheidung zuständige Stelle an die Landesrundfunkanstalt zu übermitteln hat. Bei einer solchen Novellierung der Rundfunkgebührenbefreiungsverordnungen bieten sich die Sozialämter als bürgernahe Entscheidungsträger an. Eine doppelte Datenverarbeitung wird vermieden. Die Vereinfachung des Verfahrens entspricht dem verfassungsrechtlichen Gebot der Transparenz gegenüber dem Antragsteller, der die bisher praktizierte Zusammenarbeit zwischen Sozialamt, MDR, zusätzlich GEZ, die den Charakter eines Verwirrspiels aufweist, nicht durchschauen kann.
Eine abschließende Antwort der Sächsischen Staatskanzlei ist bisher nicht erfolgt; eine Änderung des Verfahrens ist allerdings auch nur mittelfristig zu erreichen, weil sie eine Änderung der für die Bundesländer geltenden jeweiligen Befreiungsverordnungen voraussetzt. Sie muß einheitlich erfolgen, weil die Befreiungsverordnungen gemäß § 6 Abs. 2 Rundfunkgebührenstaatsvertrag übereinstimmen sollen.
Die weiteren Überlegungen haben daher von der geltenden Rechtslage auszugehen.
Fraglich ist schon, ob das Sozialamt, wenn es Daten an die Rundfunkanstalt übermittelt, die §§ 67 ff. SGB X oder das Sächsische Datenschutzgesetz anzuwenden hat. Der MDR versicherte mir, daß die Sozialämter nicht Daten verwenden, die sie bei der Ausführung des Bundessozialhilfegesetzes (oder anderer Sozialleistungsgesetze)

erhoben und verarbeitet haben, sondern nur Unterlagen nutzen, die der Betroffene zur Begründung seines Antrags auf Gebührenbefreiung vorgelegt hat. Dennoch ist eine zweckwidrige Nutzung wohl nicht auszuschließen, wenn, wie zumindest teilweise Praxis, sowohl die Sozialleistungen als auch die Gebührenbefreiung von derselben Person bearbeitet werden.

Sozialdaten sind gemäß § 67 Abs. 1 Satz 1 SGB X Einzelangaben über persönliche und sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person, die von den in § 35 SGB I genannten Stellen (dazu gehören die Sozialämter) im Hinblick auf ihre Aufgaben nach dem Sozialgesetzbuch erhoben, verarbeitet oder genutzt werden. Die Rundgebührenbefreiungsverordnungen sind nicht Teil des Sozialgesetzbuches, so daß es sich danach bei den Daten der Antragsteller nicht um Sozialdaten handelt. Die Definition in § 67 Abs. 1 SGB X wird jedoch erweitert durch § 67 Abs. 2 Nr. 4 SGB X. Aufgaben nach dem Sozialgesetzbuch sind auch Aufgaben, die den in § 35 SGB I genannten Stellen durch Gesetz zugewiesen sind.

Die Aufgabenzuweisung an die Sozialämter erfolgt durch § 5 Abs. 2 Rundfunkgebührenbefreiungsverordnung, also durch eine Rechtsverordnung. Die Aufgabenzuweisung durch eine Rechtsverordnung ist - nach meiner Auffassung abschließend - geregelt in § 67 Abs. 2 Nr. 1 SGB X, der sich auf Verordnungen bezieht, deren Ermächtigungsgrundlage sich im Sozialgesetzbuch befindet. Die hier einschlägige Ermächtigungsgrundlage, § 6 Abs. 1 Rundfunkgebührenstaatsvertrag in Verbindung mit den dazu ergangenen Landesgesetzen, ist jedoch kein Teil des Sozialgesetzbuchs.

Nach meiner Auffassung greift daher das Sozialgesetzbuch Zehntes Buch nicht ein. Hingegen läßt das Bundesministerium für Arbeit und Sozialordnung, das auf meine Anregung vom Bundesbeauftragten für den Datenschutz um Auslegung der Vorschrift gebeten wurde, eine (Landes-)Rechtsverordnung ausreichen. Die Diskussion zu dieser Frage ist noch nicht abgeschlossen. (Zur Auslegung von § 67 Abs. 2 Nr. 4 SGB X auch vorstehend Abschnitt 10.2.3).
Fraglich ist weiterhin, ob das Sozialamt Daten im Auftrag des MDR verarbeitet.
Nach meiner Auffassung ist dies zu bejahen, weil nicht das Sozialamt, sondern der MDR über den Antrag entscheidet. Das Sozialamt tritt gegenüber dem Antragsteller auch nicht als Behörde auf, die den Verwaltungsakt erläßt, sondern, wie lit. c des Formulars 7410 zu entnehmen ist, als Stelle, die den Bescheid aushändigt oder absendet (dieses Verfahren ist allerdings, wie oben ausgeführt, für den Antragsteller kaum zu durchschauen).
In Betracht kommt auch, daß wegen der weitreichenden Prüfungsbefugnisse des Sozialamts nicht nur eine Auftragsdatenverarbeitung, sondern sogar eine Funktionsübertragung anzunehmen ist.
Zu klären ist weiterhin eine ganze Reihe von Detailproblemen. So verlangt der MDR Nachweise für eine Befreiung, gemäß § 5 Abs. 4 Satz 1 Befreiungsverordnung muß der Antragsteller die Voraussetzungen jedoch nur "glaubhaft" machen. Glaubhaft machen bedeutet nach allgemeiner Auffassung, daß eine überwiegende Wahrscheinlichkeit

bestehen muß, während der Nachweis eine an Sicherheit grenzende Wahrscheinlichkeit verlangt. Daher muß dem Betroffenen zugestanden werden, seinen Antrag auch auf andere Unterlagen als solche, die einen Nachweis ermöglichen, zu stützen. Es ist daher zu prüfen, welche Unterlagen in Betracht kommen.

Noch keine ausreichende Antwort habe ich vom MDR auf die Frage nach der Beteiligung der GEZ erhalten. Sie erhält, wie ausgeführt, bei Befreiung eine Durchschrift des Bescheids. In der "Information für Mitarbeiter der Sozialbehörden", die die GEZ den Sozialämtern übergeben hat, wird jedoch ausgeführt, die GEZ nehme eine inhaltliche Prüfung vor. So werden etwa alle Befreiungsbescheide mit unlogischen Daten der zuständigen Sozialbehörde zur Prüfung zurückgesandt. In dieser Information heißt es auch: "Die Daten des Antrags auf Befreiung von der Rundfunkgebührenpflicht werden online erfaßt". Fraglich ist, zwischen wem eine Online-Verbindung besteht.

Problematisch ist, wie auch vom MDR eingeräumt wird, die Datenerhebung bei Dritten. Auf dem Antragsformular ist die Möglichkeit vorgesehen, daß nicht der Antragsteller, sondern sein Ehegatte zu den Personen gehört, die gemäß § 1 Abs. 2 Nr. 2 Befreiungsverordnung von der Rundfunkgebührenpflicht befreit werden. Der Antragsteller gibt in diesen Fällen an, daß der Ehegatte zum berechtigten Personenkreis gehört. Das kann dazu führen, daß er dem Sozialamt und dem MDR ohne Wissen oder sogar gegen den Willen des Ehegatten mitteilt, daß dieser hörgeschädigt oder wesentlich sehbehindert ist oder über ein geringes Einkommen im Sinne von § 1 Abs. 1 Satz 1 Nr. 7 Befreiungsverordnung verfügt. Weiterhin bestehen Einwände gegen einige Angaben im Formular 7410.

Die Diskussion ist also auf der Grundlage des oben skizzierten Änderungsvorschlags fortzuführen.

10.2.13 Durchführung des automatisierten BAföG-Hauptverfahrens

Die Berechnung und Auszahlung von Leistungen nach dem Bundesausbildungsförderungsgesetz mußte bereits in der Aufbauphase der sächsischen Verwaltung gewährleistet werden. Deshalb hatte das SMWK ein Privatunternehmen mit der automatisierten Verarbeitung beauftragt. Der sächsischen Verwaltung fehlten damals Fachkräfte und Rechenkapazität, so daß es andernfalls zu "Störungen im Betriebsablauf" gekommen wäre. Damit waren die Voraussetzungen nach § 80 Abs. 5 SGB X a. F. zur Auftragsvergabe an einen Privaten erfüllt.

Inzwischen hat das SMWK das Verfahren geändert. Dabei habe ich es in Fragen einer datenschutzgerechten Neustrukturierung des Verfahrens sowie hinsichtlich der Anforderungen des § 80 SGB X beraten.

Die automatisierte Datenverarbeitung erfolgt jetzt im Statistischen Landesamt. Es pflegt und wartet die zur Verarbeitung notwendigen Programme, berät und betreut die

Anwender; für Programmvorgaben und -freigaben bleibt das SMWK verantwortlich. Das Statistische Landesamt erledigt insofern nicht nur statistische Aufgaben, so daß es gemäß § 3 Abs. 3 SächsStatG Maßnahmen zur räumlichen, organisatorischen und personellen Trennung zu treffen hat. Dies werde ich kontrollieren.

Allerdings habe ich Zweifel, ob nicht ein zentrales BAföG-Verfahren beim "Studenten-BAföG" das Recht der Studentenwerke auf Selbstverwaltung und beim "Schüler-BAföG" das Recht der Kommunen auf Selbstverwaltung beeinträchtigt (§ 40 Abs. 1 BAföG i. V. m. § 1 Abs. 2 Satz 1 Sächsisches Studentenwerksgesetz bzw. § 40 Abs. 2 BAföG). Denn die Organisationshoheit gehört zum Kernbereich der Selbstverwaltung, in das von dritter Seite auch nicht aufgrund eines Weisungsrechts im Zuge der übertragenen Aufgabe (§ 85 Abs. 3 SächsVerf) eingegriffen werden darf. Das SMWK hat in Aussicht gestellt, die jetzige zentrale Lösung mittelfristig durch eine dezentrale Verarbeitung zu ersetzen. Auch hier gilt: Dezentrale Verfahren sind eher datenschutzgerecht.

10.3 Lebensmittelüberwachung und Veterinärwesen

10.3.1 Lebensmittelüberwachung: Selbstvermarkter-Statistik des SMS

Auf die Kleine Anfrage eines Landtagsabgeordneten teilte die Staatsregierung mit, daß es in Sachsen insgesamt 111 Betriebe gebe, die Fleisch - und Wurstwaren selbst vermarkten. Einige Zeit später wandte sich das SMWA mit der Frage an mich, ob es datenschutzrechtlich zulässig sei, die Namen und Anschriften der offenbar beim SMS namentlich gespeicherten Selbstvermarkter zu Zwecken der Bekämpfung von Schwarzarbeit i. S. d. Gesetzes zur Bekämpfung von Schwarzarbeit übermittelt zu bekommen. Als Rechtsgrundlage hierfür, so das SMWA, komme § 13 SächsDSG in Betracht.

Dem SMWA habe ich folgendes mitgeteilt: § 13 Abs. 1 i. V. m. § 12 Abs. 2 Nr. 3 SächsDSG scheidet als Rechtsgrundlage für eine Übermittlung der Daten vom SMS an das SMWA aus, weil das SMWA bzw. sein nachgeordneter Bereich zur Verfolgung von Ordnungswidrigkeiten nach dem Gesetz zur Bekämpfung von Schwarzarbeit nicht zuständig ist, eine Übermittlung mithin zur Aufgabenerfüllung des SMWA oder seines nachgeordneten Geschäftsbereichs nicht erforderlich ist.

Zuständig für den Vollzug des Gesetzes zur Bekämpfung der Schwarzarbeit sind - mangels spezialgesetzlicher Zuweisungen - die Landratsämter und die Bürgermeisterämter der kreisfreien Städte "als untere Verwaltungsbehörden" gemäß § 2 OWiZuVO. Eine gesetzliche Zuständigkeit im Geschäftsbereich des SMWA, namentlich eine solche der Gewerbeaufsichtsämter, ist nicht ersichtlich. Rechtsaufsichtsbehörden für die zur Verfolgung von Ordnungswidrigkeiten nach dem Gesetz zur Bekämpfung der Schwarzarbeit zuständigen Behörden sind vielmehr die

Regierungspräsidien und das SMI (§ 112 Abs. 1 SächsGemO). Das SMWA ist insofern weder Vollzugs- noch Aufsichtsbehörde. Man mag das bedauern; es zu ändern wäre besser. Eine Übermittlung der im Geschäftsbereich des SMS namentlich bekannten 111 Betriebe wäre daher zur Aufgabenerfüllung des SMWA nicht erforderlich und damit unzulässig. Zulässig ist dagegen, daß die zuständigen Landratsämter und Bürgermeisterämter der kreisfreien Städte die Lebensmittelüberwachungs- und Veterinärämter gemäß § 13 Abs. 1 Nr. 2 i. V. m. § 12 Abs. 2 Nr. 3 SächsDSG um Übermittlung von Namen und Anschriften der im jeweiligen örtlichen Zuständigkeitsbereich bekannten Fleisch- und Wursterzeuger ersuchen.

Dem SMS habe ich mitgeteilt: Die Erhebung und zentrale Speicherung von Namen und Anschriften der landwirtschaftlichen Selbstvermarkter war zur Vorbereitung einer Antwort der Staatsregierung auf die Anfrage des Abgeordneten nicht erforderlich und deswegen rechtswidrig. Die Erhebung, Übermittlung und Speicherung diente nicht der Ausführung des SächsGDG oder des SächsAGLMBG, also der Erfüllung der Aufgaben des öffentlichen Gesundheitsdienstes oder der Lebensmittelüberwachung. Es hätte zur Erfüllung der vorbezeichneten Aufgabe ausgereicht, die instanziell zuständigen Behörden im Geschäftsbereich des SMS, hier die Lebensmittelüberwachungs- und Veterinärämter, anzuweisen, aggregierte Daten der in dem jeweiligen örtlichen Zuständigkeitsbereich bekannten Selbstvermarkter zu übermitteln; spezialgesetzliche Rechtsgrundlage hierfür ist § 7 Abs. 1 SächsStatG, wonach Statistiken auch ohne Rechtsvorschrift angeordnet werden dürfen, wenn sie ausschließlich der Erfüllung der Aufgaben der öffentlichen Stelle, in deren Geschäftsgang die Daten anfallen, oder der Aufgaben der jeweils übergeordneten öffentlichen Stelle, dienen. Diese Voraussetzungen wären erfüllt gewesen.

Das SMWA hat auf ein Übermittlungsersuchen verzichtet; das SMS hat die gespeicherten Daten der 111 Betriebe gelöscht.

10.3.2 Datenverarbeitung im Bereich der Sächsischen Landestierärztekammer

Eine sehr erfreuliche Entwicklung hat ein Vorgang im Bereich der Sächsischen Landestierärztekammer (SLTÄK) genommen, über den ich in meinem 3. Tätigkeitsbericht unter 10.3.1 berichtet habe. Meine seinerzeit geäußerte Kritik an der weitgehend zur Aufgabenerfüllung der SLTÄK nicht erforderlichen und daher rechtswidrigen Datenerhebung bei Sächsischen Tierärzten hat dazu geführt, daß das Tierärzte-Meldeverfahren neugestaltet und auf die rechtswidrige Übermittlung der erhobenen Daten an Dritte verzichtet wird. Erfreulicherweise wird das bundesweit bei den Tierärztekammern Schule machen.

Vorausgegangen war folgendes: Auf Nachfrage habe ich erfahren, daß das Planungs- und Informationszentrum (PIZ) der Tierärztlichen Hochschule Hannover (TIHO Hannover) in Zusammenarbeit mit der Bundestierärztekammer e. V. und den Tierärztekammern der Länder seit 1971 eine zentrale Tierärztedatei führt. In dieser

Datei wurden seitdem alle Mitglieder der Landes-Tierärztekammern gespeichert, "wobei laufend die von den Kammern gemeldeten beruflichen Veränderungen berücksichtigt werden" ("Die qualitative und quantitative Entwicklung des tierärztlichen Berufstandes", Schriftenreihe des BMJFFG, Band 155, 1986, S. 7). In der Tat übermittelte auch die SLTÄK sowohl die Daten aus dem Anmeldeverfahren eines Tierarztes als auch später eintretende Veränderungen an die TIHO Hannover, wobei man zu Unrecht den Vorgang als Datenverarbeitung im Auftrag verstanden wissen wollte. Weiter erfuhr ich, daß diese Tierärztedaten zur Durchführung einer (Privat-)Statistik durch die Bundestierärztekammer e. V., einen Verein zur Förderung der berufsständischen Interessen der Tierärzte im politischen Raum, verwendet wurden. Zur Datenerhebung im Anmeldeverfahren, also bei der erstmaligen Meldung von Daten von Tierärzten, verwandte die SLTÄK wie alle anderen 16 Tierärztekammern in Deutschland die von mir kritisierten Erhebungsbögen "Tierärztekammer-Meldebogen" und "Art der Tätigkeit".

Eine Rechtsgrundlage für die Erhebung, Speicherung und Übermittlung der insbesondere mit dem Erhebungsbogen "Art der Tätigkeit" erhobenen Daten war in Sachsen nicht vorhandenen. Die insofern in Betracht kommenden Vorschriften des SächsHKaG über das (An-)Meldeverfahren, die Meldeordnung und die zur Überwachung der Erfüllung der Berufspflichten erforderlichen Angaben und Nachweise erlaubten lediglich die Erhebung eines Teils der auf dem "Tierärztekammer-Meldebogen" anzugebenden Daten des Tierarztes. Das SächsHKaG stellt eine vorrangige und abschließende gesetzliche Regelung über die Datenverarbeitung durch die SLTÄK als Körperschaft des öffentlichen Rechts dar; die Verarbeitung von Daten, die im Anmeldeverfahren erhoben werden, konnte mithin nicht mehr auf die allgemeinen Vorschriften des Datenschutzgesetzes gestützt werden. Der Rest, insbesondere die ins Detail gehenden Fragen zur "Art der Tätigkeit" durften - wenn überhaupt - nur mit Einwilligung des betroffenen Tierarztes erhoben und (weiter-)verarbeitet werden. Ein Hinweis auf diese Freiwilligkeit fehlte jedoch in dem Erhebungsbogen "Art der Tätigkeit". Vielmehr wurde mit der gleichzeitigen Übersendung des "Tierärztekammer-Meldebogens", dem Stempeleindruck der SLTÄK und einem Hinweis in der Kopfzeile des betreffenden Erhebungsbogens bewußt der Eindruck erweckt, als handele es sich um (Pflicht-)Angaben zur Erfüllung einer gesetzlichen Aufgabe der SLTÄK.

Die SLTÄK hat mir nunmehr mitgeteilt, daß künftig alle deutsche Tierärztekammern auf die von mir bemängelte Übermittlung der Daten aus dem Erhebungsbogen "Art der Tätigkeit" und auf die Übermittlung einer Kopie des Tierärztekammer-Meldebogens verzichten wollen. Zukünftig wolle der BTÄK e. V. zusammen mit dem "Bund der praktizierenden Tierärzte" die bisher mit den genannten Erhebungsbögen erhobenen Daten auf freiwilliger Grundlage unmittelbar bei den Tierärzten erheben. Landestierärztekammern - und damit öffentliche Stellen - werden somit an dem Verfahren der Datenerhebung nicht mehr beteiligt. Die SLTÄK wolle zukünftig nur noch Namen und Anschrift des Tierarztes an das PIZ der TIHO Hannover und den BTÄK e. V. übermitteln, soweit der einzelne Tierarzt zugestimmt hat. Damit bin ich

einverstanden.

10.4 Rehabilitierungsgesetze

10.4.1 Übermittlung von Antragsteller-Daten durch nach § 25 StrRehaG zuständige Stellen an Rehabilitierungsbehörden nach dem BerRehaG

Wer Opfer einer freiheitsentziehenden Maßnahme geworden ist, die vom Strafrechtlichen Rehabilitierungsgesetz (1. SED-Unrechtsbereinigungsgesetz) erfaßt wird, hat häufig auch Ansprüche nach dem Beruflichen Rehabilitierungsgesetz (Teil des 2. SED-UnBerG).

Das SMS wollte den betreffenden Personenkreis über diese Ansprüche unterrichten und sich zu diesem Zwecke von der Entschädigungsstelle der Staatsanwaltschaft bei dem Oberlandesgericht Dresden Namen und Anschrift derjenigen übermitteln lassen, die dort einen Antrag auf Folgeleistungen nach dem StrRehaG (§§ 16 f., 25) gestellt hatten.

Das SMJus bat mich um Stellungnahme, ob datenschutzrechtliche Bedenken dagegen bestünden, daß die Entschädigungsstelle der Staatsanwaltschaft bei dem Oberlandesgericht Dresden dem Landesamt für Familie und Soziales einen Datenträger mit den entsprechenden Namen und Anschriften überläßt.

Bei meiner Antwort bin ich davon ausgegangen, daß im Sozialstaat die Unterrichtung von Anspruchsinhabern über die Presse sowie durch das Auslegen von Faltblättern in dafür in Frage kommenden öffentlichen Stellen geschieht. Hier liegt jedoch ein Sonderfall vor, weil rechtsstaatliche Pflichten die Rehabilitierung gebieten und der Staat eine Verpflichtung hat, in der Vergangenheit verübtes Unrecht heute zu erkennen und aktiv zu mildern.

Allerdings mußte ich einwenden, daß der in Frage kommende Personenkreis auch ohne die geplante Datenübermittlung unmittelbar von der nach § 25 Abs. 1 Satz 1 und 2 StrRehaG zuständigen Stelle, also der Entschädigungsstelle der Staatsanwaltschaft bei dem Oberlandesgericht Dresden, unterrichtet werden könnte. Die Übermittlung der Namen und Anschriften von der strafrechtlichen Rehabilitierungsbehörde an die Rehabilitierungsbehörde nach dem BerRehaG war daher nicht (in dem auch von der Übermittlungserlaubnis des § 25 a StrRehaG vorausgesetzten Sinne) erforderlich.

Das SMJus hat darauf erwidert, zur Erledigung dieser Aufgabe sehe sich die Entschädigungsstelle beim Generalstaatsanwalt des Freistaates Sachsen aus organisatorischen und personellen Gründen nicht in der Lage, weswegen die Daten doch an das Landesamt für Familie und Soziales übermittelt werden müßten.

Ich habe dem SMJus geantwortet, daß die Erforderlichkeit einer - in das Grundrecht auf

informationelle Selbstbestimmung eingreifenden - Datenübermittlung sich nur ganz ausnahmsweise nach den vorhandenen personellen Kapazitäten richten kann, daß vielmehr Personal eingesetzt werden müsse, damit eine dadurch ohne weiteres vermeidbare Datenübermittlung ohne Nachteil für die gebotene Aufgabenerledigung unterbleiben kann. Die Grundrechtsbindung gemäß Art. 1 Abs. 3 GG besteht schon bei organisatorischen Entscheidungen der Verwaltung.

Da lediglich eine Informations-Broschüre zu versenden war, bedurfte es keines hohen Aufwandes, vielmehr nur der Anwendung des sogenannten Adressmittlungsverfahrens in einer sehr einfachen Form. Die Ausweichlösung, den Anschriften-Ausdruck und den Versand von einem privaten Auftragnehmer gemäß § 7 SächsDSG durchführen zu lassen, schied wegen der besonderen Schutzbedürftigkeit der Daten aus: Immerhin handelte es sich um eine Datei sämtlicher Personen, die auf dem heutigen Gebiet des Freistaates Sachsen aus politischen Gründen einer rechtsstaatswidrigen Strafverfolgung durch das SED-Regime unterworfen waren (vgl. § 8 Abs. 1 Satz 1 i. V. m. § 25 Abs. 1 Satz 1 StrRehaG) und die auf dieser Grundlage einen Antrag nach dem StrRehaG oder dessen Vorgänger-Regelungen gestellt haben. Die Überlassung einer solchen Datei an einen Privatunternehmer hätte auch bei sorgfältiger Auswahl und Vertragsgestaltung ein zu großes Risiko mit sich gebracht.

10.4.2 Verlangen nach Einverständnis mit Einsichtnahme der Rehabilitierungsbehörde in die Unterlagen der Gauck-Behörde

Jemand, der durch Gerichtsentscheidung strafrechtlich rehabilitiert worden ist (vgl. §§ 1, 7 ff. StrRehaG) und dem auf dieser Grundlage auch von der dafür zuständigen Behörde (Entschädigungsstelle der Staatsanwaltschaft bei dem Oberlandesgericht Dresden) Haftentschädigung zugesprochen worden war (vgl. §§ 16 f., 25 StrRehaG), hatte zusätzlich Leistungen bei der Rehabilitierungsbehörde nach dem 2. SED-Unrechtsbereinigungsgesetz (verwaltungsrechtliche Rehabilitierung nach dem VwRehaG, berufliche Rehabilitierung nach dem BerRehaG) beantragt. In Sachsen ist die Erledigung dieser Aufgabe inzwischen bei dem Landesamt für Familie und Soziales in Chemnitz konzentriert.

Im Rahmen des daraufhin durchgeführten Verwaltungsverfahrens verlangte die Behörde von dem Betreffenden, ihr die Erlaubnis zu erteilen, Einsicht in die ihn betreffenden Unterlagen zu nehmen, welche der Bundesbeauftragte für die Unterlagen des Staatssicherheitsdienstes der ehemaligen Deutschen Demokratischen Republik nach dem StUG verwahrt.

Das wollte dem Betroffenen nicht einleuchten, konnte doch die Behörde bei ihrer Entscheidung auch ohne diese Einsichtnahme sich auf eine Fülle von Unterlagen stützen: Auf die im Zuge der strafrechtlichen Rehabilitierung herangezogenen und entstandenen Unterlagen, zusätzliche Zeugenaussagen und auch vom Antragsteller vorgelegte Ablichtungen von Unterlagen aus dem Bestand des BStU.

Ist die zusätzliche Datenerhebung, welche die Behörde zur Voraussetzung ihrer Entscheidung machen wollte, erforderlich und angemessen?

Soweit ich in Erfahrung gebracht habe, bittet die Behörde in weniger als fünf Prozent der Fälle die Antragsteller, das Einverständnis mit einer Erteilung einer Auskunft durch den BStU bzw. mit einer Einsichtnahme in die beim BStU vorhandenen Unterlagen zu erklären.
Dem liegt folgendes zugrunde: Nach allen drei Rehabilitierungsgesetzen (§ 16 Abs. 2 StrRehaG, § 2 Abs. 2 VwRehaG und § 4 BerRehaG) sind Ausgleichsleistungen bzw. Folgeansprüche dann ausgeschlossen, wenn der Berechtigte (Verfolgte) selbst gegen die Grundsätze der Menschlichkeit oder der Rechtsstaatlichkeit verstoßen oder aber eine Machtstellung schwerwiegend zum eigenen Vorteil oder zum Nachteil eines anderen mißbraucht hat (wofür auch die Zeit *vor* dem 8. Mai 1945 in Frage kommt). Praktisch bedeutet das: Wer Opfer einer entsprechenden Unrechtsmaßnahme war, kann deren Aufhebung, etwa auch in Gestalt einer strafrechtlichen Rehabilitierung, verlangen, er soll aber nicht in den Genuß finanzieller Folgeleistungen gelangen, wenn er selbst andererseits auch im Sinne der zitierten Formulierung als Täter in Erscheinung getreten ist. Die Rehabilitierungsbehörde hat von Amts wegen zu prüfen, ob derartige Ausschlußgründe für solch eine Ausgleichsleistung bzw. einen Folgeanspruch vorliegen.
Wie im 3. Tätigkeitsbericht unter 10.4 erläutert, bestehen keine datenschutzrechtlichen Bedenken dagegen, wenn die Behörde den Antragsteller - unter Hinweis auf die Freiwilligkeit der Beantwortung - nach Umständen fragt, die einen Anfangsverdacht begründen, daß einer der Ausschlußtatbestände erfüllt ist. Da eine Stichprobe ergeben hat, daß rund neun v. H. der Antragsteller nach dem Strafrechtlichen Rehabilitierungsgesetz aktenkundig für das MfS tätig gewesen sind, ist es die Pflicht und das Recht der Behörde, im Rahmen der Erforschung des Sachverhalts von Amts wegen dieser Möglichkeit nachzugehen, wenn sich ein Anfangsverdacht ergibt.
In folgenden Fällen sieht die Rehabilitierungsbehörde es als erforderlich an, vom Antragsteller die Einwilligung in eine Einsichtnahme in die Unterlagen des BStU zu erteilen:

- Wenn der Antragsteller selbst Unterlagen zur Begründung seines Antrages eingereicht hat, diese jedoch ersichtlich unvollständig sind und wenn zugleich der Antragsteller eine Berufstätigkeit im sicherheitsrelevanten Bereich ausgeübt hat,
- wenn der Antragsteller selbst die Vermutung geäußert hat, daß es Unterlagen bei der Gauck-Behörde geben müsse, oder wenn sich den Bediensteten aufgrund ihrer Erfahrung im Umgang mit Fällen dieser Art Anhaltspunkte aufdrängen, daß der Antragsteller für das MfS tätig gewesen sein könnte.

Gegen diese allgemeine Handhabung durch das Landesamt für Familie und Soziales bestehen in Anbetracht der Tatsache, daß die Anwendung der genannten Kriterien dazu führt, daß in weniger als fünf v. H. der Fälle von den Antragstellern die Einwilligung erbeten wird, keine datenschutzrechtlichen Bedenken.

11 Landwirtschaft, Ernährung und Forsten

11.1 Verdacht einer strafbaren Datenübermittlung aus dem SML an einen privaten Dritten: Zweiter Teil

Erhärtet hat sich mein im 3. Tätigkeitsbericht (11.2) geäußerter Verdacht einer gemäß § 203 Abs. 2 Satz 1 oder 2 StGB strafbaren unbefugten Offenbarung personenbezogener Einzelangaben aus dem SML an einen privaten Dritten. Nach Abschluß meiner eigenen Ermittlungen bin ich davon überzeugt, daß ein Bediensteter des SML im Frühjahr 1994 amtliche Daten über Landwirte an den Geschäftsführer einer großen landwirtschaftlichen Erzeugergemeinschaft, der ihm aus seiner jahrzehntelangen Tätigkeit in der DDR-Landwirtschaftsverwaltung persönlich bestens bekannt war, übermittelt hat und sich dabei im Interesse der Erzeugergemeinschaft bewußt und gewollt über seine Pflicht zur Amtsverschwiegenheit hinweggesetzt hat. Einigen Betroffenen ist dadurch ein nicht unbeträchtlicher wirtschaftlicher Schaden entstanden.

Meine Erkenntnisse habe ich der zuständigen Staatsanwaltschaft mitgeteilt, deren eigene Ermittlungen noch nicht abgeschlossen sind. Das SML habe ich gemäß § 26 SächsDSG förmlich beanstandet. Es hat mir daraufhin mitgeteilt, daß zukünftig vor Datenübermittlungen an Private der Datenschutzbeauftragte des SML zu beteiligen sei.

11.2 Überwachung der Betriebe des ökologischen Landbaus

Zu Beginn des Berichtszeitraums wurde die Verwaltungsvorschrift des SML zum Zulassungs- und Kontrollverfahren nach der EG-Verordnung Nr. 2092/91 über den ökologischen Landbau und die entsprechende Kennzeichnung der landwirtschaftlichen Erzeugnisse und Lebensmittel vom 7. April 1995 im Sächsischen Amtsblatt veröffentlicht (S. 572). Alle meine Anregungen zur datenschutzgerechten Gestaltung des Zulassungs- und Kontrollverfahrens, über die ich in meinem letzten Tätigkeitsbericht unter 11.4 berichtet habe, wurden berücksichtigt.

12 Umwelt und Landesentwicklung

12.1 Datenerhebung zur Vorbereitung der Einführung codierter Abfallbehälter

Durch einen Pressebericht wurde ich auf eine "heiß umkämpfte Fragebogenaktion" aufmerksam, mit der ein Landratsamt die Einführung eines mengenabhängigen Systems der Abfallentsorgung (mit Abfallbehältercodierung) vorbereitete, bei dem im Müllabfuhrfahrzeug auf einer Chipkarte die Kenn-Nummern gespeichert werden, die in einem kleinen elektronischen Bauelement (sogenannter Transponder) auf dem Müllbehälter enthalten sind und beim Leeren des Behälters gelesen werden. Dadurch wird es möglich, in der gesetzlich gebotenen Weise (vgl. 3. Tätigkeitsbericht unter 12.2) jedem Haushalt eine individuell errechnete Abfallgebühr zuzuordnen. Mit den Fragebögen beabsichtigte die Kreisverwaltung nun, bei den einzelnen Haushalten Angaben über die gewünschte Abfallbehältergröße und -anzahl, den gewünschten Entleerungsrhythmus und ggf. die Bildung einer "Behältergemeinschaft" zu erhalten. In einem Anschreiben bat der Landrat um die "konstruktive Mitarbeit" der Bürger beim Ausfüllen der Fragebögen.

Ich konnte daran im wesentlichen nichts Rechtswidriges entdecken: Die Datenerhebung war zur Ermittlung der für die einzelnen Haushalte individuell benötigten Abfallbehältergröße und des gewünschten Entleerungsrhythmus und somit zur Aufgabenerfüllung des Landkreises als entsorgungspflichtiger Körperschaft erforderlich. Statistikrechtliche Vorschriften mußten nicht beachtet werden, denn die erhobenen Daten sollten nicht aggregiert, sondern zum Verwaltungsvollzug im Einzelfall verwandt werden.

In zwei Punkten genügte die Fragebogenaktion nicht dem Datenschutzrecht: In dem Anschreiben des Landrats wurde entgegen § 11 Abs. 2 Satz 3 SächsDSG nicht auf eine evtl. vorhandene Auskunftspflicht, oder, falls eine solche nicht bestand, auf die Freiwilligkeit der Erhebung hingewiesen. Und bei der Frage nach den übrigen Mitgliedern einer "Behältergemeinschaft" fehlte es an den Voraussetzungen, unter denen gemäß § 11 Abs. 4 SächsDSG Daten über Dritte erhoben werden dürfen. Rechtmäßig konnte nur erhoben werden, ob der Befragte selbst Mitglied oder darüber hinaus sogenannter "Verantwortlicher" (Ansprechpartner) einer Behältergemeinschaft war.

Ich habe den Landkreis gebeten, diese Hinweise künftig zu beachten und insbesondere um eine geeignete Gestaltung der geplanten neuen Abfallwirtschaftssatzung bemüht zu sein.

12.2 Datenerhebung durch ehrenamtliche Naturschutzhelfer

Ein Landratsamt legte mir den Entwurf einer Bescheinigung vor, in der die Befugnisse ehrenamtlicher Naturschutzhelfer (§ 46 Abs. 1 SächsNatSchG) aufgeführt werden soll-

ten, zwecks Beobachtung von Natur und Landschaft personenbezogene Daten zu erheben. Danach sollten die ehrenamtlichen Naturschutzhelfer, von denen es in Sachsen ungefähr 1.500 gibt, u. a. berechtigt sein, bei den Grundstückseigentümern und -nutzern, aber auch bei allen anderen Personen, "die zur Vorbereitung und Durchführung der Naturschutzmaßnahmen notwendigen Auskünfte ... insbesondere zu Eigentums- und Nutzungsverhältnissen von Grundstücken" einzuholen.

Jede Befugnis zur Einholung von Auskünften bedarf als Datenerhebung einer gesetzlichen Grundlage (Art. 20 Abs. 3 GG - Grundsatz der Gesetzmäßigkeit der Verwaltung; Vorbehalt des Gesetzes). Eine solche war hier nicht vorhanden: Gemäß § 54 Abs. 2 Satz 1 SächsNatSchG sind neben den Bediensteten auch die *Beauftragten* der Naturschutzbehörden befugt, während der Tageszeit Grundstücke zu betreten und dort Bodenuntersuchungen, Vermessungen und ähnliche Dienstgeschäfte vorzunehmen. Das zusätzliche Recht, Auskünfte zu verlangen, wird dagegen in § 54 Abs. 1 Satz 1 SächsNatSchG nur den Naturschutzbehörden selbst sowie dem Polizeivollzugsdienst verliehen. Ehrenamtliche Naturschutzbeauftragte und Naturschutzhelfer sind aber gerade nicht Bedienstete der Naturschutzbehörden selbst, sondern üben unter deren Aufsicht ein Ehrenamt aus (§ 46 Abs. 1 Satz 1, Abs. 2 SächsNatSchG). Die unterschiedliche Ausgestaltung der Absätze 1 und 2 des § 54 SächsNatSchG bringt ganz deutlich zum Ausdruck, daß die ehrenamtlichen Naturschutzhelfer nicht von vornherein dieselben Befugnisse wie die Naturschutzbehörden haben. Ihre Befugnisse beschränken sich vielmehr, neben dem genannten Betretungsrecht, auf die in § 46 Abs. 3 SächsNatSchG beschriebene Art und Weise der Datenerhebung, insbesondere auf das Beobachten von Natur und Landschaft. Sie müssen sich daher auf die "Einnahme des Augenscheins" (vgl. § 26 Abs. 1 Nr. 4 VwVfG) beschränken. Auskünfte darf die Naturschutzbehörde nur selbst und unter den Voraussetzungen des § 54 Abs. 1 SächsNatSchG einholen.

Ein gesetzlich begründetes Recht zur Einholung von Auskünften ergibt sich auch nicht dadurch, daß man die ehrenamtlichen Naturschutzhelfer als sog. Verwaltungshelfer qualifiziert und sie dadurch mit den Befugnissen der Naturschutzbehörden ausstattet: § 54 Abs. 2 Satz 1 i. V. m. § 46 Abs. 3 SächsNatSchG regelt die Befugnisse der ehrenamtlichen Naturschutzbeauftragten abschließend; für eine ergänzende Anwendung der Grundsätze über Verwaltungshelfer ist kein Raum, sie wäre Gesetzesumgehung.

Das Landratsamt hat die ehrenamtlichen Naturschutzhelfer darüber zu belehren, daß sie keine Befugnisse haben, Auskünfte einzuholen.

Das betreffende Landratsamt hat seinen Vollmachts-Entwurf entsprechend geändert. Ich gehe davon aus, daß das SMU meine Rechtsauffassung respektiert.

13 Wissenschaft und Kunst

13.1 Hochschulgesetzgebung

Die Jahre 1993 und 1994 waren gekennzeichnet durch eine umfangreiche Tätigkeit des Gesetzgebers im Bereich des Hochschulrechts. An erster Stelle zu nennen ist das Sächsische Hochschulgesetz. In Kraft getreten sind auch z. B. das Sächsische Graduiertengesetz und das Sächsische Berufsakademiegesetz, zu denen ich jeweils Stellung genommen habe (2. Tätigkeitsbericht, unter 13.1, 13.2 und 13.7). Auch einige wichtige Rechtsverordnungen sind erlassen worden, etwa die auf § 135 Abs. 1 Satz 2 SHG beruhende Studentendatenverordnung (2. Tätigkeitsbericht, Nr. 13.4). Die Gesetzgebung ist damit im Bereich der Hochschulen weitgehend abgeschlossen. Der Schwerpunkt wird in Zukunft auf dem Erlaß der weiteren vom Sächsischen Hochschulgesetz vorgesehenen Rechtsverordnungen liegen.

13.2 Evaluation der Lehre

Im Hinblick auf die in § 14 SHG vorgeschriebenen Lehrberichte ermächtigt § 135 Abs. 3 Satz 2 SHG das SMWK, in einer Rechtsverordnung u. a. die Erhebungsmerkmale und das Erhebungsverfahren festzulegen, wenn *die Hochschulen* personenbezogene Daten des wissenschaftlichen und künstlerischen Personals zur Beurteilung der Lehrtätigkeit verarbeiten.

Bestandteil dieser Lehrberichte sind auch Befragungen der Studenten zur Qualität der Lehre und die Stellungnahme des Lehrkörpers zu den Ergebnissen der Befragung. In meinem 3. Tätigkeitsbericht habe ich mich (unter 1.5) kritisch mit diesem "Professoren-TÜV" auseinandergesetzt. Die Diskussion um Sinn und Unsinn solcher Studentenbefragungen ist an den Hochschulen lebhaft weitergeführt worden. So fand ein Kolloquium der TU Dresden statt, auf dem ich Gelegenheit hatte, meine Auffassung darzulegen.
Gegenüber dem SMWK habe ich erneut Stellung genommen.
Datenschutzrecht ist bei einer solchen Umfrage berührt, weil personenbezogene Daten der Lehrenden verarbeitet werden. Dabei ist von Bedeutung, ob die Befragung die Freiheit der Lehre verletzt, denn eine mit dieser Freiheit nicht zu vereinbarende Verarbeitung personenbezogener Daten kann nicht erforderlich sein, verstößt daher gegen den Verhältnismäßigkeitsgrundsatz und stellt somit einen rechtswidrigen Eingriff in das Grundrecht auf informationelle Selbstbestimmung (Art. 33 SächsVerf) dar.
Das Staatsministerium hat sich auf den Standpunkt gestellt, Äußerungen zur Lehrfreiheit gehörten nicht zu meinem Zuständigkeitsbereich, eine Auffassung, die ich wegen des gerade dargelegten rechtlichen Zusammenhanges nicht teilen kann.

Die Befragung muß also die durch Art. 5 Abs. 1 GG, Art. 21 SächsVerf geschützte

Freiheit der Wissenschaft (Forschung und Lehre) beachten. Und ich muß - vorab - prüfen, ob das geschieht. Erst dann ist ein datenschutzrechtlich fundiertes Votum möglich.

Die Wissenschaftsfreiheit umfaßt im Rahmen der Lehraufgaben insbesondere die Abhaltung von Lehrveranstaltungen und deren inhaltliche und methodische Gestaltung (§ 5 Abs. 3 Satz 1 SHG). Die inhaltliche Gestaltung betrifft im wesentlichen die Bewertung der Themen und Gegenstände, deren Gewichtung sowie die Lehrziele der Veranstaltung. Die Lehrfreiheit umfaßt weiterhin die Entscheidungsfreiheit des Lehrenden über die den ausgewählten Inhalten am besten entsprechenden Veranstaltungsformen und -methoden. Sie gewährleistet also die freie Entfaltung nicht nur als forschender Wissenschaftler, sondern auch als wissenschaftlich Lehrender. Dieses Grundrecht unterliegt keinem Gesetzesvorbehalt!

Gegen § 5 Abs. 3 SHG und damit zugleich gegen Art. 5 Abs. 3 GG, Art. 21 SächsVerf verstößt also jede Form der Evaluation, oder zumindest die Sanktionierung aufgrund der Evaluationsergebnisse, die diese Grenze nicht berücksichtigt.

Allerdings ist bei der Prüfung zu berücksichtigen, daß die Hochschulen neben der Erfüllung ihrer Aufgaben in Forschung und Lehre auch auf eine berufliche Tätigkeit (§ 4 Abs. 1 Satz 2 SHG) vorbereiten. Die Lehre dient gerade diesem Ziel. Es besteht ein gesetzlicher Ausbildungsauftrag. Aus diesem Ausbildungsauftrag der Hochschule resultieren Amtspflichten des einzelnen Hochschullehrers.
Zulässig sind daher Angaben in einem Fragebogen, mit dem die Studentenbefragung durchgeführt wird, zum Ausfall von Lehrveranstaltung, soweit sie einen Rückschluß darauf zulassen, daß der Lehrende seine Lehrverpflichtungen ("Lehrdeputat") nicht erfüllt. Zulässig sind auch Fragen, die sich auf die Organisation beziehen, also etwa, ob sich Pflichtveranstaltungen überschneiden. Dasselbe gilt für Kriterien, die nicht auf die Überprüfung einer bestimmten Methode, sondern darauf abzielen, ob Grundanforderungen an eine rezipientengerechte Vorlesung beachtet werden, also z. B. die akustische Verständlichkeit des Vortrags (das Nuscheln des Professors genießt nicht den Schutz von Art. 5 Abs. 3 GG).
Die Frage, ob der Stoff prüfungsrelevant ist, betrifft die inhaltliche Gestaltung der Lehre. Weil die Lehrfreiheit insoweit durch den gesetzlichen Ausbildungsauftrag der Hochschule begrenzt ist, darf überprüft werden, ob der Hochschullehrer seinen Pflichten, zu denen auch die Vermittlung des prüfungsrelevanten Stoffs gehört, nachkommt. Er hat jedoch die Freiheit, über diesen Stoff hinausgehend zu lehren.
Hingegen betrifft die Frage, welche Medien eingesetzt werden, einen Aspekt der Methodenwahl. Diese Wahl unterliegt der Lehrfreiheit. Dagegen läßt sich auch nicht einwenden, der Ausbildungsauftrag erfordere den Einsatz einer optimalen Methode der Wissensvermittlung. Es ist gerade Teil der Lehrfreiheit, diese Wahl nach eigener Auffassung zu treffen.
Die bisher genannten Angaben waren "professorenbezogen". Andere sind eindeutig "studentenbezogen" (als Beispiel aus einem Fragebogen "Arbeiten Sie den Stoff regelmäßig nach?") und damit ebenfalls unter dem Gesichtspunkt der Freiheit von

Lehre und Forschung unbedenklich. Es ist allerdings dafür zu sorgen, daß von Anfang an die Anonymität des Befragten gewahrt wird.

Besondere Schwierigkeiten bereitet die Einordnung der Angaben, die Äußerungen des Studenten über die eigene Person mit Äußerungen über den Hochschullehrer verknüpfen.
Sie sind auf den ersten Blick studentenbezogen. Soweit sie jedoch Rückschlüsse auf den Dozenten zulassen, handelt es sich in Wahrheit jedoch nicht nur um auf die Person des Studenten bezogene Daten. Als Beispiel sei die Frage genannt "Welchen Schwierigkeitsgrad hat der Stoff Ihrer Ansicht nach?". Wenn geantwortet wird "zu einfach" oder "zu schwierig", läßt dies den Rückschluß zu, daß der Hochschullehrer zu niedrige oder zu hohe Anforderungen stellt. Es kann aber auch bedeuten, daß die Vorkenntnisse des Studenten außergewöhnlich hoch oder zu schlecht sind. Auf den einzelnen Studenten bezogen wird also nicht erkennbar, ob die Angabe eine Aussage über ihn oder über den Hochschullehrer enthält. Sie wird jedoch hochschullehrerbezogen, wenn die Beurteilungsskala einen Schwerpunkt zeigt. Falls also 70 % der Studenten antworten "zu schwierig" und nur 10 % "gerade richtig", scheint die Schlußfolgerung nahezuliegen, daß der Hochschullehrer es nicht verstanden hat, den Stoff so aufzubereiten, daß das Ziel der Veranstaltung erreicht wird. Damit betrifft auch eine solche Angabe den Inhalt und die Methode der Lehrveranstaltung.

Ähnlich einzuordnen sind die Angaben "die Veranstaltung motivierte mich, fachlichen Austausch mit Kommilitonen zu führen" und "werden Ihnen Zusammenhänge mit dem Inhalt anderer Lehrveranstaltungen oder Lehrgebiete deutlich?".

Die Bestimmung der Grenzen, die eine Evaluation zu beachten hat, ist bei solchen Angaben besonders schwierig.
Man könnte geltend machen, dem Hochschullehrer solle nicht eine bestimmte Lehre vorgeschrieben werden. Es solle nur eine schlechte Lehre verhindert werden. Art. 5 Abs. 3 GG sei nicht berührt, weil der Hochschullehrer ein Grundrecht auf mangelnde didaktische Leistung nicht für sich in Anspruch nehmen könne.
Nach den o. g. Kriterien kommt ein Eingriff in den Inhalt der Lehrveranstaltung (abgesehen von der Minimalforderung, daß der examensrelevante Stoff zu vermitteln ist) und die Wahl der Methode nicht in Betracht. Gerechtfertigt wäre also eine Reaktion, die an fehlender Sachkompetenz anknüpft. Eine solche Trennung dürfte in der Praxis allerdings kaum durchführbar sein. Mit einer Sanktion ist daher die Gefahr verbunden, daß in den Inhalt oder die Methode der Lehre eingegriffen wird.
Als weitere Kategorie sind die "stoffbezogenen" Angaben zu nennen ("Stehen Sie dem Stoff dieser Lehrveranstaltung interessiert gegenüber? Können Sie Ihre Antwort begründen? praxisbezogen; zu trocken und theoretisch, abstrakt; für späteren Beruf wichtig ..."). Massiv würde in die Freiheit der Lehre eingegriffen, wenn Mittel gekürzt würden, weil der Stoff z. B. wegen eines ungenügenden Praxisbezugs unbeliebt wäre. Bei Pflichtveranstaltungen allerdings stellt sich das Problem nicht.

Die Bewertung hängt nicht allein vom Stoff ab, sondern auch vom Interesse des

Studenten. Insbesondere sind auch Rückschlüsse auf die Qualität des Lehrers naheliegend. Ein guter Lehrer wird auch einen spröden Stoff ansprechend vermitteln, ein weniger guter Lehrer seine Zuhörer auch bei einem packenden Thema langweilen. In die Bewertung des Stoffs fließt also auch eine Bewertung der Stoffvermittlung ein. Damit entstehen die oben dargestellten Probleme.

Der gesetzliche Ausbildungsauftrag der Hochschulen kann also nur innerhalb eines eng gesteckten Rahmens durchgesetzt werden.

Man könnte einwenden, daß durch eine Studentenbefragung in die Freiheit der Lehre nicht eingegriffen werde, weil der Hochschullehrer die Ergebnisse einfach ignorieren könne. Zu berücksichtigen ist jedoch, daß negative Ergebnisse zu einem Ansehensverlust oder anderem, durch die hoheitliche Maßnahme der Befragung hervorgerufenen Druck, führen, der ihn bewegen könnte, etwa eine bei den Studenten unbeliebte Form der Wissensvermittlung zu ändern. Ob diese möglichen Auswirkungen ausreichen, um einen staatlichen Eingriff in die Freiheit der Lehre anzunehmen, mag bezweifelt werden. Hier kommt allerdings hinzu, daß vom SMWK konkrete Reaktionen geplant sind, etwa bei der Zuteilung von Mitteln an die Hochschulen. Gewünscht wird vom Staatsministerium ebenfalls, daß auch bei der Verteilung der Mittel innerhalb der Hochschule die Ergebnisse der Befragung Berücksichtigung finden.

Ein wesentlicher Gesichtspunkt ist die Eignung solcher Studentenbefragungen, Aussagen zur Qualität der Lehre zu treffen. In dem Kolloquium der TU Dresden war dazu von einem Teil der Vertreter der Empirischen Sozialwissenschaft differenzierte bis kritische Töne zu hören.

Ich habe dem SMWK vorgeschlagen, gemeinsam einen Fragenkatalog zu erarbeiten, der die Grenzen von Art. 5 Abs. GG, Art. 21 SächsVerf beachtet. Bisher hat es leider mein Angebot nicht angenommen.

13.3 Forschung

Der Schwerpunkt der Forschungsvorhaben, die ich geprüft habe, lag in der Medizin. Stellung genommen habe ich jedoch auch zu Projekten der sozialwissenschaftlichen Forschung und der Schulforschung. Ein deutlicher Zuwachs war bei der Justizforschung festzustellen, die ein breites Spektrum von Befragungen zur beruflichen Situation von Bewährungshelfern bis zu der Frage aufwies, ob Staatsanwaltschaften Unterlagen an die Gedenkstätte Yad Vashem übergeben dürfen.

Forschungsverbund "Public Health" Sachsen

Seit Ende der achtziger Jahre haben sich in der Bundesrepublik fünf Forschungsverbünde "Public Health" entabliert: Berlin, Niedersachsen (mit Sitz in

Hannover), Nordrhein-Westfalen (Bielefeld), München und nun der Forschungsverbund "Public Health" Sachsen als erster und bislang einziger in den neuen Bundesländern.

Ziel dieser Verbünde ist eine interdisziplinäre Forschung im Bereich "Public Health". Eine genaue Bestimmung dieses Begriffs ist schwierig. "Public Health" befaßt sich mit Gesundheitsforschung, Prävention und der Gestaltung und Erforschung von Versorgungssystemen. Es werden also nicht nur Ursachen von Erkrankungen erforscht, sondern auch Strukturen der Gesundheitsversorgung, etwa im hausärztlichen Bereich. Vertreten sind u. a. Epidemiologie, Hygiene, Psychologie, Gesundheitssystemforschung und Ökonomie. Angestrebt wird eine enge Zusammenarbeit mit Einrichtungen außerhalb der Hochschule, z. B. den Krankenkassen.

Als Projektbeispiele seien Untersuchungen zur "Qualität der Diabetikerbetreuung", zur "Versorgung bei endogenen Psychosen" und zum "Wechsel in der hausärztlichen Versorgung" genannt.

Großes Gewicht wird auch der Lehre beigemessen. Daher haben eine Reihe von Hochschulen Postgraduiertenstudiengänge "Public Health" eingerichtet.

Gefördert werden die Verbünde insbesondere vom Bundesministerium für Bildung, Wissenschaft, Forschung und Technologie (BMBF). Als Projektträger hat das Bundesministerium die "Arbeit, Umwelt und Gesundheit in der Deutschen Luft- und Raumfahrtgesellschaft (DLR)" mit der Durchführung der Förderungsmaßnahmen anstelle der bis Anfang 1995 zuständigen "Gesundheitsforschung bei der GSF" beauftragt. Aufgaben des Projektträgers sind die Beratung von Antragstellern und die sonstige organisatorische Betreuung der Vorhaben.

Der Forschungsverbund "Public Health" Sachsen hat mich um datenschutzrechtliche Stellungnahme zu einem Vorhaben gebeten, das an der TU Dresden durchgeführt wird.

Bei Vorhaben des Forschungsverbunds ist datenschutzrechtlich zu prüfen, ob bei Herausgabe von Adreßdaten durch die Meldebehörden die Vorschriften über die Übermittlung an öffentliche Stellen oder an Private gelten. Insbesondere richtet sich nach der Rechtsnatur des Forschungsverbundes, ob die Verbünde die Vorschriften des Bundesdatenschutzgesetzes über nicht-öffentliche Stellen oder ob sie das jeweilige Landesdatenschutzgesetz anwenden müssen.
In Sachsen haben sich aufgrund eines Kooperationsvertrags die TU Dresden, die Universität Leipzig und das Deutsche Hygienemuseum Dresden zum Forschungsverbund zusammengeschlossen. Durchgeführt werden die einzelnen Vorhaben jedoch von der jeweiligen Hochschuleinrichtung bzw. dem Hygienemuseum. Eine Koordination der Projekte erfolgt durch die Geschäftsstelle des Forschungsverbunds.
Datenverarbeitende Stelle ist daher die jeweilige forschende Einrichtung. Soweit es

sich um Institute der beiden Hochschulen handelt, gelten daher das Sächsische Datenschutzgesetz und für Krankenhäuser, zu denen auch Hochschulkliniken gehören, die §§ 33 und 34 SächsKHG.

14 Technischer und organisatorischer Datenschutz

14.1 Orientierungshilfe zu Datenschutzfragen des Anschlusses von Netzen der öffentlichen Verwaltung an das Internet, erstellt vom Arbeitskreis Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder

I. Einleitung

Seit einiger Zeit wächst in öffentlichen Stellen der Wunsch nach einem Zugang zu globalen Datennetzen, insbesondere zu dem Internet. Die Netzanbindung soll sowohl zur Informationsgewinnung als auch zur Bereitstellung eigener Informationen für andere dienen (zur Beschreibung des Internet und der wichtigsten Internetdienste vgl. Anlage 1).

Dabei ist der Anschluß an das Internet mit erheblichen Gefährdungen des Datenschutzes und der Datensicherheit verbunden. Die Risiken resultieren großenteils daraus, daß das Internet nicht unter Sicherheitsaspekten entwickelt wurde. Schwächen finden sich in den Protokollen für die Datenübertragung, in den Implementierungen und Installationen der Programme für die Internet-Dienste und in den angeschlossenen Rechnersystemen. So gibt es beispielsweise keine sicheren Mechanismen zur Identifikation und Authentisierung im Netz. Ohne besondere Schutzmaßnahmen kann sich ein Angreifer oft mit wenig Aufwand unter Ausnutzung der Sicherheitslücken unberechtigten Zugang zu fremden Rechnern verschaffen und dort Daten ausspähen oder sogar manipulieren oder zerstören. Dies ist besonders gravierend, weil angesichts von z.Zt. mehr als 40 Millionen Internet-Teilnehmern auch die Zahl der potentiellen Angreifer, die diese Sicherheitslücken ausnützen und somit die am Internet angeschlossenen Verwaltungsrechner bedrohen, sehr groß ist.

Das Internet bietet auch keinen Schutz vor der Informationsverfälschung.

Die vorliegende Orientierungshilfe soll den für den Betrieb von Netzen der öffentlichen Verwaltung Verantwortlichen deutlich machen, mit welchen Risiken für die Sicherheit der “internen” Netze bei einem Anschluß an das Internet zu rechnen ist und wie diese Risiken begrenzt werden können. Die Frage, ob und ggf. unter welchen Bedingungen Verwaltungen personenbezogene Daten über das Internet austauschen dürfen, ist nicht Gegenstand der Orientierungshilfe und muß jeweils konkret untersucht werden.

Die hier entwickelten Strategien zur Risikobegrenzung bedürfen im Einzelfall einer weiteren Konkretisierung, wobei neben den beschriebenen Firewall-Architekturen ggf. weitere Maßnahmen zu ergreifen sind, um eine Gefährdung personenbezogener Daten zu vermeiden (etwa Einsatz von Verschlüsselungsverfahren). Angesichts einer sich ständig verändernden Gefährdungslage infolge der "Entdeckung" neuer unerwarteter Sicherheitsprobleme bleiben auch bei Einsatz von Firewall-Systemen erhebliche Restrisiken bestehen.

Der Anschluß an das Internet ist angesichts dieser Gefährdungslage nur vertretbar, wenn zuvor eine eingehende Analyse und Bewertung der damit verbundenen Risiken erfolgt ist und die Gefahren durch technische und organisatorische Maßnahmen sicher beherrscht werden können. Die nachfolgenden Empfehlungen stellen ein Konzentrat aus den weiter unten angestellten eingehenderen Betrachtungen dar.

II. Empfehlungen

- Verwaltungsnetze dürfen an das Internet nur angeschlossen werden, wenn und soweit dies erforderlich ist. Die Kommunikationsmöglichkeiten haben sich am wirklichen Kommunikationsbedarf zu orientieren. Dabei ist auch zu prüfen, inwieweit das Behördennetz in anschließbare, nicht anschließbare und bedingt anschließbare Teile segmentiert werden muß und ob die Aufgabe mit einem nicht in das Verwaltungsnetz eingebundenen Rechner erfüllt werden kann.
- Voraussetzung für die Anbindung eines Behördennetzes an das Internet ist, daß ein schlüssiges Sicherheitskonzept vorliegt, das konsequent umgesetzt wird. Die Internet-Anbindung darf nur erfolgen, wenn die Risiken durch technische und organisatorische Maßnahmen wirksam beherrscht werden können.
- Die Sicherheit des Verwaltungsnetzes und der Schutz von personenbezogenen Daten, die auf vernetzten Systemen verarbeitet werden, ist durch geeignete Firewall-Systeme sicherzustellen, die eine differenzierte Kommunikationssteuerung und Rechtevergabe unterstützen. Dabei sind die Anforderungen, die von den Firewall-Komponenten zu erfüllen sind, vorab zu definieren, wobei sich die Verwaltung auch externen Sachverstands bedienen sollte.
- Um der Gefahr von Maskeraden und der Ausforschung der Netzstrukturen des geschützten Netzes entgegenzuwirken, ist eine gesonderte interne Adreßstruktur zu verwenden. Die internen Adressen sind durch die zentralen Firewall auf externe Internet-Adressen umzusetzen.
- Der ausschließliche Einsatz einer zentralen Firewall-Lösung ist nur dann vertretbar, wenn eine Orientierung am höchsten Schutzbedarf erfolgt, auch wenn dies Nachteile für weniger sensible Bereiche mit sich bringt. Die Frage der Kontrolle interner Verbindungen bleibt bei einer solchen Lösung offen. Ferner ist eine ausschließlich zentrale Lösung mit der Maxime der lokalen Haltung und Verwaltung von sicherheitsrelevanten Daten (Pflege von Benutzerprofilen) schwer vereinbar. Werden solche Daten nicht durch diejenigen verwaltet, die den verwalteten Bereich direkt überschauen können, besteht die Gefahr erheblicher Differenzen zwischen Realität und sicherheitstechnischem Abbild (besser: Trugbild).

- Das Konzept gestaffelter Firewalls kommt den Datenschutzanforderungen an Verwaltungsnetze entgegen, die aus einer Vielzahl verschiedener Teilnetze bestehen, in denen Daten unterschiedlicher Sensibilität von unterschiedlichen Stellen für unterschiedliche Aufgaben verarbeitet werden und in denen dementsprechend jeweils unterschiedliche Sicherheitsanforderungen bestehen. Die mit gesonderten Firewalls abgesicherten Subnetze sollten jeweils einen definierten Übergang zu dem Gesamtnetz erhalten. Die Anbindung des Gesamtnetzes an das Internet sollte stets über ein zentrales Gateway erfolgen, das durch einen Firewall geschützt wird.
- Der personelle und sachliche Aufwand für Firewall-Lösungen ist generell hoch. Es ist gleichwohl unverzichtbar, hochspezialisierte Kräfte einzusetzen, um gegen mindestens ebenso spezialisierte Angreifer gewappnet zu sein. Dieser Aufwand ist jedoch stets dann gerechtfertigt, wenn Verwaltungsnetze an das Internet angeschlossen werden sollen, in denen sensible personenbezogene Daten verarbeitet werden.
- Der Betrieb von Firewall-Systemen muß klaren Richtlinien folgen. Diese Richtlinien müssen neben Zuständigkeitsregelungen auch Vorgaben über die Protokollierung, die Behandlung von sicherheitsrelevanten Ereignissen und Sanktionen bei Sicherheitsverstößen enthalten.
- Auch bei Einsatz von Firewalls bleiben Restrisiken bestehen, denen anwendungsbezogen begegnet werden muß. So bleibt es auch beim Einsatz von Firewalls notwendig, sensible Daten nur verschlüsselt zu übertragen; hierzu gehören neben besonders sensiblen personenbezogenen Daten auch Paßwörter und sonstige Authentifikationsdaten.
- Bei einem unvertretbaren Restrisiko muß auf einen Anschluß des jeweiligen Netzes an das Internet verzichtet werden. Der Zugriff auf Internet-Dienste muß in diesem Fall auf nicht in das Verwaltungsnetz eingebundene Systeme beschränkt werden, auf denen ansonsten keine sensiblen Daten verarbeitet werden.
- Firewall-Konzepte entlasten die dezentralen Verwalter von vernetzten Systemen nicht von ihrer Verantwortung zur Gewährleistung des Datenschutzes; vielmehr erhöhen sich mit der Vernetzung die Anforderungen an die lokale Systemverwaltung, da Administrationsfehler ungleich schwerwiegendere Konsequenzen haben könnten als bei stand-alone-betriebenen Rechnern.

III. Sicherheitsrisiken im Internet

Die nachfolgend dargestellten Sicherheitsrisiken spiegeln lediglich einen kleinen Ausschnitt der möglichen Angriffe auf Rechnersysteme mit Internet-Anschluß wider. Selbst wenn Gegenmaßnahmen gegen die bekannten Gefährdungen getroffen werden, läßt sich ein hundertprozentiger Schutz ohne Verzicht auf die Netzanbindung nicht realisieren. Sobald ein Computer Zugang zu einem Datennetz hat, ist er von anderen angeschlossenen Rechnern aus erreichbar. Damit wird das eigene System der Gefahr eines unberechtigten Gebrauches ausgesetzt. Es gibt jedoch eine Reihe von Schutzvorkehrungen, um das Sicherheitsrisiko zu minimieren.

1. Protokollimmanente Sicherheitsrisiken
Sowohl die Nutzerkennung als auch das Paßwort werden bei den gängigen Diensten im Klartext über das lokale Netz (z. B. Ethernet) und über das Internet übertragen. Mit Programmen, die unter dem Namen Packet Sniffer bekannt sind, kann der Datenverkehr im Netz bzw. auf den Netzknoten belauscht und nach interessanten Informationen durchsucht werden. So können diese Abhörprogramme zahlreiche Nutzerkennungen mit den zugehörigen Paßworten ausspähen, mit deren Hilfe sich ein Angreifer einen unberechtigten Zugriff auf andere Rechner verschaffen kann.
Datenpakete können nicht nur abgehört, sondern auch manipuliert werden. Da bei vielen Internet-Diensten die Authentisierung der Rechner lediglich über die IP-Nummer des Nutzers erfolgt, kann sich dies ein Angreifer zunutze machen, indem er IP-Pakete mit gefälschten Absenderadressen ans fremde Rechnersystem schickt (IP-Spoofing). Sofern das System die IP-Adresse für vertrauenswürdig hält, wird dem Eindringling ein Zugang, unter Umständen sogar mit Administratorrechten, gewährt. Ferner kann der Übertragungsweg bei dynamischem Routing geändert werden. Pakete können abgefangen werden, so daß sie nicht an ihrem Ziel ankommen; ein Angreifer kann sie durch eigene Pakete ersetzen. Weiterhin läßt sich die Kommunikation eines authorisierten Nutzers mitschneiden und später wiedereinspielen, wodurch sich der Angreifer bei vielen Diensten die Rechte des Nutzers verschafft (z. B. beim Festplattenzugriff über NFS [Network File System]).

2. Dienstspezifische Sicherheitsrisiken
E-Mail und Usenet-News:
Private Nachrichten können mitgelesen werden, sofern sie nicht verschlüsselt sind. E-Mails und News-Artikel ohne eine digitale Signatur lassen sich leicht verändern oder fälschen. Über den elektronischen Postweg können Programme und Textdokumente mit Viren ins System gelangen. Selbst ein automatisches Durchsuchen der Nachrichten nach Viren bietet keinen vollständigen Schutz.
Die Informationen über Datum und Uhrzeit der Erstellung einer Nachricht können zu einem Persönlichkeitsprofil des Absenders ausgewertet werden. Daneben forschen Adreßsammler nach E-Mail- und Post-Adressen, um unaufgefordert Werbung zuzuschicken.
Sendmail, das auf UNIX-Rechnern am häufigsten eingesetzte Programm zum Verschicken elektronischer Post, weist zudem eine ganze Reihe von sicherheitsrelevanten Fehlern auf, die zu einer Zugangsmöglichkeit mit Administratorrechten führen können.
Zudem ist nicht sicherzustellen, daß eine E-mail den Empfänger überhaupt erreicht und daß der Absender einen Nachweis der Zustellung erhält.

Telnet:
Ist der Telnet-Dienst nicht eingeschränkt, sondern von beliebigen Adressen aus zu beliebigen Ports auf dem eigenen Rechner möglich, wird die Zugangskontrolle gefährdet. Auch ein Angreifer, dem es nicht gelingt, sich einen Zugang mit Administratorrechten zu verschaffen, hat häufig die Möglichkeit, einen nichtprivilegierten Account auf dem Rechner zu nutzen. Dieser Account kann dann als

Ausgangsbasis für den Angriff auf weitere Rechner verwendet werden.

FTP:
Schlecht gewartete FTP-Server stellen ein Risiko dar, da in älteren Versionen des FTP-Server-Programms (ftpd) Sicherheitslücken existieren, die zur Erlangung von Administratorrechten führen können. Besondere Vorsicht ist geboten, da viele Beschreibungen zur Installation und Konfiguration von Anonymous-FTP-Servern sicherheitsbedenkliche Fehler enthalten. Bei Fehlkonfigurationen kann es einem Angreifer gelingen, die Datei mit den verschlüsselten Paßwörtern aller Benutzer auf seinen Rechner zu laden und dort in aller Ruhe zu entschlüsseln. Läßt man zu, daß Benutzer eines FTP-Servers eigene Dateien in Verzeichnissen ablegen können, wo andere sie sich holen können, kann sich der FTP-Server schnell zu einem Umschlagplatz von Raubkopien entwickeln.

WWW:
Gefährdungen entstehen bei WWW-Servern durch fehlerhafte Software oder Konfigurationen. Ohne den Einsatz von SSL (Secure Socket Layer) läßt sich die Kommunikation abhören. Außerdem weisen CGI(Common Gateway Interface)-Skripte häufig Sicherheitslücken auf. Zur Zeit sind WWW-Browser in der Entwicklung, die das Ablegen von Dateien auf dem Server erlauben. Dies kann zu weiteren Sicherheitsproblemen führen. Beim Nutzen des World Wide Web können zahlreiche Daten über den Anwender und sein Verhalten (was hat wer wann aufgerufen und wie lange gelesen?) protokolliert werden, so daß ein umfassendes Persönlichkeitsprofil erstellt werden kann.

Finger:
Die Daten, die der Finger-Dienst ausgibt, können einem Angreifer Informationen über die Nutzerkennungen auf dem System liefern, die gezielt für einen Angriff verwendet werden können. Berühmt geworden ist dieser Dienst 1988 durch den sogenannten Internet-Wurm. Dabei handelte es sich um ein Angriffsprogramm, das ausnutzte, daß die beim Aufruf von Finger übergebenen Parameter in einen Puffer fester Länge geschrieben wurden. Die Daten, die nicht mehr in den Puffer paßten, überschrieben den Stack im Arbeitsspeicher, wo sie als Programmcode behandelt und ausgeführt wurden. Bei geschickter Wahl der übergebenen Zeichenreihe kann so ein beliebiger Code zur Ausführung kommen. Ähnliche Programmfehler finden sich auch heute noch in vielen anderen Serverprogrammen. Zum Beispiel ist gerade Ende 1995 ein weiterer solcher Fehler im Programm Sendmail bekannt geworden. Der Protokollierbefehl Syslog und manche WWW-Browser (auch für MS-Windows) enthalten ebenfalls Fehler dieser Art.

IV. Kommunikationsanalyse

Bevor eine öffentliche Stelle Zugang zum Internet bekommt, muß sie eine Analyse des Kommunikationsbedarfs durchführen. Bei der Beurteilung der Erforderlichkeit eines Internet-Anschlusses ist ein strenger Maßstab anzulegen. Auch wenn die Erforderlichkeit bejaht wird, ist zu prüfen, ob der Verwendungszweck nicht schon

durch den Anschluß eines isolierten Rechners erreicht werden kann.

Die Art des zu realisierenden Zugangs hängt wesentlich davon ab, welche Dienste des Internet genutzt werden sollen. Dabei ist zu unterscheiden zwischen Diensten, die von lokalen Benutzern im Internet abgerufen werden, und Diensten, die von lokalen Rechnern für Benutzer im Internet erbracht werden. Diese Kommunikationsanforderungen müssen auf Grund der unterschiedlichen Aufgaben sowohl für den zentralen Zugang zum Internet als auch für jeden einzelnen Rechner analysiert werden. Es dürfen nur die IP-Pakete weitergeleitet werden, die für den zu nutzenden Dienst bezogen auf den nutzungsberechtigten Rechner notwendig sind.

Wird bei der Analyse des Kommunikationsbedarfs festgestellt, daß die Anbindung an das Internet auf IP-Ebene notwendig ist, das TCP/IP-Protokoll also in seiner vollen Funktionalität genutzt wird, müssen weitere Sicherheitsbetrachtungen durchgeführt werden, die Voraussetzung für die Planung und Realisierung von Sicherheitskonzepten sind. Ausgangspunkte einer derartigen Risikoanalyse sind der Schutzbedarf der zu verarbeitenden Daten und die Sicherheitsziele der öffentlichen Stelle.

In Anlehnung an die Empfehlungen des BSI-Grundschutzhandbuches sind zur Feststellung des Schutzbedarfs folgende Fragen zu beantworten:

- Welche Datenpakete dürfen auf der Grundlage welchen Protokolls bis zu welchem Rechner im Netz weitergeleitet werden?
- Welche Informationen sollen nicht nach außen gelangen?
- Wie können z.B. die interne Netzstruktur und Benutzernamen nach außen unsichtbar gemacht werden?
- Welche Authentisierungsverfahren sollen benutzt werden; sind benutzerspezifische Authentisierungsverfahren notwendig?
- Welche Zugänge werden benötigt (z. B. nur über einen Internet-Service-Provider)?
- Welche Datenmengen werden voraussichtlich übertragen?
- Welche Rechner mit welchen Daten befinden sich im Netz, die geschützt werden müssen?
- Welche Nutzer gibt es im Netz, und welche Dienste sollen dem einzelnen Nutzer zur Verfügung gestellt werden?
- Welche Aktivitäten im Netz sollen protokolliert werden? (Dabei werden ggf. Fragen des Arbeitnehmerdatenschutzes tangiert)
- Welche Dienste sollen auf keinen Fall genutzt werden?
- Wird sichergestellt, daß nur die Dienste genutzt werden können, die ausdrücklich freigegeben worden sind (was nicht erlaubt ist, ist verboten)?
- Welcher Schaden kann im zu schützenden Netz verursacht werden, wenn Unberechtigte Zugang erhalten?
- Welche Restrisiken verbleiben, wenn die vorgesehenen Schutzmaßnahmen realisiert wurden?

- Welche Einschränkungen würden Benutzer durch den Einsatz von Schutzmaßnahmen akzeptieren?

Um im Rahmen der empfohlenen Kommunikationsanalyse beurteilen zu können, welche Dienste von welchem Nutzer an welchem Rechner tatsächlich benötigt werden, sollten die jeweiligen Stellen zunächst versuchen, genaue Kenntnisse über die Möglichkeiten und Gefährdungen der angebotenen Kommunikationsmöglichkeiten zu erlangen (etwa durch entsprechende Tests mit an das Internet angeschlossenen Einzelplatz-PC).

V. Firewalls

Soll ein Verwaltungsnetz an das Internet angeschlossen werden, so kann dies entweder durch einen zentralen Zugang oder durch mehrere dezentrale erfolgen. Aus Sicherheitsgründen ist ein zentraler Zugang vorzuziehen. Ist das Verwaltungsnetz erst einmal an das Internet angeschlossen, so lassen sich die durch die Anbindung hervorgerufenen Sicherheitsrisiken durch Einsatz eines Firewall reduzieren.

Unter einem Firewall (”Brandschutzmauer”) wird eine Schwelle zwischen zwei Netzen verstanden, die überwunden werden muß, um Systeme im jeweils anderen Netz zu erreichen. Die Hauptaufgabe eines Firewall besteht darin, zu erreichen, daß jeweils nur zugelassene netzübergreifende Aktivitäten möglich sind und daß Mißbrauchsversuche frühzeitig erkannt werden. Üblicherweise wird dabei davon ausgegangen, daß die Teilnehmer des internen Netzes (hier: des Verwaltungsnetzes) vertrauenswürdiger sind als die Teilnehmer des externen Netzes (hier: des Internet). Gleichwohl sind Firewall-Lösungen auch geeignet, die ”grenzüberschreitenden” Aktivitäten der internen Nutzer, d. h. den Übergang zwischen verschiedenen Teilnetzen (z. B. Ressortnetze) innerhalb eines Verwaltungsnetzes, zu begrenzen.

Firewalls weisen die folgenden Charakteristika auf:

- der Firewall ist die definierte und kontrollierte Schnittstelle zwischen dem zu schützenden und dem nicht vertrauenswürdigen Netz;
- im internen Netz besteht jeweils ein einheitliches Sicherheitsniveau; eine weitere Differenzierung nach Sicherheitsstufen geschieht - zumindest auf der Ebene des Netzes - nicht;
- der Firewall setzt eine definierte Sicherheitspolitik für das zu schützende Netz voraus; in diese müssen die Anforderungen aller vernetzten Stellen einfließen;
- es besteht die Notwendigkeit einer firewallbezogenen Benutzerverwaltung derjenigen internen Teilnehmer, die mit Rechnern in dem externen Netz kommunizieren dürfen.

Die Stärke des Firewall hängt wesentlich von der eingesetzten Technik und ihrer korrekten Administration ab; entscheidend für die Sicherheit sind jedoch auch die Staffelung und die organisatorische Einbindung von Firewalls in die IuK-Infrastruktur. Von besonderer Relevanz ist der Aspekt, daß für den von einem Firewall geschützten

Bereich das erforderliche Schutzniveau definiert wird. Diese Anforderung kann mit drei Lösungsvarianten erfüllt werden:

einheitlich hohes Schutzniveau im internen Netz, d. h. Orientierung am höchsten vorhandenen Schutzbedarf;
einheitlich niedriges Schutzniveau, d. h. Orientierung am niedrigsten vorhandenen oder einem insgesamt geringen oder mittleren Schutzbedarf;
einheitlich niedriges Schutzniveau sowie Durchführung zusätzlicher Maßnahmen zum Schutz von Netz-Komponenten mit höherem Schutzbedarf.

Die Varianten 1 und 2 entsprechen am ehesten zentralen Firewall-Lösungen, wobei angesichts der Sensibilität der in der Verwaltung verarbeiteten Daten allein Variante 1 mit den Anforderungen des Datenschutzrechts vereinbar sein dürfte. Variante 3 führt zur Lösung gestaffelter Firewalls, d. h. zu einer Konstellation, bei der neben einem zentralen, den mittleren Schutzbedarf abdeckenden Firewall (die u. a. die interne Netzstruktur nach außen sichert) bereichsbezogen und bedarfsorientiert Firewall-Anschlüsse mit unterschiedlichem Sicherheitsniveau implementiert werden können. Allerdings können selbst bei einheitlich hohem Schutzniveau im Gesamtnetz gestaffelte Firewalls sinnvoll sein, um den möglichen Schaden, der mit Sicherheitsverletzungen verbunden ist, auf ein Netzsegment zu begrenzen. Dies gilt insbesondere auch für die Abwehr von internem Mißbrauch.

1. Zentrale Firewalls

Rein zentrale Firewall-Lösungen sind durch folgende Aspekte charakterisiert:

- der zentrale Firewall bildet die einzige Schnittstelle zwischen dem kompletten zu schützenden Verwaltungsnetz und dem übrigen Internet;
- innerhalb des Verwaltungsnetzes besteht ein einheitliches Sicherheitsniveau, eine weitere Differenzierung nach Sicherheitsstufen erfolgt nicht;
- eine Kontrolle der internen Verbindungen durch den Firewall ist nicht möglich;
- der zentrale Firewall setzt eine definierte Sicherheitspolitik für das gesamte Verwaltungsnetz voraus; abweichende Sicherheitspolitiken für besonders schützenswerte Bereiche sind auf Netzebene nicht durchsetzbar;
- es besteht die Notwendigkeit einer zentralen Benutzerverwaltung. Für jeden Teilnehmer muß sowohl auf Dienstebene als auch bezogen auf die zugelassenen Adressen die zulässige Kommunikation festgelegt werden.

Da ein zentraler Firewall eine Differenzierung nach Teilnetzen nicht unterstützt und dementsprechend ein einheitliches Sicherheitsniveau für das gesamte Verwaltungsnetz voraussetzt, muß sich der Grad des gewährleisteten Schutzes nach den sensibelsten Daten richten und ist dementsprechend hoch. Dies hat jedoch für Verwaltungsbereiche mit weniger sensiblen Daten den Nachteil, unnötig hohe Schranken zu errichten. Daraus ergibt sich die Gefahr, daß von diesen Stellen zusätzliche Internet-Zugänge mit geringeren Restriktionen geschaffen werden, wodurch der gesamte Zweck des Firewall ad absurdum geführt wird.

Ein weiterer Nachteil zentraler Firewalls besteht in dem - auch aus dem Großrechnerbereich bekannten - Problem, daß eine Benutzerverwaltung, die fernab von dem jeweiligen Fachbereich erfolgt, häufig zu Abweichungen zwischen der Realität von Benutzerrechten und deren Abbildung in Form von Accounts führt.

Da sich Firewall-Lösungen primär zum Schutz gegen Zugriffe von außen eignen, sekundär auch zum Schutz gegen Zugriffe von innen nach außen, jedoch nicht zur Kontrolle der rein internen Zugriffe, besteht bei rein zentralen Lösungen die Gefahr, daß das gesamte Verwaltungsnetz als eine Einheit betrachtet wird und insofern nur die Zugriffe von oder nach außen restringiert werden. Dieser Aspekt ist zwar nur mittelbar Teil des Themas "Internetanbindung", muß bei einer Gesamtbetrachtung von Netzwerksicherheit jedoch unbedingt einbezogen werden.
Der Einsatz eines alleinigen zentralen Firewall ist allenfalls dann vertretbar, wenn alle angeschlossenen Teilnetze über ein gleiches Sicherheitsbedürfnis bzw. -niveau verfügen und zudem nicht die Gefahr des internen Mißbrauchs besteht. Davon kann in behördenübergreifenden Verwaltungsnetzen mit einer Vielzahl angeschlossener Rechner jedoch nicht ausgegangen werden.

2. Gestaffelte Firewalls (Voraussetzungen, Einsatzmöglichkeiten, Forderungen)

Gestaffelte Firewall-Lösungen sind durch folgende Aspekte charakterisiert:

- es handelt sich um eine Kombination zentraler und dezentraler Komponenten, wobei durch einen zentralen Firewall ein Mindestschutz für das Gesamtnetz gegenüber dem Internet realisiert wird und dezentrale Firewalls in Subnetzen mit besonderem Schutzbedarf ein angemessenes Schutzniveau sicherstellen;
- innerhalb des jeweiligen geschützten Subnetzes besteht jeweils ein einheitliches Sicherheitsniveau;
- eine Kontrolle der verwaltungsinternen Verbindungen ist möglich, sofern die Kommunikation den durch dezentrale Firewalls geschützten Bereich überschreitet;
- auch ein gestaffeltes Firewall-System setzt eine definierte Sicherheitpolitik für das Gesamtnetz voraus; in diese müssen insbesondere die Anforderungen an einen zu garantierenden Grundschutz einfließen; darüber hinaus sind für die Subnetze gesonderte Sicherheitsanforderungen zu definieren;
- die Benutzerverwaltung kann weitgehend dezentralisiert werden. Allerdings sind einheitliche Regeln festzulegen, nach denen Benutzer das Recht haben, über den zentralen Firewall mit Systemen im Internet in Verbindung zu treten.

Für die dezentralen Firewalls bieten sich prinzipiell die gleichen Mechanismen wie bei einem zentralen Firewall an. Die Kombination zentraler und dezentraler Schutzmechanismen erlaubt die Realisierung des Prinzips eines autonomen Schutzes; bei sorgfältiger Konfiguration bleiben besonders geschützte Subnetze auch dann gesichert, wenn der zentrale Firewall durch einen Eindringling überwunden wurde.

Mit gestaffelten Firewalls kann - anders als bei zentralen Lösungen - das

datenschutzrechtlich bedeutsame Prinzip der informationellen Gewaltenteilung abgebildet werden, mit dem es nicht zu vereinbaren wäre, wenn die Verwaltung als informatorisches Ganzes betrachtet würde. Die Teilnetze können sowohl gegen Angriffe von außen - aus dem Internet - als auch untereinander abgeschottet werden.

Da gestaffelte Lösungen besser als ausschließlich zentrale Firewalls die Anforderungen der Benutzer abbilden können, ist auch die Gefahr der Umgehung der kontrollierten Schnittstellen durch Schaffung “wilder” Internetzugänge geringer. Zudem würden sich die Folgen derartiger Verstöße gegen die festgelegte Sicherheitspolitik besser isolieren lassen.

Auch gestaffelte Firewalls sind mit einem insgesamt hohen Administrations- und Pflegeaufwand verbunden, der jedoch auf die zentralen Firewalls und jeweiligen Bereiche verteilt ist. Die Festlegung der individuellen Benutzerrechte kann dabei im wesentlichen den anwendernäheren dezentralen Firewalls zugeordnet werden**.**

Anlage 1: Dienste im Internet

Das Internet ist ein weltumspannender Zusammenschluß vieler lokaler Computernetze. Die Zahl der Benutzer wird auf etwa 40 Millionen geschätzt (Stand: Ende 1995). Bisher wurde das Internet hauptsächlich von wissenschaftlichen Einrichtungen wie Universitäten genutzt. Inzwischen hat sich der Nutzerkreis ausgeweitet, und es ist eine fortschreitende Nutzung für kommerzielle Zwecke zu beobachten. Der Datenübertragung im Internet liegen die einheitlichen TCP/IP-Protokolle (Transmission Control Protocol/Internet Protocol) zugrunde.

Jeder Rechner im Internet erhält eine eindeutige numerische Adresse, die IP-Adresse. Die zu übertragenden Daten werden in Pakete zerlegt, die u.a. mit der Absender- und der Empfänger-IP-Adresse versehen werden. Die Datenpakete werden über zumeist eine Vielzahl von Zwischenstationen weitergeleitet, die den Weg zum Zielrechner aufgrund der Adreßinformationen bestimmen (Routing). Die Zwischenstationen tauschen die Daten über Wähl- oder Standverbindungen im Telefonnetz (per Kabel oder Satellit) aus.

Die wichtigsten Dienste, die das Internet bietet, werden im folgenden beschrieben.

E-Mail: Electronic Mail (kurz E-Mail) ist der am weitesten verbreitete Internet-Dienst. E-Mail ermöglicht das Verschicken von "elektronischen Briefen" zwischen mehreren Computerbenutzern. Die Nachrichten können aus Texten, Programmen, Grafiken oder Tönen bestehen. Sender und Empfänger müssen jeweils eine eindeutige E-Mail-Adresse besitzen (Form: Name@Anschrift), die ähnlich der postalischen Anschrift funktioniert. Um E-Mails in andere Datennetze zu verschicken oder von dort zu empfangen, werden Gateways benötigt, die den Übergang von einem System zum anderen handhaben. E-Mail kann außerdem für eine indirekte Inanspruchnahme von anderen

Diensten (z. B. FTP, WWW) genutzt werden.

Usenet-News: Öffentliche Nachrichten werden im Internet in thematisch gegliederten Diskussionsforen (Newsgroups) ausgetauscht. Dieser News-Dienst wird auch als Usenet (Kurzform von Users´ Network) bezeichnet. Er gleicht einer riesigen Zeitung mit Fachartikeln, Leserbriefen und Kleinanzeigen. Zur Zeit gibt es etwa 10.000 verschiedene Newsgroups, in denen pro Monat rund 3,2 Millionen Artikel mit einem Datenvolumen von ca. 14 GB geschrieben werden (Stand: August 1995). Die Artikel werden auf zentralen Rechnern (Newsservern) in Datenbanken gehalten; der Zugriff erfolgt über Newsreader-Programme.

Telnet: Mit Hilfe von Telnet ist es möglich, auf einem entfernten Rechner eine Terminalsitzung aufzubauen (Remote Login) und textorientierte Anwendungen zu nutzen. Dazu benötigt man einen Account (Nutzerkennung und Paßwort) oder einen öffentlichen Zugang auf dem entfernten Rechner. Über Telnet sind zum Beispiel Informationssysteme wie Datenbanken oder Bibliotheken nutzen. Telnet wird ebenfalls häufig für die Fernwartung von Rechnern eingesetzt.

FTP: FTP steht für File Transfer Protocol und dient dem Übertragen von Dateien zwischen Rechnern mit Hilfe eines normierten Befehlssatzes. Auf dem eigenen Rechner läuft der FTP-Client, der die Befehle an den entfernten FTP-Server weiterleitet. Voraussetzung für die Nutzung sind Accounts auf beiden Rechnern oder eine öffentliche Zugriffsmöglichkeit auf dem FTP-Server durch "Anonymous FTP", wodurch ein eingeschränkter Zugriff auf bestimmte Dateien des entfernten Rechners ermöglicht werden kann. Weltweit gibt es Tausende Anonymous-FTP-Server, die Programme, Texte, Grafiken oder Tondateien bereithalten.

Archie: Archie ist ein mächtiger Dienst für die weltweite Suche nach Dateien auf FTP-Servern. Der Zugriff erfolgt über Telnet, E-Mail oder einen eigenen Archie-Client. Als Suchergebnis liefert Archie entweder Server-, Verzeichnis- und Dateinamen oder eine Kurzbeschreibung zu gesuchten Dateien.

WWW Der jüngste Internet-Dienst WWW (World Wide Web) kann nahezu alle anderen Dienste integrieren. Durch einen multimediafähigen Hypertext-Mechanismus wird eine einfache Bedienbarkeit erreicht. Der Kommunikation zwischen dem WWW-Client und dem WWW-Server, der die multimedialen Daten anbietet, liegt das Protokoll HTTP (HyperText Transport Protocol) zugrunde. Die WWW-Dokumente werden mit der Definitionssprache HTML (HyperText Markup Language) erstellt. Für die Generierung interaktiver WWW-Seiten können CGI (Common Gateway Interface)-Skripte installiert werden.

Gopher: Gopher ist ein menüorientiertes Werkzeug zur Recherche, das unabhängig davon eingesetzt werden kann, auf welchem Rechner die gesuchten Informationen zu finden sind, in welchem Format sie vorliegen und welche Zugriffsmöglichkeiten (FTP, Telnet, WAIS usw.) existieren. Jeder Gopher-Server ist öffentlich zugänglich. Benutzer können mit ihrem Gopher-Client nur lesend auf die angebotenen Daten zugreifen. Gopher ist im WWW integriert.

WAIS: WAIS (Wide Area Information Server) ermöglicht eine Volltextsuche in einer Vielzahl von Datenbanken ohne Kenntnis komplizierter Abfragesprachen. WAIS-Abfragen können mit Telnet, E-Mail, einem eigenen WAIS-Client oder über WWW durchgeführt werden.

Finger: Finger ist ein Werkzeug zur Suche nach Informationen über Personen und Rechner, die an der Kommunikation im Internet beteiligt sind. Es können sowohl personenbezogene Daten (Name, E-Mail-Adresse, Telefonnummer, Arbeitszeit, öffentliche Schlüssel usw.) als auch sicherheitsrelevante Informationen über angeschlossene Rechner in Erfahrung gebracht werden.

WhoIs: WhoIs wurde speziell zur Recherche nach personenbezogenen Daten von im Internet registrierten Nutzern entwickelt. Das Vorhaben, eine Datenbank mit weltweit allen Internet-Nutzern aufzubauen, konnte nicht realisiert werden. Zur Zeit existiert eine Vielzahl von einzelnen WhoIs-Servern, auf die mit Telnet oder mit besonderer Client-Software zugegriffen werden kann.

14.2 Digitale Telekommunikationsanlagen - ISDN

14.2.1 Kontrolle von Dienstgesprächen

Ein ständig wiederkehrendes Problem beim Betrieb von TK-Anlagen ist die Frage, wie in einer Dienstvereinbarung die Kontrolle telefonischer Dienstgespräche gestaltet werden soll.

Ich empfehle folgende Regelung:

(1) Zu Zwecken der haushaltsmäßigen Kostenkontrolle können zu den Dienstgesprächen *kostenstellen- bzw. nebenstellenbezogene* Listenausdrucke angefertigt werden, welche die Daten *Anzahl der Gespräche, Gesamtdauer der Gespräche* und *Kosten* enthalten dürfen.
(2) Dienstgespräche können nach einem Stichprobenverfahren wie folgt auf Mißbrauch überprüft werden (Verhaltenskontrolle):
Für einen bestimmten Zeitraum (z. B. einen Monat) werden nach einem Zufallsverfahren so viele Dienstverbindungen oberhalb von ... (z. B. 20) Gebühreneinheiten oder einer Einzelgebühr von mehr als ... (z. B. 10,-) DM

ausgewählt, daß deren Anzahl ... (z. B. 1, 5) Prozent der Gesamtanzahl der Dienstverbindungen dieses Zeitraums beträgt.
Zu den ausgewählten Dienstverbindungen wird ein Listenausdruck angefertigt, der die Daten *Nebenstelle, Beginn- und Endezeitpunkt der Verbindung, Ziel-Ruf-Nr* enthalten darf.
Die betroffenen Nebenstellen-Inhaber sind von der Auswertung in Kenntnis zu setzen.

(3) Die Listenausdrucke sind dem Dienststellenleiter bzw. den unmittelbaren Vorgesetzten der jeweiligen Nebenstellen-Inhaber zur Überprüfung zuzuleiten. Bei begründetem Verdacht auf Mißbrauch bzw. Unverhältnismäßigkeit sind die betroffenen Nebenstellen-Inhaber ihrem Vorgesetzten gegenüber erklärungspflichtig.

(4) Bei begründetemVerdacht auf einen schwerwiegenden Verstoß gegen die Dienstvereinbarung kann auf schriftliche Weisung, z. B. des Dienststellenleiters für die letzten ... (z. B. drei) Monate eine Vollauswertung (Auswertung sämtlicher dienstlicher Verbindungsdaten) des betroffenen Nebenstellen-Inhabers vorgenommen werden. Dieser ist darüber zu unterrichten.

14.2.2 Zur Gestaltung von Dienstvereinbarungen

Die mir aufgrund von § 31 Abs. 7 Satz 1 SächsDSG zugeleiteten Entwürfe von Dienstvereinbarungen (DV) im Zusammenhang mit der Einführung oder dem bereits bestehenden Betrieb von ISDN-Anlagen sind vielfach zu unbestimmt. Die Gründe dafür dürften sein:
- Eine naturgemäß oft nur lückenhafte Kenntnis der komplizierten technischen Hard- und Software-Strukturen moderner TK-Anlagen;
- Fehlende Kenntnis der geltenden Rechtsgrundlagen;
- Ungeübtheit im Abfassen juristischer Texte.

Deshalb sollen einige Hinweise und Empfehlungen zur *Gestaltung* von DV (einschließlich des organisatorischen Umfeldes) gegeben werden. Zugrunde gelegt werden nur sog. durchschaltevermittelte TK-Anlagen für synchrone Telekommunikation (Telefon und Telefax). Sprachserver für asynchrone Telekommunikation sowie Anwendungen mit PCs als Endgeräten bzw. mit Computerkopplung werden an dieser Stelle nicht berücksichtigt.

1. Bei der *rechtlichen Auslegung* der Regelung zur *Mitbestimmung* der Personalvertretung bei "Einführung und Anwendung technischer Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Beschäftigten zu überwachen" (§ 80 Abs. 3 Nr. 16 SächsPersVG), ist zu beachten, daß es nicht darauf ankommt, ob die Dienststelle eine Kontrolle der Beschäftigten beabsichtigt. Entscheidend ist nach der Rechtsprechung des Bundesverwaltungsgerichts (BVerwG, Urteil vom 2. Februar 1990 - 6 PB 11.89, PersR 1990, 113) allein, daß eine Kontrolle *möglich* ist".

2. Bei einer ISDN-TK-Anlage ist das *Gesamtsystem mitbestimmungspflichtig*, d. h. also z. B. nicht nur die Anwendung oder Einführung von Gebührenrechnern. Die Mitbestimmung muß sich vielmehr beziehen auf:
   - alle personenbezogenen Daten, die gespeichert, abgefragt oder ausgewertet werden können: Dies sind insbesondere Inhalts-(Nutz-)daten, Verbindungs- und Leistungsmerkmalsdaten, Konfigurierungsdaten, Gebührendaten, Telefonbuchdaten, Anlagennutzungsdaten, Kontroll- und Revisionsdaten, Sicherungsdaten;
   - Betriebsführungsprogramme, die den Zugriff auf personenbezogene Leistungs- und Verhaltensdaten ermöglichen;
   - parametergesteuerte Programme, die Funktionen zur Verfügung stellen, die Verhaltens- oder Leistungskontrollen ermöglichen, etwa das Leistungsmerkmal 'Lauthören' aktivieren und deaktivieren;
   - Hardwarekomponenten, die ohne spezielle Software bereits als solche zur Verhaltens- und Leistungskontrolle objektiv geeignet sind, z. B. der Vermittlungsplatz mit dem Besetztlampenfeld oder Endgeräte mit Mikrophon und Lautsprecher.

3. *Mitbestimmungspflichtig* ist die *Konfigurierung der Anlage und der Teilnehmeranschlüsse* (Zuteilung von Leistungsmerkmalen), da hierdurch das Kommunikationsverhalten der Bediensteten indirekt beeinflußt und damit deren Verhalten geregelt sowie - jedenfalls bei kommunikationsintensiven Arbeitsplätzen - die Arbeitsplatzgestaltung beeinflußt wird (vgl. § 80 Abs. 3 Nr. 14 sowie Abs. 3 Nr. 15 SächsPersVG).

4. *Eingeschränkt mitbestimmungspflichtig* sind Maßnahmen zur Hebung der Arbeitsleistung und Erleichterung des Arbeitsablaufs sowie die Einführung grundlegend neuer Arbeitsmethoden (vgl. § 81 Abs. 3 Nr. 5 und 7 SächsPersVG). Diese Voraussetzungen liegen bei Einführung einer TK-Anlage vor.

5. Die Einführung und Nutzung einer TK-Anlage erfordert *Organisationsregelungen* zu ihrer *datenschutzgerechten Nutzung* in zweifacher Hinsicht:

- Zum individuellen 'Verhalten am Telefon' und zur Nutzung einzelner Leistungsmerkmale (Beispiele: Wer darf sich unter welchen Umständen auf andere Gespräche aufschalten? - Wie werden PIN vergeben und genutzt? - Wer darf zu wem unter welchen Umständen 'umleiten'? - Wie hat sich ein 'Vertreter', zu dem 'umgeleitet' wurde, am Telefon zu melden?);
- zur rechts- und vereinbarungsgemäßen Nutzung und zur Sicherstellung, daß Mißbrauch ausgeschlossen sowie beides kontrolliert werden kann.

6. Folgende von Dienststellenleitung und Personalrat gemeinsam zu schaffenden *Rahmenbedingungen* für die beabsichtigte Einführung einer TK-Anlage und die Erstellung einer entsprechenden DV sollten unbedingt beachtet werden:

- Keine Vorentscheidungen durch Dienststellenleitung ohne Personalratbeteiligung;
- gemeinsame Orientierung an übergeordneten Kriterien bei anzustrebenden Kompromissen;
- Basisqualifikation des Personalrats in ISDN-Technik;
- umfassende Unterrichtung des Personalrats durch Dienststellenleitung und Systemhersteller.

7. Formell sollte eine DV äußerlich aus einem Haupttext und spezifischen - im wesentlichen 'technischen' - Anhängen bestehen.

   Der *Haupttext* sollte enthalten:

   - Geltungsbereich, Gegenstand, Zweck;
   - Begriffsbestimmungen;
   - Nutzung dienstlich, privat;
   - Verbindungsdatenerfassung, -speicherung, -löschung mit Sonderregelungen;
   - Gebührendatenverarbeitung, Abrechnung von Privatgesprächen, Gebührendaten-löschung;
   - Kontrollen;
   - Protokollierungen;
   - Auskunftsrechte der Betroffenen, Rechte der Personalvertretung;
   - Fortschreibung, Kündigung, Inkrafttreten;
   - ggf. spezifische Regelungen bei Mitnutzung einer TK-Anlage (Auftragsdatenverarbeitung).

   Die *Anhänge* sollten enthalten:

   - Technik, Anlagentyp, Hard- und Software;
   - Konfiguration, Endgerätetypen;
   - Leistungsmerkmale für Teilnehmer und Vermittlung;
   - Betriebsführung, Zugriffsberechtigungen;
   - Datensicherung, Revision;
   - Physische Sicherungsmaßnahmen für Anlagenräume, Zugangsberechtigungen;
   - Wartung.

   Hervorzuheben ist, daß *Sicherungsmaßnahmen* beim Betrieb der TK-Anlage in gleich hohem Maße *wie für den Betrieb von Rechenzentren* erforderlich sind.

14.3 Entwicklung von DV-Verfahren

Die datenschutzrechtlichen Anforderungen an Soft- und Hardware werden durch die rechtlichen Regelungen bestimmt, die für die mit ihrer Hilfe durchgeführte Datenverarbeitung gelten. Soweit keine besondernen Regelungen (wie z. B. SGB X für den Sozialdatenbereich) existieren, gilt das Sächsische Datenschutzgesetz als Auffanggesetz. Dabei ist bei der Entwicklung von Softwareanwendungen vorrangig § 9 SächsDSG heranzuziehen; andere Vorschriften des Sächsischen Datenschutzgesetzes müssen jedoch ebenfalls berücksichtigt werden (§ 7 Datenverarbeitung im Auftrag, § 8 automatisiertes Abrufverfahren, § 17 bis § 20 Rechte des Betroffenen, § 31 Datenschutz im öffentlichen Dienst).

Im einzelnen verweise ich auf die entsprechenden Bekanntmachungen.[1]

Datenschutzrechtliche Anforderungen an Software nach § 9 SächsDSG lassen sich hauptsächlich zwei größeren Bereichen zuordnen, der Vorbeugung und der nachträglichen Kontrolle. Die erstere umfaßt einen breiten Bereich von Maßnahmen, die alle dem Schutz vor unberechtigten Zugriffen dienen; die nachträgliche Kontrolle erschöpft sich fast in Protokollierung. Leider wird behördenintern noch zu wenig erkannt, daß Protokolle nur sinnvoll sind, wenn sie tatsächlich ausgewertet werden. Hier eröffnet sich ein wichtiges Betätigungsfeld für jeden Vorgesetzten, evtl. mit Hilfe des behördlichen Datenschutzbeauftragten.

Zugriffschutz
In der Regel gibt es zwei Schwachstellen bei der Zugriffskontrolle: das Paßwort und die Nutzerrechte.

Hinweise zur Paßwortgestaltung geben die Empfehlungen im 1. Tätigkeitsbericht, S. 160. Dabei ist zu beachten, daß ein gangbarer Mittelweg gefunden werden muß zwischen zu geringen Anforderungen, die ein leichtes „Knacken“ ermöglichen, und zu hohen Anforderungen, die dazu führen, daß der Nutzer einen Klebezettel mit dem Paßwort am Monitor anbringt. Bei der Entwicklung ist darauf zu achten, daß eine Palette von Möglichkeiten angeboten wird, damit die Paßwortgestaltung später flexibel gehandhabt werden kann. Unbedingt notwendig sind später in der laufenden Anwendung organisatorische Regelungen (über Paßwortvergabe, Aufbewahrung für Notfälle usw.).

Als generelle Regel bei der Vergabe von Nutzerrechten sollte gelten, daß von einer

1 Zu den entsprechenden Paragraphen existieren folgende Bekanntmachungen:
- Bekanntmachung des Sächsischen Datenschutzbeauftragten zur Datenverarbeitung im Auftrag (§ 7 SächsDSG) und zur Rechtsstellung des beauftragten Unternehmers (§ 2 Abs. 2 SächsDSG), SächsABl. 1993, S. 1304 ff., 2. Tätigkeitsbericht S. 173 ff.
- Bekanntmachung des Sächsischen Datenschutzbeauftragten zur Zulässigkeit automatisierter Abrufverfahren (§ 8 SächsDSG), SächsABl. 1994, S. 976 ff., 3.Tätigkeitsbericht S. 201 ff.
- Bekanntmachung des Sächsischen Datenschutzbeauftragten zu den Maßnahmen zur Gewährleistung des Datenschutzes (§ 9 SächsDSG), SächsABl. 1994, S. 979 ff., 3. Tätigkeitsbericht S. 207 ff.
- Bekanntmachung des Sächsischen Datenschutzbeauftragten zur Auskunft nach § 17 SächsDSG, SächsABl. 1994 S. 982 ff., 3. Tätigkeitsbericht S. 214 ff.

allgemeinen Zugriffsverweigerung ausgegangen wird. Im Einzelfall können dann dem Mitarbeiter Bearbeitungsrechte erteilt werden, soweit er die personenbezogenen Daten zu seiner Aufgabenerfüllung benötigt (also auch der Behördenleiter!). Deshalb müssen schon in der Entwicklung umfassende Möglichkeiten für die Vergabe von Nutzerrechten implementiert werden. Für die spätere Rechtevergabe, die sich nach der Arbeitsorganisation der Stelle richtet, muß Flexibilität gewährleistet sein, damit nicht bei jeder Organisationsumstellung auch das Programm geändert werden muß.
Oft übersehen wird die Rolle des Systemadministrators. Hier ist zu überlegen, ob man bestimmte Administrationsaufgaben (z. B. die Rechtevergabe) dem Vier-Augen-Prinzip unterwirft. Damit kann verhindert werden, daß diese Position zu unrechtmäßigen Eingriffen mißbraucht wird, die Maßnahme dient aber auch der Absicherung des Systemadministrators, der bei möglicherweise unaufgeklärten Eingriffen dann nicht mehr allein verantwortlich gemacht werden kann.

Protokollierung
Insoweit verweise ich auf die Ausführungen im 3. Tätigkeitsbericht, S.186-191. Notwendig sind insbesondere praktikable Regelungen zur Auswertung. Protokollierung ist nur dann sinnvoll, wenn sie aus- und damit verwertbar ist. Eine Unterteilung nach unberechtigten Zugriffsversuchen, die sofort kontrolliert werden, sonstigen Nutzertätigkeiten (Bearbeiten, Recherchieren u. ä.), die stichprobenweise überprüft werden, und Administrationstätigkeiten, die in jedem Einzelfall nachgeprüft werden, bietet sich an. Eine etwas aufwendigere, aber sinnvolle Möglichkeit bei unberechtigten Zugriffsversuchen ist der Aufruf eines Spielprogrammes, wobei gleichzeitig der Systemadministrator benachrichtigt wird. Dieser kann dann sofort den Verursacher ermitteln, der meint, noch in der richtigen Anwendung zu sein.

Besonders zu beachten ist dabei, daß die Erhebung von Protokolldaten Verarbeitung von Beschäftigtendaten und die entstehende Datensammlung zur Auswertung des Leistungsverhaltens geeignet ist. Die dafür geltenden Vorschriften (namentlich § 31 SächsDSG) sind zu beachten.
Sicherung der Rechte der Betroffenen
Diese sind gerichtet auf Auskunft, Löschung, Sperrung oder Berichtigung (§§ 17-20 SächsDSG). Es sind entsprechende Tools vorzusehen, die z. B. die Erfüllung des Auskunftsanspruches des Betroffenen auf den vollständigen Datensatz gewährleisten. Auch Möglichkeiten für automatische Löschung (nach bestimmten Ereignissen, z. B. Erledigung oder nach Ablauf bestimmter Fristen) sind einzubauen. Die Löschbedingungen sollten einstellbar sein, damit bei geänderten Rahmenbedingungen (z. B. neuen gesetzlichen Vorschriften, grundlegenden gerichtlichen Entscheidungen) nicht das Programm geändert werden muß.
Entwicklungsverfahren mit Testdaten
Oft werden bei Entwicklung und Testbetrieb Echtdaten verwendet. Einige datenschutzrechtliche Probleme könnten vermieden werden, wenn stattdessen bei der Entwicklung Testdaten verwendet werden. Zwar wird oft behauptet, daß nur Echtdaten eine dem zu lösenden Problem adäquate Lösung ermöglichen. Jedoch kann durch eine ausreichende Anonymisierung von Echtdaten ein geeigneter Testdatensatz erzeugt

werden. Zum Beispiel können in einer hinreichend großen Gruppe von Antragstellern nach dem Zufallsprinzip die einzelnen Daten vermischt werden (Vorname von A, Familienname von B, Wohnort von Mitarbeiter C, Grundstück von D usw.). Der so entstandene Datenbestand kann bei Bedarf durch fiktive Daten ergänzt werden.

Im Falle der Verwendung einer solchen Testdatenbank könnten Änderungen und Neueinfügungen getestet werden, gegen die sich sonst starke datenschutzrechtliche Bedenken erhöben. Auch Detailfragen, z. B. welche Rechte im Testbetrieb vergeben werden, wären dann entschärft. Der Testbetrieb mit Echtdaten bliebe dann nach umfangreichen Kontrollmaßnahmen und Beteiligungen einer abschließenden Phase vorbehalten. Notwendig ist dabei natürlich auch die hardwareseitige Trennung der Entwicklungsarbeiten vom laufenden Betrieb.

Wird eine Fremdfirma mit der Entwicklung beauftragt, so sind bei der Verwendung personenbezogener Daten die Regelungen über die Datenverarbeitung im Auftrag (§ 7 SächsDSG) zu beachten.

14.4 Wartung / Fernwartung

Wartung und Fernwartung durch Dritte ist nach meinem Dafürhalten Datenverarbeitung im Auftrag gemäß § 7 SächsDSG. Fernwartung darf nur genutzt werden, wenn keine andere Möglichkeit zur Fehlerbehebung existiert. Insbesondere muß geprüft werden, ob das noch vorhandene Risiko eines unberechtigten Zugriffs auf personenbezogene Daten in Anbetracht der Sensibilität der Daten akzeptiert werden kann. Die Zugriffsrechte des Wartungspersonals sind auf ein Minimum zu beschränken.

Im Wartungsvertrag sind - schriftlich - klare Regelungen hinsichtlich der Abgrenzung der Befugnisse und Pflichten zwischen Wartungspersonal und Personal der verantwortlichen Stelle zu treffen. Insbesondere sind Art und Umfang der Wartung festzulegen. Grundsätzlich sollte das Wartungspersonal auf das Datengeheimnis verpflichtet werden. Falls personenbezogene Daten bei der Fernwartung übertragen werden, ist ihre Nutzung für andere Zwecke vertraglich zu untersagen. Die Daten sind ausschließlich für Zwecke der Wartung zu verwenden. Nach Abschluß der Arbeiten sind diese Daten unverzüglich zu löschen.
Für eine Fernwartung sind zusätzlich folgende Maßnahmen erforderlich:

Um eine Nutzung der Fernwartungsleitung durch Unbefugte auszuschließen, sollte die Dialogverbindung nur durch den Systemverwalter des zu wartenden Rechners aufgebaut werden. Der Verbindungsaufbau sollte automatisch über festgelegte Rufnummern erfolgen, die im Rechner einprogrammiert oder hardwaremäßig eingestellt sind. Der Wartungstechniker muß sich darüber hinaus bei jedem Wartungsvorgang erneut durch ein vereinbartes Paßwort autorisieren.

2. Fernwartungsaktivitäten sollten von seiten des Auftraggebers mitverfolgt und ggf. unterbrochen werden können. Hierzu sollte ein Systemexperte bei der Anlage zur

Verfügung stehen.
3. Der Zugriff auf personenbezogene Daten kann dadurch ausgeschlossen werden, daß solche Daten nur auf Verzeichnissen oder Datenträgern gespeichert werden, die während des Wartungsvorganges nicht verfügbar sind.
4. Der Wartungstechniker sollte keinen Systemverwalterstatus erlangen können. Sofern eine physikalische Abkopplung der Dateien mit personenbezogenen Daten nicht möglich ist, ist das Einspielen von Änderungen ins Betriebssystem und in systemnahe Software durch die Fernwartungszentrale abzulehnen und ausschließlich an Ort und Stelle durchzuführen Die Übernahme der Änderung ist erst nach Freigabe der speichernden Stelle vorzunehmen.
5. Sämtliche Fernwartungsaktivitäten sind revisionssicher aufzuzeichnen. Die Protokolle müssen durch entsprechende Kommandos oder Dienstprogramme kontrolliert und ausgewertet werden können. Sie sind vor Manipulationen zu schützen.

14.5 Datenfernübertragung

Immer mehr Behörden greifen in ihrer Arbeit auf Datenfernübertragung zurück. Die folgenden Überlegungen stellen erste grundlegende Anforderungen dar.

Der technische Fortschritt führt zu niedrigen Preisen, z. B. wird die Verschlüsselung mittlerweile „Stand der Technik“; sie ist schon preiswert zu haben. Zu Fragen der Datenfernübertragung bei der Internet-Benutzung bietet Abschnitt 14.1 eine Arbeitshilfe.

Beim Anschluß an ein öffentliches Netz über Wählanschlüsse müssen zusätzliche Hard- und Software-Einrichtungen (z. B. Modem mit Rückruf, Modem mit Schalter) oder Einschränkungen der Verbindungen (z. B. nur abgehende Rufe, nur ankommende Rufe, ggf. mit Zeitbeschränkungen) oder die Einrichtung von geschlossenen Benutzergruppen zur sicheren Kommunikation eingesetzt werden.

Neben einer gesicherten Übertragungsleitung muß der Zutrittsschutz für die Kopplungstechnik (z. B. Brücken, Router, Gateway) und evtl. eine Filterung der Informationsströme in der Kopplungstechnik nach Quell- oder Zieladresse, Protokolltyp usw. gewährleistet sein.

Für die Übertragung sensibler personenbezogener Daten empfiehlt sich der Einsatz von Standleitungen (feste Punkt-zu-Punkt-Verbindung), da hier ein Anwählen von außen nicht möglich ist. Allerdings besteht auch hier die Gefahr des physischen Angriffs auf die Leitung.

Damit während der Kommunikation keine unzulässige Änderung von Daten stattfindet und die Information während der Übertragung keinen nichtautorisierten Personen zur Kenntnis gelangt, sind zumindest sensible personenbezogene Daten durch

kryptographische Verfahren und andere Verfahren (z. B. Prüfsummenverfahren, elektronische Unterschrift) zu schützen.

14.6 Dienstliche Nutzung privater Hard- und Software

In öffentlichen Verwaltungen wird vielfach private Hard- und Software auch für dienstliche Zwecke eingesetzt. Meist werden dabei keine hinreichenden Sicherheitsvorkehrungen getroffen, so daß eine den Vorschriften des Sächsischen Datenschutzgesetzes entsprechende Datenverarbeitung nicht gewährleistet ist.

Welche Gefahren bestehen bei dienstlicher Nutzung privater Hard- und Software?

- Der Dienstherr ist abhängig vom privaten Arbeitsmittel, über das er keine Verfügungsgewalt besitzt.
- Aus Kostengründen wird vor allem beim privaten Rechner meist auf die oft teure Sicherheitssoft- und -hardware verzichtet. Ein unzureichend gesicherter MS-DOS-PC ist aber für eine Verarbeitung personenbezogener Daten nicht geeignet, wie bereits im 2. Tätigkeitsbericht des Sächsischen Datenschutzbeauftragten unter 14.1 ausführlich dargelegt wurde.
- Besonders problematisch ist es, wenn tragbare Computer, wie z. B. Laptop oder Notebook, sowohl dienstlich als auch privat genutzt werden. Zu der Gefahr einer unbefugten Kenntnisnahme durch Dritte kommt die durch den häufigen Transport des Rechners erhöhte Gefahr eines Diebstahls oder Verlustes des Gerätes hinzu. Die darauf gespeicherten personenbezogenen Daten könnten in fremde Hände gelangen. Deshalb sind für tragbare Rechner unbedingt zusätzliche Sicherheitsmaßnahmen vorzusehen, die die gespeicherten personenbezogenen Daten auch nach einem Diebstahl vor unbefugter Kenntnisnahme sichern, wie z. B. Verschlüsselung.
- Dienstlich eingesetzte Programme und Daten werden auf privaten Rechnern häufig nicht regelmäßig gesichert und sind dann im Schadensfall nicht sofort wieder herstellbar.

Werden öffentliche Verwaltungen zunehmend mit Rechnern ausgestattet, so daß eine dienstliche Nutzung privater Hardware immer seltener wird, so bleibt die Problematik des Einsatzes privater Software doch unvermindert bestehen. Vor allem motivierte Mitarbeiter sind häufig mit der dienstlich installierten Software unzufrieden, weil sie zu Hause oft komfortablere Software oder eigene, besser dafür geeignete Programme entwickelt haben und diese auch im Dienst einsetzen möchten. Die “private” Software wird dann vom Mitarbeiter per Diskette auf den dienstlichen PC installiert. Dabei wird die Gefahr, schädliche Programme oder Viren “einzuschleppen”, häufig nicht beachtet. Oft bleibt die Schädigung der Programme oder Datenbestände lange Zeit unerkannt, bis Funktionsstörungen oder gar der Ausfall des ganzen Systems darauf hinweisen.

Deshalb sollte durch schriftliche Weisungen grundsätzlich der Einsatz privater Hard-

und Software zur dienstlichen Aufgabenerfüllung untersagt werden.

Für besondere Fälle besteht jedoch die Möglichkeit, eine Ausnahmeregelung für eine befristete Zeit zu erteilen, wenn die Aufgabenerfüllung der Dienststelle durch den Einsatz privater Hard- oder Software wesentlich verbessert werden könnte und die Sicherheitsrisiken beherrschbar sind.
Eine Entscheidung darüber müßte schriftlich durch die für die Fachaufgabe verantwortliche Stelle unter Beteiligung des behördlichen Datenschutzbeauftragten getroffen werden. Dabei ist außerdem zu beachten, dass

- die privaten Datenträger (Disketten) vor einer Installation auf einem Einzelplatz-PC mit entsprechenden Virenscannern geprüft werden,
- die private Hardware vor dem dienstlichen Einsatz auf evtl. vorhandene schädliche Programme, Viren usw. getestet wird,
- bereits vorhandene private Programme und Daten gelöscht werden, damit nunmehr nur dienstlich freigegebene Software eingesetzt wird,
- der Rechner nicht mehr zwischen Dienststelle und Wohnung hin und her transportiert wird,
- andere Mitarbeiter zur Aufgabenerfüllung auch bei Abwesenheit des Eigentümers auf den Rechner zugreifen können.

Bevor der Rechner wieder der ausschließlich privaten Nutzung zugeführt wird, müssen alle dienstlichen Programme und Daten so gelöscht werden, daß eine Reproduktion auch mit großem Aufwand nicht mehr möglich ist.
Neben einer Anweisung, die den grundsätzlichen Verzicht auf private Hard- und Software zur dienstlichen Aufgabenerfüllung vorschreibt, rege ich an, daß jeder PC-Benutzer zusätzlich zur evtl. gesetzlich erforderlichen Verpflichtung auf das Datengeheimnis eine besondere PC-Verpflichtungserklärung für die Benutzung von Rechnern zur Kenntnis nimmt und unterschreibt.

Ein Muster für eine solche PC-Verpflichtungserklärung ist in der Zeitschrift für Kommunikations- und EDV-Sicherheit (KES 95/4 S. 44) abgedruckt und kann als Vorlage für öffentliche Verwaltungen dienen.

Die PC-Verpflichtungserklärung dient der ordnungsgemäßen Datenverarbeitung. In ihr werden die wichtigsten Datensicherheitsmaßnahmen aufgeführt. Sie verbietet auch den Einsatz von privater Hard- und Software, In Sonderheit unlizenzierter und selbsterstellter Programme.

14.7 Löschung bzw. Vernichtung magnetischer Datenträger

Datenträger dienen der Datenerfassung, der Datenspeicherung und dem Datentransport. Datenträger sind z. B. Belege, Listen, Formulare, Protokolle und Zeichnungen, deren Inhalt unmittelbar gelesen werden kann. Dazu gehören aber auch maschinenlesbare Datenträger, wie z. B. Lochkarte, Lochstreifen, Mikrofilm und magnetische Datenträger (Magnetband, Streamer-/Magnetbandkassette, Diskette, Identifikationskarte mit Magnetstreifen, Magnetplatte).

Werden Datenträger nicht mehr benötigt, z. B. nach Ablauf von Aufbewahrungsfristen, sind sie zu löschen bzw. zu vernichten. Das Löschen stellt bekanntlich eine Phase der Verarbeitung personenbezogener Daten dar (§ 3 Abs. 2 SächsDSG). Damit unterliegt auch die Löschung bzw. Entsorgung von Datenträgern den Vorschriften des Sächsischen Datenschutzgesetzes (siehe auch 1. Tätigkeitsbericht unter 14.1.2, 3. Tätigkeitsbericht unter 14.6).

Sollen magnetische Datenträger wiederverwendet oder vernichtet werden, müssen zuvor die darauf gespeicherten personenbezogenen Daten (physisch) gelöscht werden, um sie vor unbefugter Kenntnisnahme zu schützen. Logisches Löschen ist unzureichend.

Magnetische Datenträger können physisch gelöscht werden durch:

1. Neuformatieren oder Überschreiben mit einer zufälligen Zeichenfolge
   - durch Aufruf spezieller Betriebssystemanweisungen oder
   - durch Aufruf entsprechender Dienstprogramme/Tools (z. B. WipeInfo, Wipefile, Wipedisk von Norton Utilities bzw. PC-Tools)

2. Löschgeräte

Das Löschen mit geeigneter Software durch (möglichst mehrfaches) Überschreiben der gespeicherten personenbezogenen Daten ist nur bei einem noch funktionstüchtigen magnetischen Datenträger möglich. Ist dies nicht der Fall, können Löschgeräte oder Dauermagnete eingesetzt werden, um die gespeicherten personenbezogenen Daten unkenntlich zu machen. Beim Löschen mit Löschgeräten oder Dauermagneten wird der gesamte magnetische Datenträger einem starken externen Magnetfeld ausgesetzt, das die gespeicherten Informationen löscht.

Die Norm DIN 33858 ”Löschen von schutzbedürftigen Daten auf magnetischen Datenträgern” legt dafür meßbare Kriterien, wie magnetische Feldstärke (Koerzitivkraft) und Löschdämpfung, fest.

Bei sachgerechter Anwendung können Löschgeräte magnetische Datenträger so löschen, daß eine Reproduktion der Daten auch mit großem Aufwand nicht mehr möglich ist. Allerdings beschränkt sich das Löschen mit Löschgeräten aus

physikalischen Gründen hauptsächlich auf flexible magnetische Datenträger (Diskette, Magnetband, Streamer-/Magnetbandkassette). Magnetplatten (Wechsel- und Festplatten) einer bestimmten Größe können mit derzeit bekannten Löschgeräten nicht gelöscht werden.

Besonders problematisch ist es, defekte Magnetplatten, auf denen noch personenbezogene Daten gespeichert sind und die aufgrund eines Hardwarefehlers nicht mehr überschrieben werden können, zu entsorgen. Falls ein Löschen mit einem Löschgerät nicht möglich ist, kommt dann nur manuelles (evtl. unzureichendes) Löschen mit einem Dauermagneten oder mechanisches Zerstören (z. B. Schreddern) in Frage.

Allerdings ist dies im Garantiefall nicht möglich. Während der Garantiezeit wird eine defekte Magnetplatte, die im System nicht mehr ansprechbar und damit nicht mehr löschbar ist, in der Regel vor Ort beim Kunden repariert oder ausgetauscht. Beim Austausch geht die defekte Magnetplatte mit allen darauf gespeicherten Daten in den Besitz des Lieferanten über. Dieser kann sie reparieren, evtl. mit einigem Aufwand auch den Inhalt rekonstruieren und sie mißbräuchlich nutzen. Aber auch hier kann eine datenschutzgerechte Behandlung, vereinbart durch entsprechende vertragliche Klauseln mit dem Lieferanten, erreicht werden.

Sollen magnetische Datenträger vernichtet werden, kann dies von der speichernden Stelle selbst oder durch ein Entsorgungsunternehmen durchgeführt werden. Vernichtet der Eigentümer (speichernde Stelle) die magnetischen Datenträger selbst, so ist er verpflichtet, alle personellen, technischen und organisatorischen Maßnahmen gemäß § 9 SächsDSG, namentlich Zugangskontrolle, Datenträgerkontrolle, Transportkontrolle und Organisationskontrolle, zu beachten. Wird ein Entsorgungsunternehmen mit der Vernichtung magnetischer Datenträger im Auftrag eingesetzt, sind neben den bereits zuvor aufgeführten Maßnahmen zu § 9 SächsDSG noch die Auftragskontrolle sowie die gesetzlichen Anforderungen gemäß § 7 SächsDSG zur Datenverarbeitung im Auftrag zu beachten. Dabei hat der Auftraggeber den Auftragnehmer unter besonderer Berücksichtigung der Eignung der von diesem getroffenen personellen, technischen und organisatorischen Maßnahmen sorgfältig auszuwählen, der Auftrag ist schriftlich zu erteilen. (Näher dazu meine Bekanntmachung vom 3. November 1993, SächsABl. S. 1304, 2. Tätigkeitsbericht S. 173 ff., unter I).
Auftragsdatenverarbeitung zum Löschen bzw. Vernichten von magnetischen Datenträgern kann folgende Aufgaben beinhalten:

Der Auftraggeber (speichernde Stelle) beauftragt schriftlich einen *geeigneten* Auftragnehmer, der den magnetischen Datenträger im Haus des Auftraggebers löscht. Ein sachkundiger Mitarbeiter des Auftraggebers ist dabei anwesend.

Der Auftraggeber (speichernde Stelle) beauftragt schriftlich einen *geeigneten* Auftragnehmer, den defekten Datenträger abzuholen und dann unverzüglich extern zu löschen.

Der Auftraggeber (speichernde Stelle) beauftragt schriftlich einen *geeigneten* Auftragnehmer, den defekten Datenträger im Beisein eines sachkundigen

Mitarbeiters des Auftraggebers abzuholen und in der Firma des Auftragnehmers in Anwesenheit des Mitarbeiters (der speichernden Stelle) zu löschen. Anschließend geht der Datenträger in die Verfügungsgewalt des Auftragnehmers über.

In jedem Fall muß vertraglich gesichert sein, daß der Auftragnehmer die ihm anvertrauten personenbezogenen Daten nur entsprechend den Weisungen des Auftraggebers nutzen darf und daß Personen, denen diese Daten zugänglich sind, auf die Einhaltung des Datengeheimnisses verpflichtet sind.

Ein datenschutzgerechter Mustervertrag für die Entsorgung von Datenträgern ist in der Zeitschrift Datenschutz-Berater (DSB 1995, Heft 1 S. 7 ff.) abgedruckt und kann als Vorlage für abzuschließende Verträge dienen.

14.8 Zugangskontrolle - Datenerfassung beim Pförtner

Vielfach werde ich gefragt, ob es zulässig sei, wenn beim Besuch von Behörden, Ministerien oder auch von Einrichtungen wie z. B. Asylbewerberunterkünften die Personalausweisnummer vom Pförtner notiert wird.

1. Für eine ordnungsgemäße Zugangskontrolle reicht es aus, im Besucherbuch oder besser auf einzelnen Erfassungsbögen festzuhalten, wer (Name, Anschrift) wann (Datum, Zeit des Kommens und Gehens) wen besucht hat.
   Die Speicherung der Personalausweisnummer anstelle der Anschrift (Wohnort, Straße, Hausnummer) ist kein geeignetes Mittel zur Identifizierung des Besuchers. Außerdem enthält eine Personalausweisnummer (weitere) personenbezogene Daten (z. B. Geburtsdatum), die für eine Zugangskontrolle nicht erforderlich sind. Hinzu kommt, daß dem Besucher in der Regel nicht bewußt ist, daß seine Paß-/Personalausweisnummer erhoben und in das Besucherbuch eingetragen wird. Gemäß § 11 Abs. 2 Satz 1 SächsDSG sind jedoch personenbezogene Daten grundsätzlich beim Betroffenen mit seiner Kenntnis zu erheben. Die Erhebung der Paß-/Personalausweisnummer ohne Kenntnis des Betroffenen verstößt gegen § 11 Abs. 3 SächsDSG, weil weder ein Gesetz noch eine Rechtsverordnung eine solche Datenerhebung zuläßt.

   Die Paß-/Personalausweisnummer darf - auch im Hinblick auf Nr. 16.2 der Allgemeinen Verwaltungsvorschrift zur Durchführung des Paßgesetzes vom 2. Januar 1988 nicht erhoben werden, zumal sie für die Aufgabenerfüllung nicht erforderlich ist. Bereits gespeicherte Personalausweisnummern sind unverzüglich zu löschen (z. B. durch Schwärzen oder durch Schreddern der vorhandenen Bücher oder Erfassungsbögen).

2. Die Aufforderung zur Vorlage des Personalausweises zur Identitätsfeststellung halte ich für unproblematisch. Da es in Deutschland keine Verpflichtung gibt, den Personalausweis mitzuführen, kommen aber auch alle anderen Möglichkeiten in Betracht, die Identität festzustellen (z. B. Führerschein; Anruf zu Hause; Bestätigung durch andere Person).

1. Die Aufbewahrungsdauer der gespeicherten Besucherdaten sollte aus datenschutzrechtlichen Gründen folgendermaßen geregelt werden:

   Die Speicherung personenbezogener Daten ist nur zulässig, wenn es zur (rechtmäßigen) Aufgabenerfüllung erforderlich ist. Die (rechtmäßige) Aufgabenerfüllung kann z. B. aus dem Hausrecht oder der Wohnheimordnung hergeleitet werden.
   Der Grundsatz der Erforderlichkeit beschränkt die Speicherung jedoch in zeitlicher Hinsicht. Erforderlich ist die Speicherung nur so lange und nur in dem Umfang, wie die Aufgabe der Zugangskontrolle als präventive Maßnahme zur Gefahrenabwehr aktuell ist. Daher dürfte eine Aufbewahrungsfrist für die gespeicherten personenbezogenen Daten von ca. 2 Wochen ausreichend sein. Weil die fristgerechte Löschung bei der Speicherung in einem Besucherbuch nicht praktiziert werden könnte, sollten statt dessen einzelne Erfassungsbögen verwendet werden. Diese könnten spätestens nach zwei Wochen problemlos datenschutzgerecht vernichtet werden. Die evtl. geführten Besucherbücher sollten bald vernichtet werden.

14.9 Gestaltung von Behördenpost

Von einem Petenten erhielt ich den Brief einer Gemeinde, aus dessen Sichtfenster neben der Adresse auch die Tatsache ersichtlich war, daß er *Schuldner* der Gemeindeverwaltung ist (Adressierung: "als Gesamtschuldner"). Hierdurch bestand die Gefahr, daß dieses sensible personenbezogene Datum, das auch zu Mißverständnissen führt, einem unberechtigten Empfängerkreis zur Kenntnis gelangt (z. B. dem Nachbarn, der die Post des Adressaten während des Urlaubs entgegennimmt).

Ich habe von der Stadtverwaltung verlangt, künftig nur noch Briefumschläge zu verwenden, die § 9 Abs. 1 SächsDSG entsprechen. Danach haben öffentliche Stellen alle Maßnahmen zur Gewährleistung des Datenschutzes zu treffen. Aus dem Fenster im Briefumschlag von Behördenpost darf *nur* die Adresse des Empfängers und der Absender ersichtlich sein.

Der Bürgermeister der Gemeindeverwaltung hat seine Bediensteten angewiesen, künftig datenschutzgerechte Briefumschläge zu verwenden.

15 Vortrags- und Schulungstätigkeit

Eine im Berichtszeitraum weiterhin gestiegene Zahl von Eingaben belegt, welch wichtiges Anliegen vielen die Selbstbestimmung über ihre eigenen Daten ist. Zugleich ließen zahlreiche Wünsche öffentlicher Stellen nach Informations- und Diskussionsveranstaltungen eine zunehmende Sensibilisierung der Behörden für

Belange des Datenschutzes erkennen. Die Angehörigen meiner Dienststelle und ich waren deshalb auf Seminaren, auf Tagungen und in Vorträgen bemüht, die Kenntnisse der 'Datenschutzmultiplikatoren' im öffentlichen Bereich zu vertiefen und weiteres Interesse zu wecken. Von besonderem Stellenwert war hier meine zentrale Fortbildungsveranstaltung 1996 in Delitzsch.

16 Materialien

16.1 Entschließungen der 50. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 9./10. November 1995 in Bremen

16.1.1 Zur Weiterentwicklung des Datenschutzes in der Europäischen Union

Die Konferenz der Datenschutzbeauftragten der Europäischen Union hat am 8. September 1995 in Kopenhagen in einer Resolution im Hinblick auf die für 1996 geplante Regierungskonferenz dafür plädiert, anläßlich der Überarbeitung der Unions- und Gemeinschaftsverträge in einen verbindlichen Grundrechtskatalog ein einklagbares europäisches Grundrecht auf Datenschutz aufzunehmen. Die Schaffung rechtsverbindlicher Datenschutzregelungen für die Organe und Einrichtungen der Union sowie die Schaffung einer unabhängigen und effektiven Datenschutzkontrollinstanz der EU werden angemahnt. Dieser Resolution schließt sich die Konferenz der Datenschutzbeauftragten des Bundes und der Länder an. Sie hält angesichts der fortschreitenden Integration und des zunehmenden Einsatzes von Informations- und Kommunikationstechnologien in der EU eine Weiterentwicklung des Datenschutzes im Rahmen der EU für geboten.

Sie fordert die zuständigen Politiker und insbesondere die Bundesregierung auf, dafür einzutreten, daß im EU-Vertragsrecht ein Grundrecht auf Datenschutz aufgenommen wird, die materiellen Datenschutzregelungen in der EU verbessert werden, das Amt eines Europäischen Datenschutzbeauftragten geschaffen wird sowie eine parlamentarische und richterliche Kontrolle der Datenverarbeitung der im EU-Vertrag vorgesehenen Instanzen sichergestellt wird.

Grundrecht auf Datenschutz

Bei einer Weiterentwicklung der Europäischen Union ist es unabdingbar, daß dem Grundrechtsschutz eine angemessene Bedeutung beigemessen wird. Dies sollte dadurch geschehen, daß die Verträge zur Europäischen Union mit einem Grundrechtskatalog ergänzt werden. Mit einer Entschließung vom 10. Februar 1994 hat das Europäische Parlament einen Entwurf zur Verfassung der Europäischen Union zur Erörterung

gestellt, der u. a. folgende Aussagen enthält: "Jeder hat das Recht auf Achtung und Schutz seiner Identität. Die Achtung der Privatsphäre und des Familienlebens, des Ansehens (...) wird gewährleistet".

Die Konferenz der Datenschutzbeauftragten ist mit ihrer Entschließung vom 28. April 1992 dafür eingetreten, daß in das Grundgesetz nach dem Vorbild anderer europäischer Verfassungen ein Grundrecht auf Datenschutz aufgenommen wird. Sie hat hierfür einen Formulierungsvorschlag gemacht. Auf ihren Konferenzen am 16./17. Februar 1993 und 9./10. März 1994 bekräftigten die Datenschutzbeauftragten des Bundes und der Länder ihre Position. Diese Forderung wurde aber wegen des Nichterreichens der notwendigen qualifizierten Mehrheit durch den Gesetzgeber nicht umgesetzt.

In Wirtschaft, Verwaltung und Gesellschaft der Staaten der EU erhält der Dienstleistungs- und Informationssektor eine zunehmende Bedeutung. Dies hat zur Folge, daß mit hochentwickelten Informationstechnologien von privaten wie von öffentlichen Stellen verstärkt personenbezogene Daten verarbeitet und auch grenzüberschreitend ausgetauscht werden. Diese Entwicklung wird gefördert durch die Privatisierung und den rasanten Ausbau transeuropäischer elektronischer Telekommunikations-Netze. Dadurch gerät das Grundrecht auf informationelle Selbstbestimmung in besonderem Maße auf der überstaatlichen Ebene in Gefahr. Dieser Gefahr kann dadurch entgegengetreten werden, daß in einen in den überarbeiteten EU-Vertrag aufzunehmenden Grundrechtskatalog das Grundrecht auf Datenschutz und zu dessen Konkretisierung ein Recht auf unbeobachtete Telekommunikation aufgenommen werden. Dies hätte folgende positive Auswirkungen:

- Anhand einer ausdrücklichen gemeinsamen Rechtsnorm kann sich eine einheitliche Rechtsprechung zum Datenschutz entwickeln, an die sowohl die EU-Organe wie auch die nationalen Stellen gebunden werden.
- Ein solches Grundrecht wäre die Basis für eine Vereinheitlichung des derzeit noch sehr unterschiedlichen nationalen Datenschutzrechts auf einem hohen Niveau.
- Den Bürgerinnen und Bürgern wird deutlich erkennbar, daß ihnen in einklagbarer Form der Datenschutz in gleicher Weise garantiert wird wie die traditionellen Grundrechte.
- Das grundlegende rechtsstaatliche Prinzip des Datenschutzes wird dauerhaft, auch bei Erweiterung der EU, gesichert.
- Mit der rechtlichen Konkretisierung eines Rechts auf unbeobachtete Telekommunikation würde der zunehmenden Registrierung des Verhaltens der Bürgerinnen und Bürger in der multimedialen Informationsgesellschaft entgegengewirkt und der Schutz des Fernmeldegeheimnisses auch nach dem Abbau der staatlichen Monopole im Sprachtelefondienst sichergestellt.

Materielle Datenschutzregelungen

Mit der kürzlich verabschiedeten EU-Datenschutzrichtlinie wird ein großer Fortschritt

für den Datenschutz auf europäischer Ebene erreicht. Dies darf aber nicht den Blick dafür verstellen, daß in einzelnen Bereichen spezifische, dringend nötige Datenschutzregelungen fehlen. Insbesondere sind folgende Bereiche regelungsbedürftig:

- Es bedarf eines für die EU-Institutionen verbindlichen eigenen Datenschutzrechts. Die datenschutzrechtliche Verantwortung der Mitgliedsstaaten einschließlich ihrer Datenschutzkontrolle der Übermittlung von Daten an EU-Institutionen bleibt dabei unberührt.
- Die geplante ISDN-Datenschutzrichtlinie darf weder einer völlig falsch verstandenen Subsidiarität zum Opfer fallen noch in unzureichender Form verabschiedet werden.
- Die im Bereich der Statistik bestehenden datenschutzrechtlichen Defizite sind abzubauen.
- Es soll eine Technikfolgenabschätzung bei der Förderung und Einführung neuer Informationstechniken mit Personenbezug durch die EU obligatorisch eingeführt werden.
- In den Bereich Inneres und Justiz sind aufeinander abgestimmte verbindliche Regelungen mit hohem Datenschutzstandard, die die Datenverarbeitung in Akten und die Sicherung der Datenschutzkontrolle mit umfassen, zu schaffen.
- Es bedarf der Harmonisierung des Arbeitnehmerdatenschutzes auf hohem Niveau in den Staaten der EU.
- Für das Personal der EU-Organe ist der Arbeitnehmerdatenschutz sicherzustellen, was z. B. bei der Durchführung von Sicherheitsüberprüfungen insbesondere unter Beteiligung von Behörden der Heimatstaaten von großer Bedeutung ist.

Es ist zu prüfen, inwieweit Informationszugangsrechte in weiteren Bereichen eingeführt werden sollen.

Europäischer Datenschutzbeauftragter

Die Konferenz der EU-Datenschutzkontrollinstanzen (25./26. Mai 1994, 8. September 1995) und die Konferenz der Datenschutzbeauftragten des Bundes und der Länder (25. August 1994) haben darauf hingewiesen, daß es an einer unabhängigen und effektiven Datenschutzkontrollinstanz fehlt, an die sich jeder wenden kann, wenn er der Ansicht ist, bei der Verarbeitung seiner personenbezogenen Daten durch Stellen der EU in seinen Rechten verletzt zu sein. Aufgabe eines Europäischen Datenschutzbeauftragten sollte die Behandlung aller Datenschutzbelange der EU sein. Dazu gehört nicht nur die Bearbeitung von Betroffeneneingaben, sondern auch die datenschutzrechtliche Beratung der EU-Organe und -Einrichtungen sowie deren anlaßunabhängige Kontrolle, die Begleitung informationstechnischer EU-Projekte und der entsprechenden EU-Normsetzung sowie die Zusammenarbeit mit den nationalen Kontrollinstanzen. Wegen der teilweise anders gelagerten Aufgaben sollen die Funktionen des Europäischen Datenschutzbeauftragten und des Bürgerbeauftragten nach den EG-Verträgen nicht vermengt werden. Die Bundesregierung sollte im Rahmen der Vorbereitung der

Regierungskonferenz 1996 darauf hinwirken, daß ein unabhängiger Europäischer Datenschutzbeauftragter in den Verträgen über die Europäische Union institutionell abgesichert wird.

Parlamentarische und richterliche Kontrolle

Bei der Zusammenarbeit der EU-Staaten in den Bereichen Justiz und Inneres muß mit Besorgnis festgestellt werden, daß eine ausreichende parlamentarische und richterliche Kontrolle im EU-Vertrag derzeit nicht gewährleistet ist. Die geplante Europol-Konvention ist hierfür ein Beispiel. Mit unbestimmten Formulierungen werden einem fast völlig freischwebenden Europäischen Polizeiamt informationelle Befugnisse eingeräumt, einem Amt, das keiner parlamentarischen Verantwortlichkeit und nur einer unzureichenden (teils nur nationalen) Rechtskontrolle unterworfen wird. Zur Wahrung des Datenschutzes bei der Umsetzung gemeinsamer Maßnahmen in den Bereichen Justiz und Inneres muß daher - unbeschadet der Kontrolle durch die nationalen Datenschutzbehörden - auch eine im Rahmen ihrer jeweiligen Zuständigkeiten lückenlose Kontrolle durch die nationalen Parlamente und Gerichte sowie durch das Europäische Parlament und den Europäischen Gerichtshof sichergestellt werden.

16.1.2 Zu Planungen für ein Korruptionsbekämpfungsgesetz

Derzeit gibt es Vorschläge, die Bekämpfung der Korruption durch Verschärfungen des Strafrechts und des Strafprozeßrechts mit weiteren Eingriffen in das Grundrecht auf informationelle Selbstbestimmung zu organisieren. Ein Beispiel dafür ist der Beschluß des Bundesrates vom 3. November 1995 zur Einbringung eines Korruptionsbekämpfungsgesetzes.

Nach dem vom Bundesrat beschlossenen Gesetzentwurf sollen Bestechlichkeit und Bestechung in den Kreis derjenigen Tatbestände aufgenommen werden, bei deren Verdacht die Überwachung des Fernmeldeverkehrs und der Einsatz technischer Mittel ohne Wissen des Betroffenen (§§ 100a, 100c StPO) angeordnet werden dürfen.

Die Datenschutzbeauftragten weisen demgegenüber darauf hin, daß es vorrangig um Prävention, nicht um Repression geht. Die Datenschutzbeauftragten treten für eine entschlossene und wirksame Bekämpfung der Korruption mit rechtsstaatlichen Mitteln unter strikter Beachtung der Freiheitsrechte ein.

Sie wenden sich zugleich gegen eine Rechtspolitik, welche - noch bevor sie sich darüber im klaren ist, was die bisherigen Verschärfungen und Eingriffe an Vorteilen und an Nachteilen gebracht haben - auf weitere Verschärfungen und Eingriffe setzt.

Gerade gegenüber der Korruption gibt es Möglichkeiten, welche Effektivität versprechen und gleichwohl die Privatsphäre der unbeteiligten und unschuldigen Bürgerinnen und Bürger nicht antasten:

- Rotation derjenigen Mitarbeiterinnen und Mitarbeiter einer Behörde, deren Position und Aufgaben erfahrungsgemäß für Bestechungsversuche in Betracht kommen;
- Vier- und Sechsaugenprinzip bei bestimmten Entscheidungen;
- Trennung von Planung, Überwachung und Ausführung, von Ausschreibung und Vergabe;
- Prüfverfahren und Innenrevision;
- Codes of Conduct (formalisierte "Ethikprogramme") im Bereich der Wirtschaft;
- verbesserte Transparenz von Entscheidungsprozessen in der Verwaltung.

Die in den Gesetzentwürfen vorgesehene weitere Einschränkung von Grundrechten, die mit einer abermaligen Erweiterung der Telefonüberwachung verbunden wäre, ist nur vertretbar, wenn sie nach einer sorgfältigen Güter- und Risikoabwägung zusätzlich zu den o. g. Verfahrens- und Verhaltensmaßregeln als geeignet und unbedingt erforderlich anzusehen wäre.

Die Datenschutzbeauftragten verlangen, daß vor einer zusätzlichen Aufnahme von Straftatbeständen in den Katalog der Abhörvorschrift des § 100a StPO diese Abwägung durchgeführt wird.

Die Datenschutzbeauftragten fordern weiterhin, daß eine Erweiterung des genannten Straftatenkataloges nur befristet vorgenommen wird, damit sich vor einer Verlängerung die Notwendigkeit stellt, auf der Grundlage einer sorgfältigen Erfolgs- und Effektivitätskontrolle erneut die Erforderlichkeit und Verhältnismäßigkeit einer solchen Erweiterung des Grundrechtseingriffs zu überprüfen.

Die Datenschutzbeauftragten verlangen, daß der Gesetzgeber vor weiteren Eingriffen in Freiheitsrechte eine sorgfältige Güter- und Risikoabwägung vornimmt und dabei insbesondere verantwortlich prüft, ob sich die innenpolitischen Ziele mit Mitteln erreichen lassen, welche die informationelle Selbstbestimmung der Bürgerinnen und Bürger schonen.

Schließlich gibt die anstehende erneute Erweiterung des Katalogs von § 100a StPO Veranlassung, den Umfang der darin genannten Straftaten sobald wie möglich grundlegend zu überprüfen.

16.1.3 Zu Forderungen an den Gesetzgeber zur Regelung der Übermittlung personenbezogener Daten durch die Ermittlungsbehörden an die Medien (außerhalb der Öffentlichkeitsfahndung der Ermittlungsbehörden)

1. Für die Übermittlung von personenbezogenen Daten durch Justiz und Polizei an die Medien sollte eine bereichsspezifische Rechtsgrundlage geschaffen werden. Die Regelung sollte für den betroffenen Bürger den Umfang des Eingriffs in sein Recht auf informationelle Selbstbestimmung erkennbar machen.

2. Die Übermittlung personenbezogener Daten an die Medien ist nur ausnahmsweise gerechtfertigt, wenn das Verfahren gerade im Hinblick auf die Person des Betroffenen oder die besonderen Umstände der Tat für die Öffentlichkeit von überwiegendem Interesse ist.

3. Bei der Entscheidung, ob und in welchem Umfang personenbezogene Daten an die Medien übermittelt werden, sind die schutzwürdigen Belange der Betroffenen zu berücksichtigen. Dazu zählen insbesondere die privaten und beruflichen Folgen für das Opfer, den Beschuldigten/Angeklagten und deren Angehörige sowie die Schwere, die Umstände und die Folgen des Delikts.
   Bei der Übermittlung von personenbezogenen Daten über Beschuldigte/Angeklagte sind auch der Grad des Tatverdachts und der Stand des Verfahrens zu berücksichtigen. Vor Beginn der öffentlichen Hauptverhandlung ist ein besonders strenger Maßstab an das Vorliegen eines "überwiegenden Interesses" der Öffentlichkeit anzulegen.
   Bis zur rechtskräftigen Verurteilung ist die Unschuldsvermutung zugunsten des Beschuldigten oder Angeklagten zu beachten. Zu unterlassen sind alle Auskünfte oder Erklärungen, die geeignet sind, die Unbefangenheit der Verfahrensbeteiligten zu beeinträchtigen. Akteneinsicht durch Medienvertreter kommt nicht in Betracht.

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

5. Personenbezogene Daten dürfen nicht übermittelt werden, wenn besondere bundesgesetzliche oder landesgesetzliche Verwendungsregelungen entgegenstehen.

6. Ist die Bekanntgabe der Person des Beschuldigten oder Angeklagten wegen des überwiegenden öffentlichen Interesses gerechtfertigt, muß auch bei der Übermittlung sonstiger personenbezogener Daten abgewogen werden, ob diese Informationen für die Berichterstattung über die Tat selbst oder die Hintergründe, die zu der Tat geführt haben, erforderlich sind, und in welchem Umfang der Betroffene dadurch in seinem Persönlichkeitsrecht beeinträchtigt wird.

7. Die Bekanntgabe von Vorstrafen ist nur ausnahmsweise zulässig. Sie setzt voraus, daß die frühere Verurteilung im Bundeszentralregister noch nicht getilgt und ihre Kenntnis für eine nachvollziehbare Berichterstattung über eine schwerwiegende Straftat - auch unter Berücksichtigung des Persönlichkeitsrechts des Betroffenen und des Resozialisierungsgedankens - erforderlich ist. Besondere Zurückhaltung ist bei Auskünften und Erklärungen über Sachverhalte geboten, die der früheren Verurteilung zugrunde liegen.

8. Wegen des überragenden Schutzes von Minderjährigen und Heranwachsenden ist bei Auskünften und Erklärungen über Verfahren gegen diesen Personenkreis besondere Zurückhaltung hinsichtlich der Bekanntgabe personenbezogener Daten zu wahren.

9. Opfer, Zeugen und Familienangehörige haben in der Regel keine Veranlassung gegeben, daß ihre persönlichen Lebensumstände in der Öffentlichkeit bekannt gemacht werden. Die Übermittlung personenbezogener Daten über diesen Personenkreis an die Medien kommt deshalb grundsätzlich nicht in Betracht.

10. Bildveröffentlichungen greifen wegen der damit verbundenen sozialen Prangerwirkung besonders tief in das Persönlichkeitsrecht des Betroffenen ein. Eine Bildherausgabe kommt daher für Zwecke der Medienberichterstattung nicht in Betracht.

16.1.4 Zu Datenschutzrechtlichen Anforderungen an den Einsatz von Chipkarten im Gesundheitswesen

Die Datenschutzbeauftragten des Bundes und der Länder haben auf ihrer 47. Konferenz am 9./10. März 1994 kritisch zum Einsatz von Chipkarten im Gesundheitswesen Stellung genommen. In dem Beschluß wird die Nutzung von Patientenkarten von mehreren Voraussetzungen zur Sicherung des Persönlichkeitsrechts abhängig gemacht.

Seitdem werden in mehreren Ländern Modellversuche und Pilotprojekte durchgeführt. Die Bandbreite reicht

- von allgemeinen Patientenkarten, die an möglichst viele Patienten/Versicherte ausgegeben werden, eine Vielzahl von Krankheitsdaten enthalten und von einem unbestimmten Kreis von Personen und Institutionen des Gesundheitswesens zu vielfältigen Zwecken verwendet werden können (z. B. Vital-Card der AOK Leipzig, Persönliche Patientenkarte Neuwied, BKK-Patientenkarte Berlin)
- bis zu krankheitsspezifischen Karten für bestimmte Patientengruppen mit reduziertem Datensatz und einer Definition der Verwendung (z. B. Dialyse-Card, Diab-Card, Krebsnachsorgekarte, Defi-Card).

Datenschutzrechtlich stellen sich vor allem folgende Probleme:

- Die massenhafte Einführung der Karten erzeugt einen sozialen Druck auf die Betroffenen, sie mitzuführen und vorzuzeigen. Diesen Erwartungen wird sich der Betroffene vielfach nur unter Befremden des Arztes oder sogar der Gefahr, daß dieser die Behandlung ablehnt, verweigern können.
- Die Verwendung von allgemeinen Patientenkarten bringt die Gefahr einer pauschalen Offenbarung von medizinischen Daten mit sich.
- Dem Patienten wird die Last aufgebürdet, für die Sicherheit seiner medizinischen Daten selbst zu sorgen.

Die Datenschutzbeauftragten fordern alle für Kartenprojekte im Gesundheitswesen Verantwortlichen in Politik, Industrie, Ärzteschaft, Wissenschaft und in den Krankenversicherungen auf, das Recht auf informationelle Selbstbestimmung der betroffenen Patienten bzw. Versicherten zu gewährleisten. Die 50. Konferenz hält folgende Voraussetzungen für elementar:

1. Besondere Schutzwürdigkeit medizinischer Daten

Medizinische Daten sind besonders schutzwürdig, unabhängig davon, welche Technologien eingesetzt werden, ob die Patientendaten beim Arzt gespeichert und versandt oder über ein Netz abgerufen werden oder ob der Patient die Daten auf einer Chipkarte bei sich hat. Es handelt sich oftmals um belastende, schicksalhafte Daten. Zudem geht es nicht nur um Daten des Patienten, sondern auch um fremde Einblicke in die ärztliche Tätigkeit.

2. Wirksame Entscheidung der Betroffenen über die Verwendung einer Karte

Die freie Entscheidung der Betroffenen (Patienten/Versicherten), eine Chipkarte zu verwenden, muß gewährleistet sein. Dies umfaßt die Entscheidung,

- ob Daten auf einer Chipkarte gespeichert werden,
- welche der Gesundheitsdaten auf die Karte aufgenommen werden,
- welche Daten auf der Karte wieder gelöscht werden,
- ob die Karte bei einem Arztbesuch bzw. einem Apothekenbesuch vorgelegt wird und
- welche Daten im Einzelfall zugänglich gemacht werden.

Ein Widerruf der Entscheidung muß ohne Nachteile für die Betroffenen möglich sein. Die gleiche Freiheit der Entscheidung für oder gegen die Verwendung der Chipkarte muß für Ärzte und Apotheker gewährleistet sein. Eine wirksame Entscheidung für oder gegen die Verwendung einer Chipkarte setzt eine schriftliche, objektive, vollständige und nachvollziehbare Information über Zweck, Art, Umfang und Beteiligte der Chipkarten-Kommunikation voraus. Das Gesamtkonzept des Chipkarteneinsatzes und der damit verbundenen Datenverarbeitung muß für die Betroffenen überschaubar sein.

Auf der Karte darf nicht der Datensatz der Krankenversichertenkarte nach § 291 Abs. 2 SGB V, insbesondere nicht die Krankenversicherung und die

KrankenversicherungsNr., 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 Chipkarten-vermittelte 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.

16.1.5 Zum Datenschutz bei der Neuordnung der Telekommunikation (Postreform III)

Mit der Postreform III soll die Neugestaltung des Telekommunikationssektors in Deutschland nach den Vorgaben des Liberalisierungskonzepts der Europäischen Union abgeschlossen werden. Entstehen wird ein riesiger Markt mit einer Vielzahl von großen und kleinen, teilweise auch grenzüberschreitend tätigen Netzbetreibern und Diensteanbietern. Die Akteure auf diesem Telekommunikationsmarkt werden zum größeren Teil als Privatunternehmen operieren, es werden aber auch öffentliche Stellen ihre Leistungen anbieten. Der gesetzgeberische Abschluß der Liberalisierung und der Privatisierung des TK-Sektors wird die rechtliche Grundlage bilden für den endgültigen Eintritt in das Zeitalter von weltweiter Vernetzung, Multimedia und interaktiven Diensten und damit für den rapiden Anstieg des Konsums von Angeboten der Telekommunikation, des interaktiven Rundfunks und der Datenverarbeitung.
Die Konsequenzen sind absehbar: Gegenüber der heutigen Situation werden unvergleichlich mehr personenbezogene Daten durch mehr Stellen registriert und ausgewertet werden. Betroffen sind alle, die fernsehen, telefonieren, fernkopieren, Texte und Dokumente über Datenleitung schicken oder Telebanking oder Teleshopping betreiben. Die Risiken für den Einzelnen durch die vermehrten Möglichkeiten der Verhaltens- und Umfeldkontrolle oder der Ausforschung persönlicher Lebensgewohnheiten und Eigenschaften vergrößern sich entsprechend.

Der vom Bundesministerium für Post und Telekommunikation vorgelegte Referentenentwurf für ein Telekommunikationsgesetz (TKG-E, Stand: 6. Oktober 1995) macht es erforderlich, erneut die Realisierung der grundlegenden

Rahmenbedingungen für eine datenschutzgerechte Gestaltung der künftigen Telekommunikationslandschaft - soweit die Gesetzgebungskompetenz des Bundes betroffen ist - anzumahnen.

Ein wirksamer Datenschutz muß - wie bereits jetzt gesetzlich fixiert - auch künftig gleichberechtigtes Regulierungsziel neben z. B. der Sicherstellung der flächendeckenden Grundversorgung mit Telekommunikationsdienstleistungen bleiben.

Kundenwünsche nach variablerer und komfortablerer Nutzung der technischen Möglichkeiten werden zunehmen. Gerade deshalb müssen die Prinzipien der Datenvermeidung und der strikten Begrenzung der Datenverarbeitung auf das erforderliche Ausmaß ihren Vorrang bei der Ausgestaltung der kommunikationstechnischen Infrastruktur behalten. Netzbetreiber und Diensteanbieter sollten verpflichtet werden, überall dort, wo dies technisch möglich ist, auch anonyme Zugangs- und Nutzungsformen für ihre Leistungen bereitzustellen. Für eine sichere Datenübertragung sind ohne prohibitive Zusatzkosten wirksame Verschlüsselungsverfahren bereitzustellen.

Das Recht auf informationelle Selbstbestimmung und das Fernmeldegeheimnis müssen für alle Netzbetreiber und Diensteanbieter ungeachtet ihrer Rechtsform und ihrer Kundenstruktur (z. B. sog. Corporate Networks) einheitlich auf einem hohen Niveau gesichert werden. Der bisherige Schutzstandard darf keinesfalls unter den durch die Postreform II erreichten Stand gesenkt werden. Ein hohes Datenschutzniveau ist als Grundversorgung unabdingbar; seine Gewährleistung sollte deshalb Teil der Universaldienstleistung sein. Die in Grundrechte eingreifenden Regelungen sind im Telekommunikationsgesetz selbst und nicht in Verordnungen zu treffen. Die untergesetzlichen, den Datenschutz betreffenden Normen gehören in eine einzige, nicht verstreut in mehrere Verordnungen.
Entscheidend für die Wirksamkeit des Grundrechtsschutzes ist die strikte Einhaltung der Zweckbindung der Verbindungs- und Rechnungsdaten. Das "Feststellen mißbräuchlicher Inanspruchnahme" oder die "bedarfsgerechte Gestaltung" von TK-Leistungen dürfen nicht als Anlaß für eine umfassende Auswertung dieser Angaben oder sogar der Nachrichteninhalte herangezogen werden.
Für den Kunden bzw. Teilnehmer ist es von größter Bedeutung, die Verarbeitungsvorgänge im TK-Bereich überschauen zu können. Er muß auch künftig über die Nutzungsrisiken bestimmter Kommunikationstechniken (z. B. Mobilfunk) ebenso wie über seine Widerspruchsmöglichkeiten umfassend aufgeklärt werden. Keinesfalls darf die Einwilligung des Betroffenen mißbraucht werden um bereichsspezifische Schutznormen oder effiziente Datensicherungsvorkehrungen zu umgehen.

Um auch und gerade für das besonders schutzwürdige Fernmeldegeheimnis einen durchgängig hohen Schutzstandard zu sichern, braucht es eine unabhängige Kontrolle nach bundesweit einheitlichen Kriterien. Die Zuweisung dieser Überwachungsaufgabe an die im TKG-Entwurf vorgesehene Regulierungsbehörde ist wegen deren

mangelhafter Unabhängigkeit und der von ihr wahrzunehmenden Regulierungsaufgaben, die mit Interessenkonflikten verbunden sein werden, nicht akzeptabel.

Deshalb sollte aufgrund seiner langjährigen fachlichen Erfahrung bei der Kontrolle der TELEKOM und seiner umfassenden Querschnittskenntnisse im TK-Bereich der Bundesbeauftragte für den Datenschutz eine zentrale Funktion für die Kontrolle im Telekommunikationsbereich erhalten. Die Aufgaben, die die Landesbeauftragten für den Datenschutz und die Aufsichtsbehörden im Rahmen ihrer Zuständigkeiten erfüllen, sind gesetzlich klar zu regeln.

Die Akzeptanz der Informationsgesellschaft der Zukunft hängt wesentlich ab von der Sicherung des Grundrechts auf unbeobachtete Kommunikation. Das Telekommunikationsgesetz wird einen entscheidenden Baustein für die rechtliche Ausgestaltung der künftigen TK-Infrastruktur bilden. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher dazu auf, die von ihr vorgeschlagenen Regelungen im weiteren Gesetzgebungsverfahren zu berücksichtigen und sich für ihre Umsetzung auch auf der europäischen Ebene (z. B. in der ISDN-Richtlinie) einzusetzen.

16.2 Entschließungen der 51. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14./15. März 1996 in Hamburg

16.2.1 Zur Modernisierung und europäischen Harmonisierung des Datenschutzrechts

Die Datenschutzrichtlinie der Europäischen Union vom Oktober 1995 verpflichtet alle Mitgliedstaaten, ihr Datenschutzrecht binnen drei Jahren auf europäischer Ebene zu harmonisieren. Die Richtlinie geht zu Recht von einem hohen Datenschutzniveau aus und stellt fest: "Die Datenverarbeitungssysteme stehen im Dienste des Menschen."

Die Datenschutzbeauftragten begrüßen diesen wichtigen Schritt zu einem auch international wirksamen Datenschutz. Sie appellieren an den Gesetzgeber in Bund und Ländern, die Umsetzung der Richtlinie nicht nur als Beitrag zur europäischen Integration zu verstehen, sondern als Aufforderung und Chance, den Datenschutz fortzuentwickeln. Die Datenschutzbeauftragten sprechen sich für eine umfassende Modernisierung des deutschen Datenschutzrechts aus, damit der Einzelne in der sich rapide verändernden Welt der Datenverarbeitung, der Medien und der Telekommunikation über den Umlauf und die Verwendung seiner persönlichen Daten soweit wie möglich selbst bestimmen kann.
Die wichtigsten Ziele sind:

1. Weitgehende Vereinheitlichung der Vorschriften für den öffentlichen und privaten Bereich mit dem Ziel eines hohen, gleichwertigen Schutzes der Betroffenen, beispielsweise bei der Datenerhebung und bei der Zweckbindung bis hin zur Verarbeitung in Akten.
2. Erweiterung der Rechte der Betroffenen auf Information durch die datenverarbeitenden Stellen über die Verwendung der Daten, auf Auskunft, auf Widerspruch und im Bereich der Einwilligung.
3. Verpflichtung zu Risikoanalyse, Vorabkontrolle, Technikfolgenabschätzung und zur Beteiligung der Datenschutzbeauftragten bei der Vorbereitung von Regelungen mit Auswirkungen auf den Datenschutz.
4. Verbesserung der Organisation und Stärkung der Befugnisse der Datenschutzkontrolle unter den Gesichtspunkten der Unabhängigkeit und der Effektivität.
5. Einrichtung und effiziente Ausgestaltung des Amtes eines internen Datenschutzbeauftragten in öffentlichen Stellen.
6. Weiterentwicklung der Vorschriften zur Datensicherheit, insbesondere im Hinblick auf Miniaturisierung und Vernetzung.

Darüber hinaus machen die Datenschutzbeauftragten folgende Vorschläge:

7. Erweiterung des Schutzbereichs bei Bild- und Tonaufzeichnungen und Regelung der Video-Überwachung.
8. Stärkere Einbeziehung von Presse und Rundfunk in den Datenschutz; Aufrechterhaltung von Sonderregelungen nur, soweit dies für die Sicherung der Meinungsfreiheit notwendig ist.
9. Sonderregelungen für besonders empfindliche Bereiche, wie den Umgang mit Arbeitnehmerdaten, Gesundheitsdaten und Informationen aus gerichtlichen Verfahren.
10. Sicherstellung der informationellen Selbstbestimmung bei Multimedia-Diensten und anderen elektronischen Dienstleistungen durch die Pflicht, auch anonyme Nutzungs- und Zahlungsformen anzubieten, durch den Schutz vor übereilter Einwilligung, z. B. durch ein Widerrufsrecht, und durch strenge Zweckbindung für die bei Verbindung, Aufbau und Nutzung anfallenden Daten.
11. Besondere Regelungen für Chipkarten-Anwendungen, um die datenschutzrechtliche Verantwortung aller Beteiligten festzulegen und den Einzelnen vor unfreiwilliger Preisgabe seiner Daten zu schützen.
12. Schutz bei Persönlichkeitsbewertungen durch den Computer, insbesondere durch Beteiligung des Betroffenen und Nachvollziehbarkeit der Computerentscheidung.
13. Verstärkung des Schutzes gegenüber Adressenhandel und Direktmarketing.
14. Verbesserung des Datenschutzes bei grenzüberschreitender Datenverarbeitung; Datenübermittlung ins Ausland nur bei angemessenem Datenschutzniveau.

16.2.2 Zum Transplantationsgesetz

Bei der anstehenden gesetzlichen Regelung, unter welchen Voraussetzungen die Entnahme von Organen zur Transplantation zulässig sein soll, werden untrennbar mit der Ausformung des Rechts auf Selbstbestimmung auch Bedingungen des Rechts auf informationelle Selbstbestimmung festgelegt.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder betont hierzu, daß von den im Gesetzgebungsverfahren diskutierten Modellen die "enge Zustimmungslösung" - also eine ausdrückliche Zustimmung des Organspenders - den geringsten Eingriff in das Recht auf informationelle Selbstbestimmung beinhaltet. Sie zwingt niemanden, eine Ablehnung zu dokumentieren. Sie setzt auch kein Organspenderregister voraus.

Mit einer engen Zustimmungslösung ist auch vereinbar, daß der Organspender seine Entscheidung z. B. einem nahen Angehörigen überträgt.

16.3 Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 29. April 1996 zu Eckpunkten für die datenschutzrechtliche Regelung von Mediendiensten

In letzter Zeit finden Online-Dienste und Multimedia-Anwendungen zunehmend Verbreitung. Mit den - häufig multimedialen - Angeboten, auf die interaktiv über Telekommunikationsnetze zugegriffen werden kann, sind besondere Risiken für das Recht auf informationelle Selbstbestimmung der Teilnehmer verbunden; hinzuweisen ist insbesondere auf die Gefahr, daß das Nutzerverhalten unbemerkt registriert und zu Verhaltensprofilen zusammengeführt wird. Das allgemeine Datenschutzrecht reicht nicht aus, die mit den neuen technischen Möglichkeiten und Nutzungsformen verbundenen Risiken wirkungsvoll zu beherrschen.

Die Datenschutzbeauftragten des Bundes und der Länder halten es für dringend erforderlich, durch bereichsspezifische Regelungen technische und rechtliche Gestaltungsanforderungen für die elektronischen Dienste zu formulieren, die den Datenschutz sicherstellen. Leitlinie sollte hierbei der Grundsatz der Datenvermeidung bzw. -minimierung sein. Die Datenschutzbeauftragten haben dazu in einer Entschließung vom 14./15. März 1996 zur Modernisierung und zur europäischen Harmonisierung des Datenschutzrechts vorgeschlagen, daß die informationelle Selbstbestimmung bei Multimediadiensten und anderen elektronischen Dienstleistungen durch die Pflicht, auch anonyme Nutzungs- und Zahlungsverfahren anzubieten, durch den Schutz vor übereilter Einwilligung, z. B. durch ein Widerspruchsrecht, und durch strenge Zweckbindung für die bei der Verbindung, Nutzung und Abrechnung anfallenden Daten sichergestellt wird.

Die Datenschutzbeauftragten weisen darauf hin, daß auch mit Inhalten, die durch Mediendienste verbreitet werden, datenschutzrechtliche Probleme verbunden sein können. Auf diese Probleme wird im folgenden jedoch - ebenso wie auf die Datenschutzaspekte der Telekommunikation - nicht näher eingegangen. Bei den datenschutzrechtlichen Eckpunkten wird ferner bewußt darauf verzichtet, den Regelungsort - etwa einen Länder-Staatsvertrag oder ein Bundesgesetz - anzugeben. Die Datenschutzbeauftragten appellieren an die Gesetzgeber in Bund und Ländern, eine angemessene datenschutzgerechte Regulierung der neuen Dienste nicht an Kompetenzstreitigkeiten scheitern zu lassen.

1. *Anonyme bzw. datensparsame Nutzung*:
Die Dienste und Multimedia-Einrichtungen sollten so gestaltet werden, daß keine oder möglichst wenige personenbezogene Daten erhoben, verarbeitet und genutzt werden; deshalb sind auch anonyme Nutzungs- und Zahlungsformen anzubieten. Auch zur Aufrechterhaltung und zur bedarfsgerechten Gestaltung von Diensten und Dienstleistungen (Systempflege) sind soweit wie möglich anonymisierte Daten zu verwenden. Soweit eine vollständig anonyme Nutzung nicht realisiert werden kann, muß jeweils geprüft werden, ob durch andere Verfahren, z. B. die Verwendung von Pseudonymen, ein unmittelbarer Personenbezug vermieden werden kann. Die Herstellung des Personenbezugs sollte bei diesen Nutzungsformen nur dann erfolgen, wenn hieran ein begründetes rechtliches Interesse besteht.

2. *Bestandsdaten*:
Bestandsdaten dürfen nur in dem Maße erhoben, verarbeitet und genutzt werden, soweit sie für die Begründung und Abwicklung eines Vertragsverhältnisses sowie für die Systempflege erforderlich sind. Die Bestandsdaten dürfen zur bedarfsgerechten Gestaltung von Diensten und Dienstleistungen sowie zur Werbung und Marktforschung genutzt werden, soweit der Betroffene dem nicht widersprochen hat. Für die Werbung und Marktforschung durch Dritte dürfen Bestandsdaten nur mit der ausdrücklichen Einwilligung des Betroffenen verarbeitet werden.

3. *Verbindungs- und Abrechnungsdaten*:
Verbindungs- und Abrechnungsdaten dürfen nur für Zwecke der Vermittlung von Angeboten und für Abrechnungszwecke erhoben, gespeichert und genutzt werden. Sie sind zu löschen, wenn sie für die Erbringung der Dienstleistung oder für Abrechnungszwecke nicht mehr erforderlich sind. Soweit Verbindungsdaten ausschließlich zur Vermittlung einer Dienstleistung gespeichert werden, sind sie spätestens nach Beendigung der Verbindung zu löschen. Die Speicherung der Abrechnungsdaten darf den Zeitpunkt, die Dauer, die Art, den Inhalt und die Häufigkeit bestimmter von den einzelnen Teilnehmern in Anspruch genommener Angebote nicht erkennen lassen, es sei denn, der Teilnehmer beantragt eine dahingehende Speicherung. Verbindungs- und Abrechnungsdaten sind einer strikten Zweckbindung zu unterwerfen. Sie dürfen über den hier genannten Umfang hinaus nur mit der ausdrücklichen Einwilligung des Betroffenen erhoben, verarbeitet und genutzt werden. Unberührt hiervon bleibt die Speicherung von Daten von Verantwortlichen für

Angebote im Zusammenhang mit Impressumspflichten.

4. *Interaktionsdaten*:
Werden im Rahmen von interaktiven Dienstleistungen darüber hinaus personenbezogene Daten erhoben, die nachweisen, welche Eingaben der Teilnehmer während der Nutzung des Angebots zur Beeinflussung des Ablaufs vorgenommen hat (Interaktionsdaten; hierzu gehören z. B. Daten, die bei lexikalischen Abfragen, in interaktive Suchsysteme - etwa elektronische Fahrpläne und Telefonverzeichnisse - und bei Online-Spielen eingegeben werden), darf dies nur in Kenntnis und mit ausdrücklicher Einwilligung des Betroffenen geschehen. Interaktionsdaten dürfen nur unter Beachtung einer strikten Zweckbindung verarbeitet und genutzt werden. Sie sind grundsätzlich zu löschen, wenn der Zweck, zu dem sie erhoben wurden, erreicht wurde (so müssen Daten über die interaktive Suche von Angeboten unmittelbar nach Beendigung des Suchprozesses gelöscht werden). Eine weitergehende Verarbeitung dieser Daten ist nur auf Grundlage einer ausdrücklichen Einwilligung des Betroffenen zulässig.

5. *Einwilligung*:
Der Abschluß oder die Erfüllung eines Vertragsverhältnisses dürfen nicht davon abhängig gemacht werden, daß der Betroffene in die Verarbeitung oder Nutzung seiner Daten außerhalb der zulässigen Zweckbestimmung eingewilligt hat. Soweit Daten aufgrund einer Einwilligung erhoben werden, muß diese jederzeit widerrufen werden können. Für die Form und Dokumentation elektronisch abgegebener Einwilligungen und sonstiger Willenserklärungen ist ein Mindeststandard zu definieren, der einen fälschungssicheren Nachweis über die Tatsache, den Zeitpunkt und den Gegenstand gewährleistet. Dabei ist sicherzustellen, daß der Teilnehmer bereits vor der Einwilligung soweit wie möglich über den Inhalt und die Folgen seiner Einwilligung und über sein Widerrufsrecht informiert ist. Deshalb müssen die Betroffenen sowohl vor als auch nach Eingabe der Erklärung die Möglichkeit haben, auf Einwilligungen, Verträge und sonstige Informationen über die Bedingungen der Nutzung von Diensten, Multimedia-Einrichtungen und Dienstleistungen zuzugreifen und diese auch in schriftlicher Form zu erhalten. Da Verträge oder andere rechtswirksame Erklärungen, die in einer Fremdsprache verfaßt sind, unter Umständen juristische Fachbegriffe enthalten, die nur vor dem Hintergrund der jeweiligen Rechtsordnung zu verstehen sind, sollten zumindest diejenigen Dienste, die eine deutschsprachige Benutzeroberfläche anbieten, derartige Unterlagen auch in deutscher Sprache bereitstellen.

6. *Transparenz der Dienste und Steuerung der Datenübertragung durch die Teilnehmer*:
Die automatische Übermittlung von Daten durch die beim Betroffenen eingesetzte Datenverarbeitungsanlage ist auf das technisch für die Vertragsabwicklung notwendige Maß zu beschränken. Eine darüber hinausgehende Übermittlung ist nur aufgrund einer besonderen Einwilligung zulässig. Im Hinblick darauf, daß die Teilnehmer bei der eingesetzten Technik nicht erkennen können, in welchem Dienst sie sich befinden und

welche Daten bei der Nutzung von elektronischen Diensten bzw. bei der Erbringung von Dienstleistungen automatisiert übertragen und gespeichert werden, ist sicherzustellen, daß die Teilnehmer vor Beginn der Datenübertragung hierüber informiert werden und die Möglichkeit haben, den Prozeß jederzeit abzubrechen. Die zur Nutzung vom Anbieter oder Netzbetreiber bereitgestellte Software muß eine vom Nutzer aktivierbare Möglichkeit enthalten, den gesamten Strom der ein- und ausgehenden Daten vollständig zu protokollieren. Bei einer Durchschaltung zu einem anderen Dienst bzw. zu einer anderen Multimedia-Einrichtung müssen die Teilnehmer über die Durchschaltung und damit mögliche Datenübertragungen informiert werden. Diensteanbieter haben zu gewährleisten, daß sie keine erkennbar unsicheren Netze für die Übertragung personenbezogener Daten nutzen bzw. den Schutz dieser Daten durch angemessene Maßnahmen sicherstellen. Entsprechend dem Stand der Technik sind geeignete (z. B. kryptographische) Verfahren anzuwenden, um die Vertraulichkeit und Integrität der übertragenen Daten sowie eine sichere Identifizierung und Authentifikation zwischen Teilnehmern und Anbietern zu gewährleisten.

7. *Rechte von Betroffenen*:
Die Rechte von Betroffenen auf Auskunft, Sperrung, Berichtigung und Löschung sind auch bei multimedialen und sonstigen elektronischen Diensten zu gewährleisten. Soweit personenbezoge Daten im Rahmen eines elektronischen Dienstes veröffentlicht wurden, der dem Medienprivileg unterliegt, ist das Gegendarstellungsrecht der von der Veröffentlichung Betroffenen sicherzustellen.

8. *Datenschutzkontrolle*:
Eine effektive, unabhängige und nicht anlaßgebundene Datenschutzaufsicht ist zu gewährleisten. Den für die Kontrolle des Datenschutzes zuständigen Behörden ist ein jederzeitiger kostenfreier elektronischer Zugriff auf die Dienste und Dienstleistungen und der Zugang zu den eingesetzten technischen Einrichtungen zu ermöglichen. Bei elektronischen Diensten, für die das Medienprivileg gilt, ist die externe Datenschutzkontrolle entsprechend zu beschränken.

9. *Geltungsbereich*:
Der Geltungsbereich der jeweiligen Regelungen ist eindeutig festzulegen. Es ist sicherzustellen, daß die Datenschutzbestimmungen auch gelten, sofern personenbezogene Daten nicht in Dateien verarbeitet werden.

10. *Internationale Datenschutzregelung*:
Im Hinblick auf die zunehmende Bedeutung grenzüberschreitender elektronischer Dienste und Dienstleistungen ist eine Fortentwicklung der europäischen und internationalen Rechtsordnung dringend erforderlich, die auch bei ausländischen Diensten, Dienstleistungen und Multimedia-Angeboten ein angemessenes Datenschutzniveau gewährleistet. Die Verabschiedung der sog. ISDN-Datenschutzrichtlinie mit einem europaweiten hohen Schutzstandard ist überfällig. Kurzfristig ist es notwendig, den Betroffenen angemessene Mittel zur Durchsetzung ihrer Datenschutzrechte gegenüber ausländischen Betreibern und Dienstleistern in die

Hand zu geben. Die in Deutschland aktiven Dienste aus Nicht-EG-Staaten haben im Sinne der EG-Datenschutzrichtlinie (95/46/EG) vom 24. Oktober 1995 einen verantwortlichen inländischen Vertreter zu benennen.