Sächsischer Landtag DRUCKSACHE 1/4580
1. Wahlperiode

Schutz des Persönlichkeitsrechts im öffentlichen Bereich

2. Tätigkeitsbericht

des

Sächsischen Datenschutzbeauftragten

Dem Sächsischen Landtag

vorgelegt zum 31. März 1994

gemäß § 27 des Sächsischen Datenschutzgesetzes

Eingegangen am: 31.3.1994 Ausgegeben am: 20.4.1994

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 Bezeichnungen 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
Devrientstraße 19 Postfach 120905
01067 Dresden 01008 Dresden
Telefon: 0351-4855909
Fax : 0351-4855993

Herstellung: Elke Otto Verlag & Druckerei, Dresden
Gedruckt auf chlorfreiem Papier.

Inhaltsverzeichnis

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.

AMG	Gesetz über den Verkehr mit Arzneimitteln (Arzneimittelgesetz) vom 24. August 1976 (BGBl. I S. 2445), zuletzt geändert durch Art. 18 des Gesetzes zur Sicherung und Strukturverbesserung der gesetzlichen Krankenversicherung (Gesundheitsstrukturgesetz) vom 21. Dezember 1992 (BGBl. I S. 2266)
AO	Abgabenordnung
AufbewBest	Bestimmungen über die Aufbewahrungsfristen für das Schriftgut der ordentlichen Gerichtsbarkeit, der Staatsanwaltschaften und der Justizvollzugsbehörden (Aufbewahrungsbestimmungen), abgedruckt in Wannenmacher/Schaller, Sächsische Justizverwaltungsvorschriften für die Geschäftsstelle, Nr. 105
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. 16 des Gesetzes zur Sicherung und Strukturverbesserung der gesetzlichen Krankenversicherung (Gesundheitsstrukturgesetz) vom 21. Dezember 1992 (BGBl. I S. 2266)
BArchG	Gesetz über die Sicherung und Nutzung von Archivgut des Bundes (Bundesarchivgesetz) vom 6. Januar 1988 (BGBl. I S. 62), zuletzt geändert durch das Gesetz zur Änderung des Bundesarchivgesetzes vom 13. März 1992 (BGBl. I S. 506)
BAT(-O)	Erster Tarifvertrag zur Anpassung des Tarifrechts - Manteltarifliche Vorschriften (BAT-O) vom 10. Dezember 1990 (SächsABl. Nr. 10/1991 S. 1)
BDSG	Gesetz zur Fortentwicklung der Datenverarbeitung und des Datenschutzes (Bundesdatenschutzgesetz)
BGB	Bürgerliches Gesetzbuch
1. BMeldDÜV	Verordnung zur Durchführung von regelmäßigen Datenübermittlungen zwischen Meldebehörden verschiedener Länder (1. Meldedaten-Übermittlungsverordnung des Bundes) vom 18. Juni 1983 (BGBl. I S. 943)
2. BMeldDÜV	Verordnung zur Durchführung von regelmäßigen Datenübermittlungen der Meldebehörden an Behörden oder sonstige öffentliche Stellen des Bundes (2. Meldedaten-Übermittlungsverordnung des Bundes) vom 26. Juni 1984 (BGBl. I S. 810)

BVerfGG	Bundesverfassungsgerichtsgesetz
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)
BVG	Gesetz über die Versorgung der Opfer des Krieges (Bundesversorgungsgesetz) vom 20. Dezember 1950 (BGBl. I S. 791) in der Fassung der Bekanntmachung vom 22. Januar 1982 (BGBl. I S. 21), zuletzt geändert durch Art. 11 des Gesetzes zur Bereinigung von Kriegsfolgengesetzen (Kriegsfolgenbereinigungsgesetz) vom 21. Dezember 1992 (BGBl. I S. 2094)
BZRG	Gesetz über das Zentralregister und das Erziehungsregister (Bundeszentralregistergesetz)
DA	Dienstanweisung für die Standesbeamten und ihrer Aufsichtsbehörden vom 23. November 1987 (BAnz. Nr. 227 a), zuletzt geändert durch Änderungsverwaltungsvorschrift vom 23. März 1992 (BAnz. Nr. 57)
EKD-Datenschutzgesetze	Kirchengesetz über den Datenschutz vom 10. November 1977 (ABl. EKD 1978 S. 2) Neufassung: Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland vom 12. November 1993 (Amtsblatt der Evangelisch-Lutherischen Landeskirche Sachsen, Nr. 2/A15, 31. Januar 1994)
EVertr	Vertrag zwischen der Bundesrepublik Deutschland und der Deutschen Demokratischen Republik über die Herstellung der Einheit Deutschlands (Einigungsvertrag) vom 31. August 1990 (BGBl. II S. 889)
EStG	Einkommensteuergesetz 1990
G 10	Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Gesetz zu Art. 10 Grundgesetz) vom 13. August 1968 (BGBl. I S. 949), zuletzt geändert durch Art. 2 des Gesetzes über die parlamentarische Kontrolle nachrichtendienstlicher Tätigkeit des Bundes und zur Änderung des Gesetzes zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses vom 27. Mai 1992 (BGBl. I S. 997)
GBO	Grundbuchordnung
GeschlechtskrG	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)

GG	Grundgesetz für die Bundesrepublik Deutschland (Grundgesetz)
GO	Geschäftsordnung des Landtages des Freistaates Sachsen vom 10. Juli 1992 (nicht verkündet)
GVG	Gerichtsverfassungsgesetz vom 27. Januar 1877 (RGBl. I S. 41; BGBl. III 300-2) in der Fassung vom 9. Mai 1975 (BGBl. I S. 1077), zuletzt geändert durch das Gesetz zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der Kriminalität vom 15. Juli 1992 (BGBl. I S. 1302)
GVO	Verordnung über den Verkehr mit Grundstücken (Grundstücksverkehrsordnung [früher Grundstücksverkehrsverordnung - GVVO]) vom 15. Dezember 1977 (DDR-GBl. I 1978 Nr. 5 S. 73) in der Fassung der Bekanntmachung vom 18. April 1991 (BGBl. I S. 999), geändert durch Art. 4 des 2. VermRÄndG vom 14. Juli 1992 (BGBl. I S. 1257, 1266) und jetzt neu gefaßt durch Art. 15 § 1 des Registerverfahrensbeschleunigungsgesetzes vom 20. Dezember 1993 (BGBl. I S. 2182, 2221)
HEG	Sächsisches Hochschulerneuerungsgesetz vom 25. Juli 1991 (GVBl. S. 261), geändert durch Änderungsgesetz vom 31. Juli 1992 (GVBl. S. 401)
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)
KDO	Anordnung für den kirchlichen Datenschutz vom 28. Februar 1991 (Kirchliches Amtsblatt für das Bistum Dresden-Meißen, Nr. 7, 12. März 1991, S. 74) inhaltsgleich: Anordnung über den kirchlichen Datenschutz für die Apostolische Administratur und den caritativen Bereich Görlitz vom 12. Dezember 1990 (Amtsblatt der Apostolischen Administratur Görlitz, Nr. 3, 20. Februar 1991, S. 5) Neufassung: Anordnung über den Kirchlichen Datenschutz (Amtsblatt der Apostolischen Administratur Görlitz, Nr. 2, 10. Januar 1994, S. 1)
Krebsregister-sicherungsgesetz	Gesetz zur Sicherung und vorläufigen Fortführung der Datensammlungen des "Nationalen Krebsregisters" der ehemaligen Deutschen Demokratischen Republik vom 21. Dezember 1992 (BGBl. I S. 2335)
LBStUG	Gesetz über die Rechtsstellung des Sächsischen Landesbeauftragten für die Unterlagen des Staatssicherheitsdienstes der ehemaligen Deutschen Demokratischen Republik (Landesbeauftragtengesetz) vom 30. Juni 1992 (GVBl. S. 293)

LuftVG	Luftverkehrsgesetz vom 1. August 1922 (RGBl. I S. 681) in der Fassung der Neubekanntmachung vom 14. Januar 1981 (BGBl. I S. 61), zuletzt geändert nach Maßgabe des Art. 11 durch Art. 1 und 2 des Zehnten Gesetzes zur Änderung des Luftverkehrsgesetzes vom 23. Juli 1992 (BGBl. I S. 1370)
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
MVVO	Erste Verordnung des Sächsischen Staatsministeriums des Innern zur Durchführung des Sächsischen Meldegesetzes (Meldevordruckverordnung) vom 6. September 1993 (GVBl. S. 863)
Ordensgesetz	Gesetz über Titel, Orden und Ehrenzeichen vom 26. Juli 1957 (BGBl. I S. 844)
OWiG	Gesetz über Ordnungswidrigkeiten (Ordnungswidrigkeitengesetz)
PAG	[Sächs.] Gesetz über die Aufgaben und Befugnisse der Polizei vom 13. September 1990 (GVBl. I S. 1489)
PartG	Parteiengesetz in der Fassung der Bekanntmachung vom 3. März 1989 (BGBl. I S. 327), zuletzt geändert durch das Sechste Gesetz zur Änderung des Parteiengesetzes und anderer Gesetze vom 28. Januar 1994 (BGBl. I S. 142)
PStG	Personenstandsgesetz
Registerverfahrens-beschleunigungsgesetz	Gesetz zur Vereinfachung und Beschleunigung registerrechtlicher und anderer Verfahren vom 20. Dezember 1993 (BGBl. I S. 2182)
RVO	Reichsversicherungsordnung
SächsAG G 10	Gesetz zur Ausführung des Gesetzes zu Art. 10 Grundgesetz im Freistaat Sachsen vom 16. Oktober 1992 (GVBl. S. 464)
SächsArchG	Archivgesetz für den Freistaat Sachsen vom 17. Mai 1993 (GVBl. S. 449)
SächsBG	Beamtengesetz für den Freistaat Sachsen vom 17. Dezember 1992 (GVBl. S. 615)
SächsBrandschG	Gesetz über den Brandschutz und die Hilfeleistung der Feuerwehren bei Unglücksfällen und Notständen im Freistaat Sachsen vom 2. Juli 1991 (GVBl. S. 227), zuletzt geändert durch Gesetz vom 19. August 1993 (GVBl. S. 815)
SächsDO	Disziplinarordnung für den Freistaat Sachsen vom 28. Februar 1994 (GVBl. S. 333)
SächsDSG	Gesetz zum Schutz der informationellen Selbstbestimmung im Freistaat Sachsen (Sächsisches Datenschutzgesetz) vom 11. Dezember 1991 (GVBl. S. 401)

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 18. Dezember 1993 (GVBl. S. 937)
SächsGKV	Gesetz über den kommunalen Versorgungsverband Sachsen vom 19. November 1992 (GVBl. S. 551)
SächsKAG	Sächsisches Kommunalabgabengesetz vom 16. Juni 1993 (GVBl. S. 502)
SächsKHG	Gesetz zur Neuordnung des Krankenhauswesens (Sächsisches Krankenhausgesetz) vom 19. August 1993 (GVBl. S. 675)
SächsKRG	Sächsisches Krebsregistergesetz vom 19. Juli 1993 (GVBl. S. 589)
SächsLKrO	Landkreisordnung für den Freistaat Sachsen vom 19. Juli 1993 (GVBl. S. 577)
SächsMG	Sächsisches Meldegesetz vom 21. April 1993 (GVBl. S. 353), zuletzt geändert durch § 13 des Sächsischen Ordnungswidrigkeitengesetzes vom 20. Januar 1994 (GVBl. S. 174)
SächsPersVG	Sächsisches Personalvertretungsgesetz vom 21. Januar 1993 (GVBl. S. 29)
SächsPolG	Polizeigesetz des Freistaates Sachsen vom 30. Juli 1991 (GVBl. S. 291)
SächsStatG	Sächsisches Statistikgesetz vom 17. Mai 1993 (GVBl. S. 453)
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)
SächsVwVfG	Vorläufiges Verwaltungsverfahrensgesetz für den Freistaat Sachsen vom 21. Januar 1993 (GVBl. S. 74)
SäHO	Vorläufige Haushaltsordnung des Freistaates Sachsen (Vorläufige Sächsische Haushaltsordnung) vom 19. Dezember 1990 (GVBl. S. 21)
SchulG	Schulgesetz für den Freistaat Sachsen vom 3. Juli 1991 (GVBl. S. 213)
SGB I	Sozialgesetzbuch - Allgemeiner Teil - vom 11. Dezember 1975 (BGBl. I S. 3015), Art. II § 1 Nr. 14 neugefaßt durch Art. 4 des Gesetzes über die Einführung eines Wohngeldsondergesetzes vom 20. Juni 1991 (BGBl. I S. 1250)
SGB IV	Sozialgesetzbuch - Gemeinsame Vorschriften für die Sozialversicherung - vom 23. Dezember 1976 (BGBl. I S. 3845), geändert nach Maßgabe des Art. 35 durch Art. 3 des Gesetzes zur Sicherung und Strukturverbesserung der gesetzlichen Krankenversicherung (Gesundheitsstrukturgesetz) vom 21. Dezember 1992 (BGBl. I S. 2266)

SGB V	Sozialgesetzbuch - Gesetzliche Krankenversicherung - vom 20. Dezember 1988 (BGBl. I S. 2477), geändert nach Maßgabe des Art. 35 durch Art. 1 und 2 des Gesetzes zur Sicherung und Struktur-verbesserung der gesetzlichen Krankenversicherung (Gesundheitsstrukturgesetz) vom 21. Dezember 1992 (BGBl. I S. 2266)
SGB VI	Sozialgesetzbuch - Gesetzliche Rentenversicherung - vom 18. Dezember 1989 (BGBl. I S. 2261, berichtigt 1990 BGBl. I S. 1337), zuletzt geändert durch Art. 1 des Gesetzes zur Ergänzung der Rentenüberleitung (Rentenüberleitungs-Ergänzungsgesetz - Rü-ErgG) vom 24. Juni 1993 (BGBl. I S. 1038)
SGB VIII	Sozialgesetzbuch - Kinder- und Jugendhilfe - vom 26. Juni 1990 (BGBl. I S. 1163), § 24 neugefaßt durch Art. 5 Nr. 1 des Gesetzes über Aufklärung, Verhütung, Familienplanung und Beratung vom 27. Juli 1992 (BGBl. I S. 1398)
SGB X	Sozialgesetzbuch - Verwaltungsverfahren - vom 18. August 1980 (BGBl. I S. 1469), zuletzt geändert durch das Rentenüberleitungs-Ergänzungsgesetz vom 24. Juni 1993 (BGBl. I S. 1038)
SHEG	Sächsisches Hochschulerneuerungsgesetz vom 25. Juli 1991 (GVBl. S. 261), zuletzt geändert durch Gesetz vom 31. Juli 1992 (GVBl. S. 401)
HG	Gesetz über die Hochschulen im Freistaat Sachsen (Sächsisches Hochschulgesetz) vom 4. August 1993 (GVBl. S. 693)
StGB	Strafgesetzbuch
StPO	Strafprozeßordnung
StUG	Gesetz über die Unterlagen des Staatssicherheitsdienstes der ehemaligen Deutschen Demokratischen Republik (Stasi-Unterlagen-Gesetz) vom 20. Dezember 1991 (BGBl. I S. 2272)
StVG	Straßenverkehrsgesetz
StVZO	Straßenverkehrs-Zulassungs-Ordnung
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. 15 § 2 des Registerverfahrensbeschleunigungsgesetzes vom 20. Dezember 1993 (BGBl. I S. 2182, 2223)
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)
VVG	Versicherungsvertragsgesetz
VwGO	Verwaltungsgerichtsordnung
VwVfG	Verwaltungsverfahrensgesetz

WaffG	Waffengesetz
Wohnungsbelegungs-gesetz	Gesetz über die Gewährleistung von Belegungsrechten im kommunalen und genossenschaftlichen Wohnungswesen vom 22. Juli 1990 (DDR-GBl. I S. 894) mit den in Anlage II zum Einigungsvertrag, Kapitel XIV, Abschnitt III Nr. 1 geregelten Maßgaben
WPflG	Wehrpflichtgesetz in der Fassung der Bekanntmachung vom 13. Juni 1986 (BGBl. I S. 879), zuletzt geändert durch Art. 2 Nr. 10 des Gesetzes zur Aufhebung des Heimkehrergesetzes und zur Änderung anderer Vorschriften vom 12. Dezember 1991 (BGBl. I S. 2317)
WRV	Weimarer Reichsverfassung vom 11. August 1919 (RGBl. S. 1383)

Sonstiges

AfNS	Amt für Nationale Sicherheit
AOK	Allgemeine Ortskrankenkasse
AZR	Ausländerzentralregister
BGHZ	Amtliche Sammlung der Entscheidungen des Bundesgerichtshofs in Zivilsachen
BKK	Betriebskrankenkasse
BVerfGE	Amtliche Sammlung der Entscheidungen des Bundesverfassungsgerichts
BVerwGE	Amtliche Sammlung der Entscheidungen des Bundesverwaltungsgerichts
BZR	Bundeszentralregister
EG	Europäische Gemeinschaft(en)
EU	Europäische Union
EWG	Europäische Wirtschaftsgemeinschaften
Gauck-Behörde	Der Bundesbeauftragte für die Unterlagen des Staatssicherheitsdienstes der ehemaligen Deutschen Demokratischen Republik
IKK	Innungskrankenkasse
IM	Inoffizieller Mitarbeiter (des MfS/AfNS)
MfS	Ministerium für Staatssicherheit
PersV	Die Personalvertretung (Zeitschrift)
SK	Sächsische Staatskanzlei
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

1 Datenschutz im Freistaat Sachsen

Mit Freude über den Erfolg, den die Arbeit meiner Behörde für den Schutz des Einzelnen vor dem Mißbrauch seiner Daten im vergangenen Jahr im Freistaat Sachsen erreicht hat, und mit einem besonderen Dank an alle meine Mitarbeiter lege ich diesen Bericht vor.

In den Angriffen der vergangenen Monate auf mein Amt und meine Person erkenne ich eine Bestätigung dafür, daß ich meine gesetzlichen Aufgaben wirksam wahrgenommen habe, sowie die Ermutigung, dies fortzusetzen.

Ich kann die Situation des Datenschutzes im Freistaat Sachsen nicht zusammenfassend beurteilen; dazu sind die Fachkenntnisse, aber auch das Einfühlungsvermögen in den öffentlichen Stellen zu unterschiedlich. Die Sensibilität für den Konflikt zwischen dem Anspruch der Allgemeinheit und der Individualität (nicht: dem Individualismus!) hat aber insgesamt erfreulich zugenommen. Es gibt bereits große Bereiche, in denen es zu einer wechselseitig anregenden und ergiebigen Zusammenarbeit mit meiner Behörde gekommen ist. Ich hoffe, daß ich dort den Wünschen nach praktischer, effektiver Verwaltung gerecht werden konnte, ohne meine Aufgabe zu vernachlässigen.

Der Diskussion über die inhaltliche Richtigkeit meiner Auffassungen stelle ich mich gern, und ich bin bereit zu lernen. Datenschutz ist beileibe nicht das dringlichste Problem im Freistaat Sachsen, das es zu lösen gilt; aber in diesem Detailbereich zeigt sich besonders klar, wo die Reise hingeht, wie sich der Kompromiß zwischen dem Gemeinschaftsanspruch und dem Individualrecht entwickelt.

1.1 Wer kontrolliert eigentlich den Datenschutzbeauftragten?

Immer wieder ist die Unabhängigkeit des Datenschutzbeauftragten ein Stein des Anstoßes. Sie ergibt sich weder aus dem Wortlaut des Grundgesetzes noch aus dem Text der Sächsischen Verfassung (Art. 57), sondern aus dem Volkszählungsurteil des Bundesverfassungsgerichts (BVerfGE 65, 1 ff.): In den (amtlichen) Leitsätzen der Entscheidung heißt es: "Auch hat er [der Gesetzgeber] organisatorische und verfahrensrechtliche Vorkehrungen zu treffen, welche der Gefahr einer Verletzung des Persönlichkeitsrechts entgegenwirken." Auf Seite 46 der Urteilsbegründung heißt es: "Wegen der für den Bürger bestehenden Undurchsichtigkeit der Speicherung und Verwendung von Daten unter den Bedingungen der automatischen Datenverarbeitung *und auch* im Interesse eines vorgezogenen Rechtsschutzes durch rechtzeitige Vorkehrungen *ist die Beteiligung unabhängiger Datenschutzbeauftragter von erheblicher Bedeutung* für einen effektiven Schutz des Rechts auf informationelle Selbstbestimmung (Hervorhebungen durch den Verf.)." Die Entscheidungsgründe müssen zur Ermittlung des Sinnes der Urteilsformel herangezogen werden (BVerfGE 19, 377 [391 f.]). Die Entscheidungen des Bundesverfassungsgerichts enthalten "gemäß § 31 Abs. 1 Bundesverfassungsgerichtsgesetz eine über den Einzelfall hinausgehende Bindungswirkung, insofern die sich aus dem Tenor und den *tragenden Gründen* der Entscheidung ergebenden Grundsätze für die Auslegung der Verfassung von den Gerichten und Behörden in allen künftigen Fällen beachtet werden müssen." (Ständige

Rechtsprechung des Bundesverfassungsgerichts, zuletzt BVerfGE 79, 256 [264]).

Der Sächsische Gesetzgeber ist dem Postulat der Unabhängigkeit des Datenschutzbeauftragten gefolgt und hat in § 23 Abs. 4 SächsDSG bestimmt: "Der Datenschutzbeauftragte ist in der Ausübung seines Amtes unabhängig, weisungsfrei und nur dem Gesetz unterworfen. Er untersteht der Dienstaufsicht des Präsidenten des Landtages, soweit seine Unabhängigkeit dadurch nicht beeinträchtigt wird. Für die Erfüllung seiner Aufgaben ist ihm die notwendige Personal- und Sachausstattung zur Verfügung zu stellen."

Es heißt manchmal: "Seine Unabhängigkeit bezahlt der Datenschutzbeauftragte mit seiner Wirkungslosigkeit." Daran ist etwas: In der Tat hat der Datenschutzbeauftragte *keine* Exekutivfunktionen; seine Entscheidungen sind weder für den einzelnen Bürger noch für eine von ihm beratene oder kontrollierte Behörde *verbindlich*. Dennoch bleibt die Tätigkeit meiner Behörde nicht wirkungslos: Zum einen folgen die Behörden in den meisten Fällen meinem Rat, zum anderen gibt mir das Sächsische Datenschutzgesetz in § 26 die Möglichkeit, datenschutzrechtliche Verstöße zu beanstanden und Behörden zur Mängelbeseitigung aufzufordern. Befolgt die öffentliche Stelle die Aufforderung nicht, so steht es ihr frei, ihre Ansicht - auch vor der Öffentlichkeit und dem Parlament - zu rechtfertigen.

Jederzeit bleibt es mir unbenommen, die Öffentlichkeit, insbesondere die Presse und die Medien, von meinen Beobachtungen und meiner Auffassung zu informieren. Dieses Recht findet seine Grenzen nur in den allgemeinen Gesetzen, insbesondere denen zum Schutz der Persönlichkeit.

Der Datenschutzbeauftragte entfaltet - insoweit ist einem merkwürdig weit verbreiteten Vorurteil zu begegnen - keine heimliche Tätigkeit; er sammelt offen seine Informationen bei den öffentlichen Stellen, um sie zu beraten oder zu kontrollieren. Allerdings nennt er seine Petenten in der Regel nicht (§ 23 Abs. 6 SächsDSG).

Üblicherweise erhalten die kontrollierten Stellen, wenn ich "fündig werde", einen Bericht, der Diskussionen auslösen soll. Nach förmlichen Beanstandungen gibt es meist keine zusätzliche Äußerung meiner Behörde, weil zuvor bereits die Argumente ausgetauscht sind.

Schließlich ermöglicht mein jährlicher Tätigkeitsbericht jedermann, meine Tätigkeit und die Qualität meiner Arbeit zu beurteilen. Die Staatsregierung kann dazu Stellung nehmen; dankenswerterweise hat das SMS dies frühzeitig getan.
Ich stelle mich gern fundierter Kritik.

1.2 Der Datenschutzbeauftragte im "ministerialfreien Raum"

Solange es die Institution der unabhängigen Datenschutzbeauftragten in Bund und Ländern gibt, so alt (und erfolglos) sind die Versuche, die Datenschutzbeauftragten entweder der Exekutive oder der Legislative zuzuordnen. Belz (Sächsische

Verwaltungsblätter 1994 S. 49 f.) sieht im Sächsischen Datenschutzbeauftragten "ein Hilfsorgan des Sächsischen Landtages" und übersieht dabei, daß Art. 57 der Sächsischen Verfassung lautet: "*Zur Wahrung des Rechtes auf Datenschutz und* zur Unterstützung bei der Ausübung der parlamentarischen Kontrolle wird *beim* Landtag ein Datenschutzbeauftragter berufen." Es ist also nicht lediglich so, daß der Sächsische Datenschutzbeauftragte ausschließlich unterstützende Hilfsfunktionen gegenüber dem Parlament wahrnimmt, sondern er ist zunächst der unabhängige und weisungsfreie, lediglich dem Gesetz unterworfene "Anwalt der Bürger", wenn es darum geht, deren Privatsphäre zu sichern. Hier hat er aus eigener Initiative tätig zu werden.

Diese objektive, ausschließlich sachbezogene Aufgabe des Sächsischen Datenschutzbeauftragten wird auch in § 27 Abs. 3 S. 1 und 2 SächsDSG deutlich: Die Aufträge, "Gutachten zu erstellen oder besondere Berichte zu erstatten" oder Hinweisen auf einzelne Angelegenheiten nachzugehen, können dem Sächsischen Datenschutzbeauftragten in gleicher Weise vom Landtag wie von der Staatsregierung erteilt werden, auf den Inhalt meiner Ausarbeitungen hat jedoch nur das Gesetz einen Einfluß.

So ergibt sich aus der Rechtsordnung zwanglos und widerspruchsfrei, daß der Datenschutzbeauftragte weder als Teil der Exekutive noch als Teil der Legislative angesehen werden kann. Er ist in einem Freiraum angesiedelt, der in der juristischen Literatur gemeinhin als "ministerialfreier Raum" bezeichnet wird. Sehr unterschiedliche Bereiche werden diesem - wie zuzugeben ist - schillernden Begriff zugeordnet: Bundestagsverwaltung, Wehrbeauftragter, Bundespräsidialamt, Bundesschuldenverwaltung, Deutsche Bundesbank, die Bundesaufsichtsämter, der Sachverständigenrat ("Die fünf Weisen"), Bundesprüfstelle für jugendgefährdende Schriften, die Verwaltung des Verfassungsgerichtshofs, Landesrechnungshof, beratende Ausschüsse, Prüfungsämter und viele andere. All diese Stellen können weder der Exekutive noch der Legislative sauber zugeordnet werden; das Schwergewicht ihrer Tätigkeit neigt nach der einen oder anderen Seite. Jedenfalls ist kein Regierungschef und Minister für ihre Tätigkeit gegenüber dem Parlament verantwortlich.

Aus Art. 20 Abs. 2 GG läßt sich - und dies wird in Rechtsprechung und Literatur nicht ernsthaft bestritten - keineswegs herleiten, daß es nur die dort genannten "drei klassischen Gewalten" gebe und daß jede staatliche Einrichtung ihrer Funktion nach einer von ihnen ausschließlich zugeordnet werden könne. Man versteht unter Gewaltenteilung heute: Die Unterscheidung verschiedener Funktionen innerhalb der einen Staatsgewalt, die Bildung von Einrichtungen (Organen), die in einer diesen Funktionen gerecht werdenden Weise ausgestaltet sind, das Verbot, Funktionen wahrzunehmen, die einer *anderen* Gewalt zugewiesen sind (Gewalten*trennung*) und die gegenseitige Kontrolle und Hemmung dieser Gewalten. Die Beschränkung auf die klassische Dreizahl ist zugunsten einer Ausdifferenzierung aufgegeben.

Die eine Staatsgewalt erscheint in der Verfassung als eine Verwebung zahlreicher Kompetenzen und Inkompatibilitäten und ist aus trennenden und verschränkenden Elementen zusammengesetzt. Dies System ist dabei nicht auf die eigentlichen Träger hoheitlicher Gewalt beschränkt. Die "Gubernative", also die Regierung, unterliegt aus guten Gründen nur einer eingeschränkten Dauerkontrolle durch das Parlament, mehr

noch gilt dies für die Judikative. Ein weitgehend von parlamentarischer Kontrolle freigestellter Datenschutzbeauftragter, der dabei zugleich das Parlament zu unterstützen hat, sprengt also keineswegs das System der Verfassung. Der Grund liegt darin, daß er anders als Verwaltung und Justiz eine innerstaatliche und lediglich beratende, aufdeckende Einrichtung ist und keine "Staatsgewalt" gegenüber dem Einzelnen anwendet. Es bestehen daher auch im Hinblick auf den Grundsatz der Gewaltenteilung keine Bedenken gegen die Ministerialfreiheit und Unabhängigkeit des Datenschutzbeauftragten (dazu auch BVerfGE 9, 268 [282]).

Da er keine bestimmende, sondern nur eine beratende Funktion hat, wirken alle Versuche, ihn der Exekutive oder Legislative zuzuordnen, schematisch und gewollt. Die Unabhängigkeit des Datenschutzbeauftragten wird vom Bundesverfassungsgericht ausdrücklich gefordert, sie ist zwanglos ein nützlicher Teil des berühmten Systems der "checks and balances" geworden.

Da der Datenschutzbeauftragte vom Landtag auf die Dauer von sechs Jahren gewählt ist, ist er in Ausübung seines Amtes durchaus demokratisch legitimiert.

So ist der Sächsische Datenschutzbeauftragte weder Vollzugsorgan der Regierung noch des Parlaments, vielmehr hat er in Eigeninitiative und Eigenverantwortung die gesetzlichen Vorschriften über den Schutz personenbezogener Daten anzuwenden, ohne daß es eine Instanz gäbe, die eventuelle Rechtsfehler (von denen ich sicherlich nicht frei bin) verbindlich feststellen könnte. Denn auch die förmliche Beanstandung ist nach übereinstimmender Auffassung in Rechtsprechung und Literatur kein justitiabler Verwaltungsakt, sondern lediglich ein Werturteil, das letzten Endes unverbindlich bleibt, mag es auch in der politischen Diskussion von Bedeutung sein.

1.3 Die Dienstaufsicht über den Datenschutzbeauftragten

Meine Tätigkeit im Sommer 1992 im Zusammenhang mit einer damaligen Eingabe wurde im November 1993 zum Gegenstand einer Strafanzeige gegen mich: Der Anzeigenerstatter machte geltend, ich hätte meine amtlichen Befugnisse bei einer zugunsten eines Petenten vorgenommenen Grundbucheinsicht mißbraucht und die Grundstücksdaten für eine privates Erwerbsinteresse benutzt. Für den daraufhin von der CDU-Fraktion gestellten Antrag, mich abzuwählen, kamen am 16. Dezember 1993 nicht die notwendige Zweidrittelmehrheit von 107 Stimmen (§ 23 Abs. 3 SächsDSG), sondern 76 Stimmen zusammen. Der Sachverhalt ist seit Anfang 1994 Gegenstand disziplinarrechtlicher (Vor-) Ermittlungen, die ich erbeten habe und unterstütze, deren endgültiges Ergebnis ich aber im übrigen abzuwarten habe.

Wie erwähnt untersteht der Sächsische Datenschutzbeauftragte der Dienstaufsicht des Präsidenten des Landtages, "soweit seine Unabhängigkeit dadurch nicht beeinträchtigt wird" (§ 23 Abs. 4 Satz 2 SächsDSG). Dienstaufsichtsbeschwerden eines Ministers, die an den Landtagspräsidenten gerichtet sind, lassen vermuten, daß der Begriff der Dienstaufsicht fehlinterpretiert wird. Denn anders als die Rechts- und Fachaufsicht beschränkt sich die Dienstaufsicht auf den Aufbau, die innere Ordnung, die *allgemeine*

Geschäftsführung und die Personalangelegenheiten der Behörde. Sie wacht über die *Erfüllung allgemeiner Dienstpflichten* einzelner Bediensteter. Den Versuch eines Ministers, über den Landtagspräsidenten die Anwendung datenschutzrechtlicher Vorschriften durch meine Behörde und mich im Wege der Dienstaufsicht überprüfen zu lassen, habe ich daher zurückgewiesen. Eine Umfrage bei meinen Kollegen des Bundes und der Länder ergab, daß es sich bei diesem Versuch um einen einmaligen Vorgang handelt.

1.4 Einschränkung der Zuständigkeit?

Aus einer angeblichen Stellung des Datenschutzbeauftragten als eines Hilfsorgans des Parlaments versucht Belz (a. a. O.) herzuleiten, meiner Kontrolle sei der Kernbereich exekutiver Eigenverantwortlichkeit im Sinne des Artikels 51 Abs. 2 und des Artikels 54 Abs. 4 SächsVerf verschlossen. Die Prämisse wird dem Wortlaut des Artikels 57 SächsVerf nicht gerecht ("*zur Wahrung des Rechtes auf Datenschutz und* zur Unterstützung bei der Ausübung der parlamentarischen Kontrolle ...") und ist daher falsch. Abgesehen davon ist auch das Ergebnis in sich unrichtig: Gerade diese Kernbereiche sind die wesentlichen Felder, die im Interesse der tragenden Gründe des Volkszählungsurteils einer besonderen Kontrolle durch den unabhängigen Datenschutzbeauftragten bedürfen. Es geht insofern nicht um die Verantwortlichkeit der Exekutive gegenüber der Legislative, sondern die Verwaltung muß in ihrem Umgang mit personenbezogenen Daten im Interesse der Betroffenen einer unabhängigen Kontrolle offenstehen. Würden Bereiche von dieser Kontrollbefugnis ausgenommen, so wäre der Exekutive der Umgang mit personenbezogenen Daten in wesentlichen - meist heimlichen - Bereichen kontrollfrei möglich. Gerade weil der Einzelne vom heimlichen Umgang mit seinen Daten nichts erfährt, kann er die Justiz nicht einschalten. Deshalb muß der Datenschutzbeauftragte als "Anwalt des Bürgers" und ohne konkretes Mandat gerade dort wirken können. Das Bundesverfassungsgericht grenzt zwar Kernbereiche von Exekutive, Legislative und Judikative voneinander ab, hält Übergriffe für verfassungswidrig (hierzu z. B. BVerfGE 67, 139) und betont, daß nicht jede Einflußnahme des Parlaments auf die Verwaltung unbedenklich ist (so schon BVerfGE 9, 268 [280]); im Volkszählungsurteil wird die *Kontrollfunktion des Datenschutzbeauftragten* (im Interesse des Einzelnen, nicht des Parlaments) *jedoch unbeschränkt* eröffnet. Ganz bewußt hat der Sächsische Landtag auch auf Einschränkungen der Befugnisse des Datenschutzbeauftragten verzichtet, wie sie im § 24 Abs. 2 S. 4 des Bundesdatenschutzgesetzes enthalten sind.
Allerdings - und dies klang im Berichtszeitraum einmal an - sind interne Überlegungen, Entwürfe, Stellungnahmen, Pläne etc., die weder innerhalb der Staatsregierung noch nach außen hin Verbindlichkeit entfaltet haben, meiner Kontrolle nicht zugänglich (siehe dazu BVerfGE 67, 100 [139]).

1.5 Zur Möglichkeit einer Abwahl

Schließlich wird in dem genannten Aufsatz von Belz behauptet, das in § 23 Abs. 3 SächsDSG vorgeschriebene Quorum von zwei Dritteln der Mitglieder des Landtages für

die Abberufung des Datenschutzbeauftragten sei verfassungswidrig, weil Art. 48 Abs. 3 der Sächsischen Verfassung das Prinzip der einfachen Mehrheit für alle Abstimmungsfälle vorsieht: "Der Landtag beschließt mit der Mehrheit der abgegebenen Stimmen, sofern diese Verfassung nichts anderes bestimmt. Für die vom Landtag vorzunehmenden Wahlen kann die Geschäftsordnung Ausnahmen zulassen." Dem letzten Satz dieser Vorschrift ist - folgt man führenden Kommentatoren - nicht etwa zu entnehmen, daß es dem Gesetzgeber verwehrt sei, *in Gesetzen* Ausnahmen vorzusehen; vielmehr bedeutet der Hinweis auf *die Geschäftsordnung* - die im Rang unterhalb eines Gesetzes angesiedelt ist - nur, daß es dem Landtag möglich ist, ausnahmsweise unterhalb einer gesetzlichen Norm, nämlich in seiner Geschäftsordnung, Ausnahmen vom Mehrheitsprinzip vorzusehen. Die in der Verfassung als Regelfall vorgesehene Abstimmungsmehrheit ist abhängig von der Zahl der anwesenden Abgeordneten. Wird die Beschlußfähigkeit nicht gerügt, ist es rein theoretisch möglich, daß zwei Abgeordnete einen dritten überstimmen. Gleiches gilt, wenn sich eine große Anzahl anwesender Abgeordneter der Stimme enthält.

Auch durch Gesetze (oder völkerrechtliche Verträge) können Ausnahmen vom relativen Mehrheitsprinzip angeordnet werden. In der Garantie der Institution des Sächsischen Datenschutzbeauftragten bestimmt die Verfassung (Art. 57 S.2): "Das Nähere bestimmt ein Gesetz." Somit ergibt sich die Befugnis des Gesetzgebers, Amt und Unabhängigkeit des Datenschutzbeauftragten durch Gesetz zu bestimmen, *unmittelbar* aus der Verfassung. Schließlich ist auch zu bedenken, daß das Sächsische Datenschutzgesetz vom 11. Dezember 1991 in Kraft war, als die Verfassung am 27. Mai 1992 in Kraft trat und bestimmte, daß das Nähere ein Gesetz bestimmt. Von einem "Widerspruch" im Sinne des Art. 120 Abs. 1 der Landesverfassung ist daher keine Rede.

Der Entwurf der europäischen Datenschutzrichtlinie sieht vor, daß der öffentliche und der private Bereich einer *unabhängigen* Datenschutzkontrolle ("independent supervisory authority", "autorité independante") unterliegen müssen. Soweit ich sehe, wird diese Unabhängigkeit der Daten-Kontrollbehörde von keiner Seite in Zweifel gezogen. Wie sollte aber von wirklicher Unabhängigkeit die Rede sein, wenn der Leiter der Behörde von einer (ständig wechselnden) einfachen Mehrheit im Parlament abhängig wäre?

Käme man mit Belz tatsächlich zu der Auslegung, daß das Quorum der Zweidrittelmehrheit für die Abwahl verfassungswidrig wäre, so wäre die entsprechende Formulierung des Gesetzes nichtig. Dann bliebe der in § 23 Abs. 3 Satz 2 SächsDSG unmittelbar danach folgende Satz stehen: "Die Vorschriften des Beamtenrechts bleiben unberührt." Schon nach derzeitiger Rechtslage entfaltet diese Vorschrift eine unübersehbare Wirkung: Denn eine Abwahl ist auch bei Zustandekommen des Quorums von zwei Dritteln nicht ohne weiteres (etwa aus Gründen politischer Konstellation) möglich, sondern nur dann, wenn die Voraussetzungen vorliegen, um einen Beamten aus dem Dienst zu entfernen. Weder besoldungsrechtliche noch versorgungsrechtliche Gründe hätten diesen Satz notwendig erscheinen lassen; sie sind ohnehin auch für den Fall der Abwahl geregelt. Der Satz lautet auch nicht: "*Im übrigen* ...", sondern gilt einschränkungslos und ohne jeden Abstrich und damit auch als *Voraussetzung* für den Fall einer Abwahl. Die Position des Sächsischen Datenschutzbeauftragten ist - aus guten Gründen - stärker als die eines "normalen" Beamten.

Mit Recht sagt Belz, daß die Stellung des Sächsischen Datenschutzbeauftragten mit der eines Richters vergleichbar ist (wobei zu betonen ist, daß der Sächsische Datenschutzbeauftragte keine verbindlichen Urteile erläßt, sondern lediglich berät oder exekutivisch folgenlos beanstanden kann).

Meine Arbeit im Berichtszeitraum hat deutlich gemacht, daß ein Datenschutzbeauftragter seine Aufgabe nur in wirklicher Unabhängigkeit zu erfüllen vermag.

Ich hoffe, dies ist mir gelungen.

1.6 Zehn Jahre Volkszählungsurteil und die aktuelle Frage des Datenschutzes in Deutschland

Das Bundesverfassungsgericht hat am 15. Dezember 1983 den Grundrechtscharakter der "informationellen Selbstbestimmung" festgeschrieben und damit den Datenschutz zu einer elementaren Funktionsbedingung des freiheitlichen demokratischen Gemeinwesens erklärt, das auf der Handlungs- und Mitwirkungsfähigkeit seiner Bürger gründet. Dieses Grundrecht gewährleistet dem Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. Es ist das zentrale Mittel zur Gestaltung der Informationsbeziehungen zwischen dem Einzelnen und den Institutionen in Staat und Gesellschaft. Das Bundesverfassungsgericht hat seine Grundposition in der Zwischenzeit in einer Reihe weiterer Urteile eindrucksvoll bekräftigt.

Allerdings: Dieses Grundrecht kann im überwiegenden Interesse der Allgemeinheit durch Gesetze eingeschränkt werden, die freilich den Grundsätzen der Bestimmtheit und der Verhältnismäßigkeit entsprechen und organisatorische Vorkehrungen sowie Verfahrensregelungen treffen müssen, die der Gefahr einer Verletzung des Persönlichkeitsrechtes entgegenwirken. Wie mit personenbezogenen Daten umzugehen ist, darf weder administrativer Zweckmäßigkeit noch dem Markt überlassen bleiben, sondern ist im Gesetzgebungsverfahren, d. h. vor den Augen der Öffentlichkeit, zu entscheiden.
Das Grundrechtsverständnis von der Selbstbestimmung des Bürgers als Regelfall und ihrer Einschränkung als Ausnahme ist allerdings keineswegs von allen Seiten als Selbstverständlichkeit akzeptiert worden: Nach 10 Jahren ist eine positive, aber auch eine kritische Bilanz zu ziehen. Nach dem Volkszählungsurteil sind, wenn auch in vielen Fällen in langwierigen Verfahren, viele gesetzgeberische Aktivitäten entfaltet worden. Dabei mußte mancher datenschutzrechtliche Fortschritt hart erkämpft werden.

In Dutzenden von Gesetzen ist nunmehr das "Kleingedruckte" des Rechts auf informationelle Selbstbestimmung bereichsspezifisch geregelt. Das so entstandene Normengeflecht ist engmaschig und kompliziert. Dies steht der Intention des Verfassungsgerichtes, der Bürger solle aus einfachen Gesetzen erkennen können, mit welcher Verarbeitung seiner Daten er zu rechnen hat, häufig entgegen. Ich stelle in Frage, ob diese Normenflut mit ihren perfektionistischen und detaillistischen Regelungen der Verwirklichung des Grundsatzes der Verhältnismäßigkeit dient und wirklich

notwendig ist. Die Effizienz der staatlichen Verwaltung leidet unter der Last dieser Regelungen; enge, starre Gesetze behindern die Kreativität der Gesellschaft.

Die Fülle und Kompliziertheit der Datenverarbeitung in den unterschiedlichen Verwaltungsbereichen ist für diese Regelungsdichte verantwortlich. Sie ist notwendige Folge der Entwicklung hin zur "Informationsgesellschaft", aber auch zu einem in allen Lebensbereichen vorsorgenden, versorgenden, entmündigenden und herrschenden Staat.

In *wesentlichen* Bereichen blieb dagegen der Datenschutz ungeregelt. Auf Bundesebene gibt es z. B. bis heute keine hinreichenden datenschutzrechtlichen Vorschriften auf den Gebieten des Arbeitnehmerdatenschutzes, der Justizmitteilungen und der Zwangsvollstreckung, des Abgabenrechts, des Mieterschutzes, der Arbeit von Auskunfteien, Detekteien und privaten Sicherheitsdiensten und der Bundespolizeibehörden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat an den Bundesgesetzgeber appelliert, diese Lücken umgehend im Sinne der informationellen Selbstbestimmung zu schließen.

Zwei große Themenbereiche beherrschen die Innenpolitik und prägen die derzeitige Situation des Datenschutzes: Die innere Sicherheit und der Zustand unserer Wirtschafts- und Sozialordnung. Auf diesen Feldern werden die Menschen verängstigt; sie rufen nach mehr Staat. Auf beiden Gebieten wird die - vermeintliche - Lösung darin gesucht, die gesetzlichen Möglichkeiten zur Verarbeitung personenbezogener Daten erheblich auszuweiten und dabei die Rechte des Einzelnen einzuschränken.

Auf dem Gebiet der *Strafverfolgung* haben sich bisher die Ermittlungen auf den Beschuldigten konzentriert; die prozessuale Aufklärung geschah im wesentlichen offen. Jetzt setzt man auf Heimlichkeit und interessiert sich für Unbeteiligte. Es geht weniger um die Aufklärung eines konkreten Tatverdachts, sondern um flächendeckende Sammlung personenbezogener Daten unter dem Stichwort "vorbeugende Verbrechensbekämpfung". Der Staat hält sich nicht mehr an die Grenzen der Ausforschung, die selbstverständlich waren, und er trifft dabei auf breite öffentliche Zustimmung. Vor der Euphorie, mit Datensammlungen könne man dem Verbrechen einen Schritt voraus sein oder ihm einen entscheidenden Schlag versetzen, kann ich nur warnen.

Im Bereich der *Wirtschafts- und Sozialordnung* wird auf drastische Weise versucht, durch die Einführung neuer Überwachungsverfahren die Kosten zu mindern. Daten werden abgeglichen im Sinne der Kostendämpfung (so etwa bei der Intensivierung der Kontrolle der Ärzte im Gesundheitsstrukturgesetz) oder um mißbräuchliche Inanspruchnahme von Sozialleistungen aufzudecken (insbesondere durch regelmäßige Datenabgleiche bei Sozialhilfe und Arbeitsförderung). Aber, es geht wohl nicht anders ...

In der Informationsgesellschaft ist der effektive Schutz der Privatsphäre die Voraussetzung für eine angstfreie und verantwortliche Teilnahme der Bürger an ihrer Gesellschaft.

Die wichtigste Folge dieser Einsicht ist, daß Datenschutzvorschriften nicht nur Rechtssicherheit, sondern auch *materielle Freiheitsräume* garantieren müssen. Dies bedeutet, daß bei der Entscheidung, ob der Einzelne einer Auskunftspflicht unterworfen werden soll, ob seine Daten außer für den Erhebungszweck auch für andere Zwecke freigegeben werden sollen, wie lange Daten aufbewahrt werden dürfen und welche Datenverarbeitungsvorgänge dem Betroffenen verborgen bleiben dürfen, *jeweils strenge Maßstäbe angelegt* werden müssen.

Datenschutzrechtliche Verstöße gehen meist auf Unkenntnis und mangelndes Problembewußtsein der öffentlichen Stellen zurück. *Aus- und Fortbildung* in Fragen des Datenschutzes muß daher erheblich mehr Gewicht beigemessen werden als bisher. Insbesondere sind Bemühungen zu fördern, den Datenschutz in den einschlägigen Ausbildungsplänen (Informatikunterricht in den Schulen, beim Rechts- und Informatikstudium) sowie den Fortbildungsveranstaltungen der öffentlichen Verwaltung als obligatorisches Fach zu verankern. Denn Datenschutz zwingt zu einfachen - häufig sogar billigeren - Lösungen.

Die *Datenverarbeitungstechniken* haben sich gegenüber der Zeit des Volkszählungsurteils geradezu revolutionär verändert. Der Umsetzung dieses Urteils durch spezifische Rechtsgrundlagen muß daher verstärkt die Entwicklung geeigneter technisch-organisatorischer Maßnahmen zu Seite gestellt werden. Der Blick des Datenschutzes muß sich stärker auf die Technik des Verarbeitungsprozesses selbst richten. Dies bedeutet nicht nur die Entwicklung spezifischer Datenschutzvorkehrungen für neue Informations*techniken* (z. B. Chipkarte), sondern auch neuer *Anwendungs*formen (z. B. Mauterhebung).

Die *Europäische Union* wird zunehmend zur Informationsgemeinschaft. Dies macht einen europäischen Datenschutz erforderlich. Die Konferenz der Datenschutzbeauftragten teilt mit den europäischen Nachbarn nicht nur die Überzeugung, daß der Datenschutz in Europa harmonisiert werden muß, sondern auch, daß die Rechte der Gemeinschaftsbürger auf einem hohen Niveau gesichert werden müssen, damit die Öffnung der Grenzen für Güter, Kapital und Dienstleistungen - und damit auch für persönliche Daten - nicht zu verfassungswidrigen Nachteilen für den Einzelnen führt.

1.7 Altdaten

1.7.1 Maßnahmen, Erfahrungen

Die gemäß § 35 SächsDSG bestehende Meldepflicht für Altdaten habe ich in meinem 1. Tätigkeitsbericht in den Abschnitten 1.3.2 und 16.1.1 ausführlich dargestellt.

Es scheint, daß die gemäß § 35 Abs. 2 S. 2 SächsDSG bestehende Pflicht der tatsächlichen Inhaber der Altdaten, diese "*unter Verschluß zu nehmen*", im großen und ganzen ausreichend erfüllt worden ist. Jedenfalls sind mir keine Verstöße bekannt geworden.

Vereinzelt gehen immer noch Meldungen gemäß § 35 Abs. 2 SächsDSG ein.

Der Grad der Vollständigkeit, mit der gemeldet worden ist, läßt sich schwer abschätzen. Sicher ist, daß die öffentlichen Stellen vollständiger gemeldet haben als die Unternehmen.

Meinen im 1. Tätigkeitsbericht angekündigten Versuch, Unternehmen an ihre Meldepflicht zu erinnern und dadurch die Altdatenbestände auf diesem Gebiet mit höherem Vollständigkeitsgrad zu sichern, habe ich bald abgebrochen: Die Erfolge waren gering. Außerdem war es - und dies gilt vor allem für den Unternehmensbereich - wesentlich dringender, die Klärung des weiteren Verbleibs der gemeldeten Altdaten in Gang zu bringen, d. h. § 35 Abs. 4 S. 1 SächsDSG umzusetzen. Mit zunehmendem Zeitablauf wächst nämlich die Gefahr, daß die Inhaber der Altdaten den Eindruck gewinnen, daß es dem Freistaat Sachsen mit der Sicherung der Altdaten doch nicht so ernst sei, wie es dem Willen des Gesetzgebers entspräche, der in den Regelungen der §§ 35 SächsDSG und 5 Abs. 2 i. V. m. 4 Abs. 2 S. 2 SächsArchG zum Ausdruck kommt, mit denen sich Sachsen in erfreulicher Weise profiliert hat.

Ich habe das zuständige SMI, das seit Juni 1993 mit dem Sächsischen Archivgesetz auch über die nötige Regelung verfügt, die an § 35 Abs. 4 S. 1 SächsDSG anschließt und diese Vorschrift konkretisiert, mehrfach gedrängt und dabei die Unterstützung meiner Dienststelle bei der Entscheidung über den Verbleib der gemeldeten Alt-Unterlagen angeboten. Denn mein Mitarbeiter, der die Altdatenmeldungen bearbeitet hat, verfügt durch deren Auswertung sowie durch stichprobenweise Einsicht in Altdatenbestände auf diesem Gebiet wohl über die größte Erfahrung und den besten Überblick.
Man hat sich auf der Leitungsebene des SMI mit der Entscheidung über einen ersten Anfang der Übernahmeaktion jedoch sehr viel Zeit gelassen, nachdem diese Aktion in Zusammenarbeit zwischen dem Archivreferat des SMI und meiner Dienststelle bereits gut vorbereitet war.
Es ist freilich klar, daß dem staatlichen Archivwesen des Freistaates Sachsen die nötige personelle und räumliche Kapazität zur Verfügung gestellt werden muß, damit der in den genannten Vorschriften zum Ausdruck kommende politische Wille auch praktisch umgesetzt werden kann.

Für den Komplex der *schulischen Altdaten* hatte ich weitgehende Vorarbeiten für eine gemeinsame Verwaltungsvorschrift des SMK und des SMI über den Umgang mit Altdatenbeständen im Schulbereich (VwVAltdaten im Schulbereich) geleistet. Meine im 1. Tätigkeitsbericht (Abschnitt 1.3.4) geäußerte Erwartung, diese Verwaltungsvorschrift werde bald erlassen werden, hat getrogen: Beide Ministerien hatten anscheinend kein Interesse an der Angelegenheit.

1.7.2 Die Auswertung der Meldungen

Die *Auswertung* der Meldungen ist im wesentlichen abgeschlossen. Sie ist im einzelnen im Abschnitt 16.3.1 erläutert.

2 Parlament

2.1 Unklare Regelung in Parteiengesetznovelle

Auf meine Initiative hin hat sich der Bundesbeauftragte für den Datenschutz mit einer Regelung des Gesetzes zur Änderung des Parteiengesetzes (PartG) vom 28. Januar 1994 befaßt, die Anlaß zu Fehldeutungen geben kann:

So bestimmt der neugefaßte § 24 Abs. 1 PartG, daß die Landesverbände der Parteien und die ihnen nachgeordneten Gebietsverbände ihrem Rechenschaftsbericht lückenlose Aufstellungen *aller* Zuwendungen - dies sind Mitgliedsbeiträge und Spenden, unabhängig von ihrer Höhe - mit Namen und Anschriften der Zuwender beifügen müssen.

Die Rechenschaftsberichte der Parteien sind gemäß § 23 Abs. 2 PartG nach Überprüfung durch einen Wirtschaftsprüfer oder einen vereidigten Buchprüfer dem Präsidenten des Deutschen Bundestages vorzulegen, der die Berichte sodann als Bundesdrucksache verteilt.

Vorgenannte Regelungen können somit den Schluß nahelegen, Namen und Anschriften *aller Zuwender* müßten veröffentlicht werden.

Ich halte den § 24 Abs. 1 PartG unter verfassungsrechtlichen Gesichtspunkten (Stimmigkeit des Gesetzeswerkes in sich, Grundsatz der Verhältnismäßigkeit) für mißglückt:

Dafür spricht:

- Nach § 25 Abs. 2 PartG sind *Spenden* jenseits der Publizitätsgrenze von 20.000 DM zur Veröffentlichung mit Namen und Adressen der Spender bestimmt. Diese Begrenzung hätte keinen Sinn, wenn man dem Wortlaut des § 24 Abs. 1 (grenzenlose Veröffentlichung aller Zuwendungen) folgen würde.

- Die Pflicht der Parteien, ihren Rechenschaftsberichten eine lückenlose Aufstellung aller Zuwendungen beizufügen, dient ausschließlich *der Kontrolle durch den Wirtschaftsprüfer* (§ 23 Abs. 2 Satz 1 PartG). Nur an diese Stellen sollen die Detailinformationen über Mitgliedsbeiträge und Kleinspenden gelangen. Dagegen sind dem Präsidenten des Deutschen Bundestages - wie die ausdrückliche gesetzliche Fixierung der Publizitätsgrenze belegt - nur Spenden über 20.000 DM einzelfallbezogen mitzuteilen.

Diese Auslegung des § 24 Abs. 1 Satz 4 PartG wird dem verfassungsrechtlichen Gebot des Persönlichkeitsschutzes, der Koalitionsfreiheit wie auch dem mit der Novellierung des Parteiengesetzes verfolgten Ziel, die Parteienfinanzierung transparent zu gestalten, gleichermaßen gerecht.

2.2 Untersuchungsausschuß "Personalüberprüfung durch die Staatsregierung"

Der Sächsische Landtag hat am 19. März 1993 gemäß Art. 54 Abs. 1 SächsVerf und §

2 UAusschG den 2. Untersuchungsausschuß mit dem Ziel eingesetzt, exemplarisch in den Staatsministerien des Innern und für Kultus die Entlassungs- und Weiterbeschäftigungspraxis zu durchleuchten.

Nach Art. 57 SächsVerf habe ich mich von Anfang an dem 2. Untersuchungsausschuß zur Unterstützung seiner parlamentarischen Kontrolle zur Verfügung gestellt und ihn - soweit erforderlich - in datenschutzrechtlicher Hinsicht beraten.

Insbesondere habe ich mich zu der Pflicht der Ministerien geäußert, dem Ausschuß Personalakten zur Einsicht vorzulegen: Nach der Rechtsprechung des Bundesverfassungsgerichts (BVerfGE 67, 100 [130]) steht dem Untersuchungsausschuß ein weitgehendes Informationsrecht zu. Nur wenn ein unverhältnismäßiger Eingriff in die Privatsphäre des Betroffenen zu besorgen wäre, stößt dieses Informationsrecht an seine Grenzen.

Grundsätzlich bestehen keine Bedenken gegen eine Vorlage von Personalakten an den Untersuchungsausschuß, soweit sie dem Untersuchungsauftrag dienlich sind. Da aber Personalakten ihrem Wesen nach vertraulich zu behandeln sind, habe ich Vorkehrungen zum Schutz der betroffenen Bediensteten im Untersuchungsausschuß angeregt:

1. Die Untersuchungsausschußmitglieder sollten sich verpflichten, Verschwiegenheit über ihnen aus den Personalunterlagen bekannt gewordene personenbezogene Interna zu bewahren.

2. Personalangelegenheiten sollten ausschließlich in *nichtöffentlicher* Sitzung behandelt werden, es sei denn, daß die einzelnen Fälle anonymisiert werden (z. B. durch Numerierung oder Vergabe von Buchstaben), so daß außenstehende Dritte keine Rückschlüsse auf eine bestimmte Person ziehen können.

3. Die Behandlung der Personalakten zur Vorbereitung der Ausschußsitzung sollte formal festgelegt werden. Dabei sollte darauf hingewirkt werden, daß *nur die Ausschußmitglieder* zur Vorbereitung der Sitzung Einsicht in die Personalakten - zweckmäßigerweise an *einem* Ort (z. B. im Büro des Ausschußsekretärs) - nehmen können.

Ich habe auch auf Verschwiegenheitspflichten der Ausschußmitglieder und mögliche Sanktionen (z. B. §§ 203 Abs. 2 Nr. 4; 353 b StGB) hingewiesen.

In einer weiteren Stellungnahme habe ich mich auf Anforderung des Ausschußvorsitzenden zur Personalaktenführung allgemein und zur Behandlung von "Gauck"-Unterlagen, denen insgesamt Personalaktenqualität zukommt, im besonderen geäußert.

Als der Ausschuß die Frage diskutierte, ob die Öffentlichkeit auszuschließen sei, wenn ehemalige Polizeibedienstete der DDR nicht nur zu früheren amtlichen Funktionen (diese sind öffentlich zu behandeln), sondern auch zu eventuellen früheren konkreten Dienstaufgaben oder Verfehlungen im Rahmen bestimmter Polizeieinsätze befragt werden, habe ich für eine Behandlung in geschlossener Sitzung plädiert. Ich habe mich

dabei an § 171 b GVG orientiert, da "schutzwürdige Interessen" der Zeugen auch dann verletzt würden, wenn sie von ihrer Möglichkeit, nach § 55 StPO die Auskunft zu verweigern, Gebrauch machen, zumal der Auftrag des Untersuchungsausschusses weniger dahin ging, frühere einzelne Verstöße gegen die Grundsätze der Menschlichkeit oder Rechtsstaatlichkeit, sondern zunächst die Einstellungspraxis nach der Wende aufzuklären.

Der Juristische Dienst des Landtages hat - mit durchaus schwerwiegenden Argumenten, insbesondere zur grundsätzlichen Öffentlichkeit des Untersuchungsausschusses - die gegenteilige Meinung begründet. Seine Kompetenz zur Beratung des Ausschusses in *allen* juristischen Fragen, mithin auch zu Datenschutzproblemen, habe ich *neben meiner* Beratungsfunktion zu akzeptieren.
Der Ausschuß hat die sachliche Kontroverse dadurch salomonisch entschieden, daß die Beweisanträge von Behauptungen zu früheren Verfehlungen der Zeugen bereinigt wurden.

Erfreulich war ein einstimmiger Beschluß des 2. Untersuchungsausschusses, wonach meinen Mitarbeitern und mir Einsicht in die stenographischen Ausschußprotokolle gewährt wird, soweit es meine Aufgaben in begründeten Fällen erfordern.

2.3 Personenbezogene Daten in Berichten des Petitionsausschusses

Die Sächsische Verfassung garantiert jedermann das Recht, sich mit Bitten oder Beschwerden (Petitionen) an den Landtag zu wenden. Der beim Landtag eingerichtete *Petitionsausschuß* prüft die Eingaben und gibt dem Landtag Empfehlungen zur Beschlußfassung. Der Petitionsausschuß ist gemäß § 67 Abs. 2 der Geschäftsordnung des Landtags verpflichtet, dem Landtag monatlich einen Bericht über die Beschlußempfehlungen vorzulegen.

In einem Bericht fiel mir auf, daß die Petenten mit Namen und Wohnort angegeben waren.
Ich habe dem Petitionsausschuß daraufhin mitgeteilt, daß seine Berichte durch die Veröffentlichung als Landtagsdrucksachen einer Vielzahl von Personen zur Kenntnis gelangen. Da die Beschlußempfehlungen lediglich einen *allgemeinen Überblick* über die Anzahl und den wesentlichen Inhalt der Petitionen sowie die Tätigkeit des Petitionsausschusses geben sollen, ist aus datenschutzrechtlicher Sicht unbedingt darauf zu achten, daß ein Personenbezug nicht hergestellt werden kann.

Mir wurde von der Landtagsverwaltung versichert, daß der Datenschutz bei den Berichten in Zukunft besonders beachtet wird.

3 Europäische Gemeinschaft / Europäische Union

3.1 EG-Richtlinie zum Datenschutz

Der dem Ministerrat der EG seit Oktober 1992 vorliegende überarbeitete EG-Richtlinienentwurf wurde im Juni 1993 von der Arbeitsgruppe Wirtschaftsfragen in erster Lesung beraten.

Im Rahmen der zweiten - entscheidenden - Lesung sind noch wichtige Fragen zu klären, die auch die Konferenz der Datenschutzbeauftragten der EG-Staaten in einer Entschließung vom 29. April 1993 aufgezeigt hat. Hiervon betroffen sind zunächst der generelle Anwendungsbereich der Richtlinie und das Recht der Mitgliedsstaaten, einen gegenüber der Richtlinie höheren Schutzstandard im nationalen Recht festzuschreiben. Auch werden Fragen einer verstärkten Zweckbindung, einer Vereinfachung oder Befreiung von der Dateien-Meldepflicht sowie der Umfang der Befugnis der Kontrollbehörden noch zu erörtern sein.

Aus deutscher Sicht ist insbesondere von Bedeutung, ob die Institution des betrieblichen Datenschutzbeauftragten noch Eingang in die Richtlinie findet oder zumindest - parallel zur Richtlinie - weiter bestehen bleiben kann. Inzwischen sind Anzeichen zu vernehmen, wonach die EG-Kommission eine Sonderregelung über die Bestellung betrieblicher Datenschutzbeauftragter formulieren wird, die klarstellt, daß entsprechende Regelungen in den Mitgliedsstaaten beibehalten werden können. Ich warne vor einer Institutionalisierung der betrieblichen Datenschutzbeauftragten; sie können jedenfalls eine externe Datenschutzkontrolle nicht einschränken oder ersetzen.

Es ist geplant, die Beratungen der Richtlinie unter deutschem Vorsitz mit der zweiten Lesung noch im zweiten Halbjahr 1994 abzuschließen. Das Ergebnis der Beratungen wird sodann dem Europäischen Parlament vorgelegt werden. Mit der Verabschiedung der Richtlinie ist nicht vor 1995 zu rechnen.

Ich werde in Brüssel Einzelheiten künftiger Datenschutzkontrollen besprechen.

3.2 EG-Ministervereinbarung über die Einrichtung einer Europol-Drogenzentralstelle

Zur Bekämpfung des illegalen Drogenhandels und der damit verbundenen Geldwasch-aktivitäten sieht eine EG-Ministervereinbarung vom 28. April 1993 die Einrichtung einer Europol-Drogenzentralstelle vor. Die bei dieser Stelle eingesetzten Verbindungsbeamten der beteiligten Mitgliedsstaaten sollen Zugriff auf einschlägige nationale kriminalpolizeiliche Informationen und Erkenntnisse erhalten. Der Vereinbarung zufolge haben die Verbindungsbeamten nach Maßgabe der Bestimmungen ihrer nationalen Gesetze sowie einschlägiger Rechtsvorschriften über die Verarbeitung personenbezogener Informationen und unter Einhaltung der vom liefernden Staat angegebenen Bedingungen über die Nutzung solcher Informationen zu handeln.

Aus meiner Sicht ist datenschutzrechtlich von Bedeutung, auf welcher Rechtsgrundlage ein Verbindungsbeamter Zugriff auf sächsische Polizeidatenbestände nehmen kann und eine Datenübermittlung zwischen den Verbindungsbeamten verschiedener Staaten erfolgt. Ferner ist zu klären, welche Bedingungen seitens der Mitgliedstaaten aufgestellt werden, damit eine Datenübermittlung von den deutschen an ausländische Verbindungsbeamte erfolgen kann.

Es ist sicherzustellen, daß nur Informationen einschließlich personenbezogener Daten zwischen den Mitgliedsstaaten über drogenbezogene Straftaten, nicht jedoch über andere, von der Ministervereinbarung nicht erfaßte Straftaten, ausgetauscht werden.

Es muß gewährleistet sein, daß durch die Übermittlung von Datenbeständen, die sich im Besitz des Freistaats Sachsen befinden, nicht gegen den Zweck eines deutschen Gesetzes, insbesondere nicht gegen Vorschriften zur Speicherungs-, Nutzungs- oder Übermittlungsbeschränkung oder zur Löschungsverpflichtung verstoßen wird.

Das SMI habe ich über die datenschutzrechtlichen Problemfelder unterrichtet und um Stellungnahme gebeten. Wie mir das Landeskriminalamt mitteilte, könne vor Abschluß der Beratung dieser Thematik in den maßgeblichen beschlußfassenden Gremien (Arbeitskreis II der Innenministerkonferenz und Arbeitsgemeinschaft Kripo) seitens des Freistaates Sachsen nicht definitiv Stellung bezogen werden. Die Angelegenheit werde ich weiter im Auge behalten.

4 Medien

Reality-TV

Im Wettstreit um hohe Einschaltquoten entstanden die Sendungen des sog. Reality-TV. Videos, die Beteiligte, z. B. Mitarbeiter der Rettungsdienste direkt am Ort eines Unfalles, einer Rettungsaktion oder eines Katastropheneinsatzes gedreht haben, werden später gesendet, so z. B. in den Sendereihen "Notruf" (RTL) oder "Retter" (SAT 1).

Wegen des Persönlichkeitsrechts der Verunglückten und anderer persönlich Betroffener ist das bedenklich. Denn das Fernsehen ist zwar nach Art. 5 Abs. 1 Satz 2 GG in seiner Berichterstattung grundsätzlich frei. Nach Abs. 2 findet aber die Presse- und Medienfreiheit ihre Schranken u. a. in den allgemeinen Gesetzen. Bei der Berichterstattung sind also die Unantastbarkeit der Würde jedes Einzelnen nach Art. 1, die freie Entfaltung der Persönlichkeit nach Art. 2 Abs. 1 und das daraus abgeleitete Recht auf informationelle Selbstbestimmung zu beachten. Einzelheiten dazu sind in den Medien- oder Rundfunkgesetzen der Länder festgelegt (z. B. Staatsvertrag über den Mitteldeutschen Rundfunk vom 19.5.1991; Gesetz über den privaten Rundfunk und neue Medien in Sachsen vom 17.6.1991).

Nach meiner Auffassung verletzen in der Regel Aufnahmen mit Videokamera oder Filmkamera von Menschen in Not, Opfern von Unglücksfällen, von Schwerstkranken oder Sterbenden deren Recht auf informationelle Selbstbestimmung.

Videoaufnahmen werden gelegentlich auch von Polizisten, Feuerwehrleuten oder von Mitarbeitern von Rettungsdiensten im Rahmen ihrer Dienstaufgaben gemacht, um Unfallsituationen für spätere Zwecke zu dokumentieren, Beweise über den Unfallhergang oder auch den Rettungsvorgang zu sichern (z. B. Aufnahmen von Falschparkern, welche die Rettungsaktionen behindern) oder um die Aufnahmen später für die Ausbildung von Rettungspersonal zu verwenden.

Wenn auf solchen Filmaufnahmen die Opfer zu identifizieren sind, erheben die filmenden Mitarbeiter von Rettungsdiensten oder der Feuerwehr während ihrer Einsätze personenbezogene Daten. Sie dürfen nur für den Zweck benutzt werden, für den ursprünglich erhoben worden sind. Eine Unfalldokumentation oder die Beweissicherung im Rahmen der Dienstaufgaben kann datenschutzrechtlich erlaubt sein. Die Verwendung für einen anderen Zweck, hier für Sendungen im Fernsehen, ist aber unzulässig. Datenschutzbestimmungen untersagen Bediensteten von Behörden, dienstliche Aufnahmen an Fernsehstationen weiterzugeben, wenn auf den Unfallaufnahmen ein Opfer zu erkennen ist.

Gerade Unfallopfer, Leidende, in Not geratene Menschen, Hilflose oder Sterbende, haben ein Recht darauf, daß ihre Menschenwürde, ihr Recht auf informationelle Selbstbestimmung, beachtet, sie nicht unfreiwillig ins öffentliche Rampenlicht gezogen und ihr Unglück vermarktet wird.

Wenn Aufnahmen, auf denen der Betroffene identifizierbar ist, unzulässig an

Fernsehsender übermittelt werden, können die Betroffenen möglicherweise eine Unterlassung der Sendung oder nach erfolgter Sendung Schadensersatz verlangen.

Deshalb ist es richtig, wenn sich Polizisten, Feuerwehrleute, Rettungsassistenten, Rettungssanitäter und Notärzte von sich aus oder in ihren Organisationen von diesen "Schaustellungen menschlicher Not" im Fernsehen distanzieren und für interne dienstliche Zwecke angefertigte Videos nicht an Fernsehstationen weiterleiten.

Ich hoffe, daß die öffentliche Kritik an der Art der Berichterstattung über Extremsituationen und bei Unfällen die Eigenverantwortlichkeit der Programmveranstalter und ihrer Mitarbeiter in den Fernsehredaktionen stärkt, die Sendungen im Sinne des Rechts der Opfer auf informationelle Selbstbestimmung und auf Achtung ihrer Würde zu gestalten. Anderenfalls muß der Gesetzgeber tätig werden.

5 Inneres

5.1 Personalwesen

5.1.1 Verwaltungsvorschrift des SMI über die Führung und Verwaltung von Personalakten

In zwei umfangreichen Stellungnahmen habe ich mich zu dem Entwurf der Verwaltungsvorschrift geäußert. Auch wenn ein Großteil meiner Anregungen umgesetzt worden ist, enthält die am 17. Dezember 1993 in Kraft getretene Verwaltungsvorschrift (SächsABl. S. 1337) noch immer wesentliche datenschutzrechtliche Mängel, namentlich in folgender Hinsicht:

Anwendungsbereich
Die Verwaltungsvorschrift ist aufgrund von § 160 SächsBG erlassen worden und gilt nur für Beamte.

Da weder die Tarifverträge noch allgemeine Vorschriften des Arbeitsrechts den Umgang mit den Personalakten von Angestellten und Arbeitern im öffentlichen Dienst regeln, werden deren Personalakten in der Praxis meist nach beamtenrechtlichen Vorschriften behandelt. Dabei wird übersehen, daß die analoge Anwendung beamtenrechtlicher Vorschriften zu Fehlern führen kann, und zwar aus folgenden Gründen: Wegen des Fehlens spezieller Regelungen zur Aktenführung in den Tarifverträgen (bis auf das Akteneinsichtsrecht) ist das Sächsische Datenschutzgesetz als Auffanggesetz anzuwenden. Insbesondere § 31 SächsDSG, der die Personaldatenverarbeitung für Bewerber und Beschäftigte im öffentlichen Dienst regelt, führt bei einigen Fallgestaltungen zu einem anderen Ergebnis als die Anwendung des Sächsischen Beamtengesetzes (z. B. Entfernung nachteiliger Unterlagen für einen Beamten nach drei Jahren auf Antrag - bei Angestellten von Amts wegen gem. § 19 SächsDSG; zur Aufbewahrungsfrist von Personalakten vgl. nachstehend unter 5.1.2).

Vor diesem Hintergrund habe ich angeregt, eine für Arbeiter, Angestellte und Beamte gleichermaßen geltende Verwaltungsvorschrift (unter Beteiligung des SMF und ohne Verstoß gegen die Tarifautonomie) zu erlassen. In einer solchen "einheitlichen" Verwaltungsvorschrift hätten da, wo es erforderlich ist, unterschiedliche Regelungen für Arbeiter und Angestellte einerseits und Beamte andererseits getroffen werden können. Leider ist das SMI diesem Vorschlag nicht gefolgt.

Die derzeitige Rechtslage unterstreicht den dringenden Handlungsbedarf für die Tarifparteien (auf den ich bereits in meinem 1. Tätigkeitsbericht unter 5.1.1 hingewiesen habe), endlich für Regelungen auf diesem Gebiet zu sorgen.

Rückgabe von Beihilfeunterlagen
Außerhalb der Landesverwaltung darf die Beihilfebearbeitung dem Kommunalen Versorgungsverband Sachsen (KVS) übertragen werden. Es ist unverständlich, warum die Verwaltungsvorschrift - *abweichend von der bisherigen Praxis* - vorsieht, die Beihilfeunterlagen nach Abschluß der Bearbeitung der jeweiligen Personalstelle

zuzuleiten, nicht aber dem Antragsteller, der sie dem KVS übersandt hat (was soll und will die Personalstelle mit den Unterlagen anfangen? Zu welchem Zweck sollen medizinische Daten des Bediensteten und seiner Familie zur Kenntnis der Personalstelle gelangen?). Erfolgt demgegenüber die Beihilfebearbeitung für *Staats*bedienstete - im Landesamt für Finanzen oder in einer anderen Beihilfestelle (sie muß organisatorisch von der Personalverwaltung getrennt sein) -, sind die Unterlagen nach derselben Verwaltungsvorschrift hingegen an den Beamten zurückzusenden. In dieser Ungleichbehandlung sehe ich keinen Sinn.

Anhörungsrecht
Das dem Beamten zustehende *Anhörungsrecht* wird in der Verwaltungsvorschrift auf eine bloße *Informationspflicht* der Behörde reduziert. Dies widerspricht nicht nur dem Gesetzeswortlaut, sondern ignoriert auch die in der Rechtsprechung zu Anhörungen entwickelten Grundsätze. Auf die Möglichkeit mündlicher Stellungnahmen und deren Behandlung geht die Verwaltungsvorschrift nicht ein.

Abschriften und Kopien aus Personalakten
Nach der Verwaltungsvorschrift darf eine Personalakte nicht in ihrer Gesamtheit abgeschrieben oder kopiert werden. Ich habe darauf hingewiesen, daß durch diese Beschränkung eine aus wenigen Schriftstücken bestehende Personalakte nicht kopiert werden dürfte, dagegen aber eine sehr umfangreiche unter Auslassung weniger Schriftstücke. Mein Vorschlag, Kopien und Abschriften zuzulassen, solange dies einen vertretbaren Rahmen nicht sprengt, ist leider nicht umgesetzt worden. Es bleibt das Grundrecht jedes Bediensteten, jederzeit genau zu wissen, was seine Personalakte enthält. Warum sollte er keine Kopie erhalten?

Entfernung von Unterlagen aus der Personalakte vor Einsichtnahme
Nach der Verwaltungsvorschrift soll vor der Einsichtnahme in die Personalakte eine Terminabsprache zwischen dem Beamten und der Personalstelle auch deshalb erfolgen, damit zuvor bestimmte Unterlagen aus der Personalakte entfernt werden können. Dies widerspricht dem Recht auf Einsichtnahme in die *vollständige* Personalakte, selbst wenn sie Daten Dritter enthält (z. B. im Zusammenhang mit Beschwerden und Behauptungen, die dienstrechtlich relevant werden können).

Keine Kostenerstattung bei Ausübung des Akteneinsichtsrechts
Nach der Verwaltungsvorschrift werden Kosten (insbesondere Reisekosten), die dem Beschäftigten durch die Akteneinsicht entstehen, *nicht* erstattet. Ich habe mich dafür eingesetzt, daß die Verwaltungsvorschrift positiv feststellt, daß Reisekosten zu erstatten sind und Kopien kostenlos angefertigt werden können. Es geht nicht an, daß Betroffene aus Kostengründen von der Geltendmachung eines ihnen zustehenden (Schutz-)Rechts abgehalten werden. Zudem verstößt eine solche Regelung gegen den Grundsatz einer gleichmäßigen Behandlung, da sie Beamte bevorzugt, deren Beschäftigungsbehörde zugleich personalaktenführende Stelle ist.

Keine Akteneinsicht bei Urlaub in der Personalabteilung
Nach der Verwaltungsvorschrift darf das Akteneinsichtsrecht eingeschränkt werden, wenn der zuständige Mitarbeiter der Personalstelle in Urlaub ist. Ich halte dies für problematisch. Es ist Aufgabe des Dienstherrn, durch Bestellung einer

Urlaubsvertretung die Rechte des Beamten zu wahren.

Automatisierte Verarbeitung ärztlicher Unterlagen
Durch die Verwendung des einschränkenden Wortes "grundsätzlich" dürfen nach der Verwaltungsvorschrift entgegen der gesetzlichen Regelung (§ 124 Abs. 3 SächsBG) ärztliche Unterlagen in Ausnahmefällen automatisiert verarbeitet werden. Auf die Streichung dieses Wortes habe ich leider ohne Erfolg hinzuwirken versucht. Besonders bedauerlich ist, daß sogar mein Hinweis auf den unvollständigen (und damit unverständlichen) Satz 2 in Nr. 8.5 ignoriert worden ist.

Sofern ich feststellen sollte, daß es aufgrund der in Teilen rechtswidrigen Verwaltungsvorschrift zu datenschutzrechtlichen Verstößen kommt, werde ich diese beanstanden.

Schon kurz nach Inkrafttreten der Verwaltungsvorschrift hat sich gezeigt, daß in ihr Weisungen zur Führung eines Versandnachweises und zur Rücklaufkontrolle von Personalakten fehlen, weswegen eine ergänzende "Anordnung zur Regelung der Aufbewahrung und Versendung von Personalakten" ergehen mußte.

5.1.2 Aufbewahrungsfrist für Personalakten von Arbeitern und Angestellten

Mehrfach wurde bei mir angefragt, wie lange die Personalakten von Arbeitern und Angestellten im öffentlichen Dienst aufzubewahren seien. Probleme haben sich deshalb ergeben, weil in den Tarifverträgen oder allgemeinen arbeitsrechtlichen Vorschriften klare Regelungen (wie etwa im Beamtenrecht) fehlen. Eine analoge Anwendung des § 123 Abs. 1 SächsBG, der die Aufbewahrungsfrist für die Personalakten von Beamten festlegt, auf die Personalakten von Arbeitern und Angestellten scheidet aus, weil die beamtenrechtliche Vorschrift an die grundsätzlich anders gestaltete Beamtenversorgung anknüpft. Als problematisch hat sich die Angelegenheit auch deshalb erwiesen, weil das Sächsische Datenschutzgesetz einerseits die Löschung personenbezogener Daten in Akten vorschreibt, wenn sie zur Aufgabenerfüllung der speichernden Stelle nicht mehr erforderlich sind (und das zuständige Archiv die Übernahme abgelehnt hat), andererseits aber die Löschung verbietet, wenn sie schutzwürdige Belange des Betroffenen beeinträchtigen könnte.

Wegen der grundsätzlichen Bedeutung dieser Frage habe ich mich an das SMF gewandt. Von dort wurde mitgeteilt, daß die Personalakte eines ausgeschiedenen Arbeitnehmers fünf Jahre nach Vollendung seines 65. Lebensjahres aufzubewahren sei, die Personalakten eines vorher verstorbenen Arbeitnehmers fünf Jahre nach Ablauf des Todesjahres.

Was die Aufbewahrung von Bezüge- und Lohnunterlagen betrifft, hat mich das SMF darüber informiert, daß wegen der in der Rentenversicherung noch erforderlichen Kontenklärungen und Leistungsbewilligungen in den neuen Bundesländern der Gesetzgeber eine Rechtsänderung beabsichtige, wonach Arbeitgeber in den neuen Bundesländern die am 31. Dezember 1991 vorhanden gewesenen Bezüge- und Lohnunterlagen aus übergeführten Einrichtungen oder Einrichtungen, deren Aufgaben übernommen wurden, noch bis zum 31. Dezember 2006 aufzubewahren hätten.

5.1.3 Umgang mit Gauck-Unterlagen in der Personalakte

Mehrere personalverwaltende Stellen haben bezweifelt, ob Gauck-Unterlagen und auch andere Unterlagen aus Personalüberprüfungen als Bestandteil der Personalakte anzusehen seien mit der Folge, daß der Beschäftigte zur vollständigen Einsicht in diese Unterlagen berechtigt wäre.

Das Sächsische Beamtengesetz enthält in §§ 117 ff. detaillierte Regelungen zum Umgang mit Personalunterlagen. Ob sie (als Original oder Kopie) Bestandteil einer Personalakte sind, richtet sich unabhängig vom Aufbewahrungsort allein nach ihrem Inhalt. Sie gehören nach der Definition des § 117 Abs. 2 SächsBG stets dazu, wenn sie mit dem Dienstverhältnis in einem *unmittelbaren* inneren Zusammenhang stehen.

Die Tarifverträge für Angestellte und Arbeiter enthalten - trotz jahrelanger Bemühungen und Hinweise der Datenschutzbeauftragten des Bundes und der Länder - keine hinreichenden Regeln zu Personalunterlagen (siehe aber Akteneinsichtsrecht nach § 13 BAT-O). Aus Gründen der Gleichbehandlung der Beschäftigten und einer einheitlichen Aktenführung in den Personalstellen muß von einem einheitlichen, also dem beamtenrechtlichen Personalaktenbegriff ausgegangen werden: Sachliche Gründe für eine *Ungleichbehandlung* sind unerfindlich; überdies zwingt das Recht auf informationelle *Selbstbestimmung* dazu, daß jeder Beschäftigte wissen (können) muß, *wer was wann* und bei welcher Gelegenheit über ihn *weiß*.

Nach diesen Grundsätzen haben der Erklärungsbogen des Beschäftigten, die Anfrage bei der Gauck-Behörde sowie deren "Mitteilung" (ein ausgefülltes Formular, das die Einschätzung der Gauck-Behörde enthält) *sicher* Personalaktenqualität. Gleiches gilt für Protokolle etc. von Personalkommissionen u. ä. *Anderes* gilt aber für die *Anlagen*, die der Mitteilung der Gauck-Behörde häufig zum Zwecke beispielhafter Erläuterung beigefügt sind. Sie enthalten z. B. Berichte des Bediensteten, die dieser früher als IM für das MfS gefertigt hat. *Hier fehlt die Unmittelbarkeit des inneren Zusammenhangs* mit dem jetzigen Dienst- beziehungsweise Beschäftigungsverhältnis, deshalb sind sie nicht Bestandteil der Personalakte. Außerdem bestimmt § 16 Abs. 4 StUG: "Dem Mitarbeiter (des MfS) kann auf Antrag Auskunft aus den von ihm erstellten Berichten und Einsicht in diese gewährt werden, wenn er glaubhaft macht, daß er hieran ein *rechtliches* Interesse hat. Dies gilt nicht, wenn das berechtigte Interesse Betroffener oder Dritter an der Geheimhaltung überwiegt." Dieser Opferschutz - der auch heute noch gute Gründe hat - ist von der Gauck-Behörde sicherzustellen. Er hat auch dann grundsätzlich Vorrang, wenn die Berichte der personalführenden Stelle zugänglich sind. Folglich müssen diese Anlagen gesondert - und sicher! - aufbewahrt werden, und sind zu vernichten, wenn sie nicht mehr, z. B. in einem Gerichtsverfahren, benötigt werden.

Außerdem hatte ich zu beurteilen, ob und unter welchen Voraussetzungen Personalstellen die ihnen von der Gauck-Behörde übersandten Unterlagen dem *Sächsischen Landesbeauftragten für die Stasi-Unterlagen* zur Stellungnahme weiterleiten dürfen. Dies richtet sich zunächst nach der spezialgesetzlichen Regelung des § 3 LBStUG, der als Aufgaben und Befugnisse des "Landesbeauftragten" unter anderem nennt: Unterstützung des Bundesbeauftragten (Gauck), Beratung der Anspruchsberechtigten (auch Täter), Information und Beratung öffentlicher Stellen

(z. B. Personalstellen). Abs. 4 lautet: "Der Landesbeauftragte darf die zur Erfüllung seiner Aufgaben erforderlichen personenbezogenen Daten nach Maßgabe des StUG verarbeiten." Folglich besteht eine gesetzliche Befugnis des Landesbeauftragten zum Umgang mit Mitteilungen und Anlagen der Gauck-Behörde. Da der Landesbeauftragte die Pflicht zur Beratung hat, muß er - jedenfalls immer dann, wenn er von der Gauck-Behörde, von einer Personalstelle oder vom Beschäftigten darum ersucht wird - an der Personalentscheidung "*mitwirken*", wie dies in § 121 Abs. 1 S. 2 2. Fall SächsBG als Voraussetzung für eine Datenübermittlung genannt ist.

Wegen des oben begründeten Gebotes der Gleichbehandlung und weil das Sächsische Datenschutzgesetz zum selben Ergebnis führt, gilt das gleiche für Angestellte und Arbeiter. Da § 121 Abs. 1 SächsBG vom "gleichen Dienstherrn" spricht, kommt diese Vorschrift nur für die öffentlich Bediensteten des Freistaates selbst in Betracht. Bei Kommunalbediensteten und Bediensteten anderer öffentlich-rechtlicher Körperschaften ist die Problematik nur über §§ 13, 31 Abs. 1 SächsDSG zu lösen. Ich halte die Datenübermittlung an den Landesbeauftragten für erforderlich und damit für zulässig. Ich habe zunächst eine andere - restriktive - Auffassung vertreten, konnte mich aber den guten Argumenten des Landesbeauftragten und des SMJus als seiner Rechtsaufsichtsbehörde nicht verschließen.
Es ist ja auch zu berücksichtigen, daß der Landesbeauftragte sich auf die spezialgesetzliche Grundlage des StUG (§ 37 Abs. 1 Nr. 7, § 38 Abs. 1) und des LBStUG (§ 3 Abs. 4) stützt und Unterlagen interpretiert, die von der Gauck-Behörde stammen.

Andere Teile der Personalakte sind für eine umfassende und richtige Beratung nach bisheriger Erfahrung des Landesbeauftragten nicht erforderlich und sind daher dem Landesbeauftragten *nicht* zugänglich. Sollte die Erforderlichkeit (im Sinne des § 13 SächsDSG) in begründeten Ausnahmefällen bejaht werden, so müßte zunächst - entsprechend dem Grundsatz der Verhältnismäßigkeit - die Einwilligung des Beschäftigten eingeholt oder eine anonyme Sachbehandlung versucht werden.

Bei der Beurteilung der "Systemnähe" ehemaliger Funktionäre (z. B. ehemalige Nomenklaturkader im öffentlichen Dienst, Anerkennung von Vordienstzeiten) stellt sich dasselbe Problem. Ich neige zu der Auffassung, daß auch frühere Kaderakten, die Aufschluß zur Systemnähe geben können, Teile der heutigen Personalakte sind. Ich werde mich bemühen, dazu eine einheitliche Auffassung der Ressorts herbeizuführen.

Für seine freundliche Zusammenarbeit möchte ich dem Landesbeauftragten und seinen Mitarbeitern danken.

5.1.4 Aufbewahrungsfrist für Unterlagen der Personalkommissionen der Hoch-schulen

Mehrere Universitäten haben die Frage nach der Aufbewahrungsfrist für die in den Personal- und den Fachkommissionen entstandenen Unterlagen gestellt.

Zur Aufbewahrungsdauer von Personalunterlagen, die im Zusammenhang mit der Überprüfung des Hochschulpersonals nach dem Sächsischen

Hochschulerneuerungsgesetz entstanden sind, habe ich die Auffassung vertreten, daß sie sich nach der für die Aufbewahrung der Personalakten geltenden Frist richtet, da diese Unterlagen Bestandteil der Personalakte sind (zu den Fristen im einzelnen vorstehend unter 5.1.2). Denn entscheidend für die Zuordnung zur Personalakte ist, daß die Unterlagen in einem inneren unmittelbaren Zusammenhang mit dem Dienstverhältnis stehen (materielle Personalakte). Nach der Rechtsprechung (BVerwG RDV 1991, 251; BVerwG NJW 1963, 123; BVerwG NVwZ 1984, 445) erfüllen diese Voraussetzung auch behördeninterne Vorgänge, die eine das Dienstverhältnis betreffende Entscheidung vorbereitet haben. Unerheblich ist, ob sich die Unterlagen tatsächlich in der Personalakte befinden (formelle Personalakte) oder gesondert aufbewahrt werden.

5.1.5 Anhörungsverfahren zur Personalüberprüfung im öffentlichen Dienst; Einsichtnahme in die Personalakte nach Beendigung des Arbeitsverhältnisses

Ein Petent hat mir die Umstände mitgeteilt, die zur Auflösung seines Arbeitsverhältnisses geführt haben, und um Auskunft über sein Recht auf Einsicht in die Personalakte nach Beendigung des Arbeitsverhältnisses gebeten. Der Sachverhalt war folgender:

Im Frühjahr 1993 hatte der Petent, Bedientsteter einer Stadt, eine Vorladung zum Oberbürgermeister für den nächsten Tag erhalten, ohne daß ihm ein Grund genannt worden wäre. Bei Wahrnehmung des Termins war er einer Personalkommission gegenübergestellt worden, die ihm nicht sämtliche von der Gauck-Behörde eingegangenen Unterlagen vorlegte, sondern nur vier von ihm unterschriebene Dokumente aus seiner Armeezeit vor etwa 20 Jahren. Wieder einen Tag später war ihm ein Schreiben übergeben worden, wonach der Stadt unter Hinweis auf den Einigungsvertrag eine Fortsetzung des Arbeitsverhältnisses nicht zuzumuten sei; er solle sich am nächsten Tag im Personalbüro melden. Dort war er dann vor die Wahl gestellt worden, die bereits ausgefertigte außerordentliche Kündigung zu erhalten oder einen Auflösungsvertrag abzuschließen. Der Petent hatte daraufhin den ihm angebotenen Auflösungsvertrag unterzeichnet, ohne sich der vollen Tragweite dieses Schrittes bewußt gewesen zu sein.

Die Stadt hat mir in ihrer Stellungnahme mitgeteilt, daß die Anhörung nach den in einer innerdienstlichen Anweisung zur Durchführung von Personalüberprüfungen festgelegten Verfahrensgrundsätzen erfolgt sei. Die von mir daraufhin überprüfte Anweisung war im wesentlichen nicht zu beanstanden. Ich habe jedoch die Einschränkung des rechtlichen Gehörs (Rechtsstaatsprinzip - Art. 20 Abs. 3 GG) bemängelt, weil dem Betroffenen keine angemessene Frist zur Äußerung eingeräumt und er über den Grund einer Vorladung nicht ausreichend informiert wurde. Denn rechtliches Gehör bedeutet angemessene Gelegenheit zur Stellungnahme. Deshalb ist dem Betroffenen stets mitzuteilen, in welcher Angelegenheit und zu welchem Vorwurf er gehört werden soll. Zur Vorbereitung ist ihm eine angemessene Frist einzuräumen, die mit nur einem Tag zu kurz bemessen ist.

Zudem habe ich angeregt, in Anlehnung an § 28 VwVfG dem Betroffenen nach einer Anhörung die Kündigungsabsicht einschließlich der für die Entscheidung erheblichen

Tatsachen mitzuteilen und - bei Vorliegen der betreffenden Voraussetzungen - wahlweise den Abschluß eines Auflösungsvertrages als Alternative anzubieten. Dies gibt nicht nur dem Betroffenen Gelegenheit, sein weiteres Vorgehen zu überlegen und ggf. einen Bevollmächtigten mit seiner Vertretung zu beauftragen, sondern trägt auch dazu bei, arbeitsgerichtliche Verfahren zu vermeiden.

Zum Recht auf Einsicht in die Personalakte habe ich dem Petenten und der Stadt mitgeteilt, daß auch nach Beendigung des Arbeitsverhältnisses ein unbeschränktes Akteneinsichtsrecht besteht. Die von der Gauck-Behörde übersandte Mitteilung und alle im Zusammenhang mit dem Überprüfungsverfahren entstandenen Unterlagen dürfen als materieller Bestandteil der Personalakte eingesehen werden.

Dem Urteil des Bundesarbeitsgericht vom 8. April 1992 (RDV 1993, 171) zu § 13 BAT vermag ich nicht zu folgen. Denn danach haben Arbeiter und Angestellte - im Gegensatz zu Beamten - nur während des Arbeitsverhältnisses ein Akteneinsichtsrecht. Diese Auslegung von § 13 BAT steht weder im Einklang mit dem Gleichbehandlungsgrundsatz noch mit dem Urteil des Bundesverfassungsgericht zum informationellen Selbstbestimmungsrecht.

5.1.6 Aktualisierung von Personalakten der Lehrer

Für Unruhe in der Lehrerschaft sorgte die vom SMK angeordnete Aktualisierung der Personalakten. Diese war erforderlich geworden, weil aufgrund des sogenannten "Modrow-Erlasses" seinerzeit zahlreiche Lehrer selbst oder die damalige personalführende DDR-Stelle aus Personalakten auch Unterlagen entfernt hatten, die notwendiger Bestandteil einer Personalakte sind. Im Zuge der Aktualisierung haben sich mehrfach Lehrer und Personalräte an mich gewandt, weil sie bezweifelten, daß einige der von den Oberschulämtern und staatlichen Schulämtern angeforderten Unterlagen zu den Personalakten genommen werden dürften. Außerdem richteten sich die Bedenken dagegen, daß die Unterlagen in mehrfacher Ausfertigung vorzulegen und zuvor vom Schulleiter zu beglaubigen waren.

Ich konnte mich dieser Skepsis nicht verschließen und habe empfohlen, bis zu einer Klärung mit dem SMK vorerst nur solche Unterlagen zu den Personalakten zu geben, die zweifelsfrei erforderlich sind.

Es hat sich herausgestellt, daß die Schulämter von den Vorgaben des SMK abgewichen sind und die Erforderlichkeit der Unterlagen nach eigenen - nicht immer datenschutzrechtlichen - Kriterien bestimmt haben. So nahmen beispielsweise einige Schulämter Kopien von Personalausweisen zur Akte (als Nachweis der Staatsangehörigkeit!), andere vollständige Kopien von Scheidungsurteilen (nach Beglaubigung durch den Schulleiter oder dessen Sekretärin). Das SMK selbst hatte in seiner Vorgabe überhaupt keine Scheidungsunterlagen vorgesehen.

Da das SMK das Verfahren nicht vorher mit mir abgestimmt hatte, habe ich im nachhinein feststellen müssen, daß die ungenaue, nicht sach- und datenschutzgerechte Vorgabe des SMK mitursächlich für die eingetretene Verunsicherung war. Ich habe dem SMK meine Bedenken im einzelnen vorgetragen und angeregt, die Aktualisierung

zunächst zurückzustellen oder sich vorerst an dem Entwurf der Verwaltungsvorschrift des SMI zur Führung und Verwaltung von Personalakten zu orientieren, der damals bereits vorlag.

Da das SMK vor Inkrafttreten dieser Verwaltungsvorschrift dazu keine Veranlassung sah, bleibt die Reaktion des SMK auf die nunmehr am 17. Dezember 1993 in Kraft getretene Verwaltungsvorschrift abzuwarten. Ich werde mich mit Nachdruck für eine korrekte Personalaktenführung einsetzen und dies kontrollieren.

5.1.7 Belegverkehr zwischen Personalstellen und Landesamt für Finanzen (LfF)

Die Festsetzung, Abrechnung und Zahlbarmachung der Vergütungen und Bezüge für die Arbeiter, Angestellten, Beamten, Richter und Staatsanwälte des Landes wird zentral vom LfF vorgenommen. Zur Erfüllung dieser Aufgabe ist es auf die Mitteilung bezügerelevanter Daten durch die personalverwaltenden Stellen angewiesen. Sowohl Petenten als auch Personalstellen haben nachhaltig um Klärung gebeten, welche Unterlagen, Angaben oder Daten das LfF tatsächlich benötigt.

Das SMF hat mir im Berichtszeitraum ein umfangreiches Gesamtkonzept für ein Verfahren zum Daten- und Belegverkehr zwischen personalverwaltenden Stellen und den Bezügestellen des LfF zur datenschutzrechtlichen Prüfung vorgelegt. Das Konzept erfaßt vorerst den Tarifbereich, da die Zahl der Arbeiter und Angestellten die der Beamten weit überwiegt. Das Ziel, nicht nur ein landesweit einheitliches Verfahren im Interesse einer ordnungsgemäßen Festsetzung und Auszahlung der Vergütungen zu schaffen, sondern das Verfahren auch datenschutzgerecht zu gestalten, konnte in einer erfreulichen Zusammenarbeit erreicht werden. 1994 soll mir ein entsprechendes Konzept für die Beamten- und Richterbesoldung vorgelegt werden.

Ausgehend von den Aufgaben des LfF erfaßt das Konzept die bezügerelevanten Vorgänge. Sie sind in einer Arbeitsanleitung für die Personalstellen zusammengestellt, aus der sich in übersichtlicher Form ergibt, welche Unterlagen in welchen Fällen dem LfF vorzulegen und welche Formblätter zu verwenden sind. Dadurch wird vermieden, daß Personalstellen Unterlagen weitergeben oder Daten mitteilen, die für die Bezügestellen im LfF nicht erforderlich sind.

In der Arbeitsanleitung wurden auch alle Unterlagen gekennzeichnet, die der Betroffene dem LfF entweder direkt oder im verschlossenen Umschlag über die Dienst- bzw. Personalstelle zuleiten kann (z. B. Geburts-, Sterbe- und Heiratsurkunden, Lohnsteuerkarten, Anträge auf Zahlung von Kindergeld, Erklärungen zum Ortszuschlag, Tenor des Scheidungsurteils, Anträge auf unverzinsliche Gehaltsvorschüsse). Ich habe darauf hingewiesen, daß die Beschäftigten über diese Möglichkeit informiert werden müssen und daß die Personalstellen - falls der Beschäftigte die Unterlagen dem LfF *unverschlossen* über die Personalstelle zuleitet - keine Kopien für die dort vorhandenen Personalakten fertigen dürfen, da diese Unterlagen ausschließlich Bestandteil der vom LfF geführten *Vergütungsakte* (Teilakte der Personalakte, jedoch nicht Teil der Grundakte) sind.

In der Vergangenheit war umstritten, ob das LfF den Abdruck eines Kündigungsschreibens oder Auflösungsvertrages erhalten darf oder nur eine "Kurzmitteilung" mit dem Enddatum des Arbeitsverhältnisses. Da die Gewährung und zutreffende Festsetzung von Abfindungen bzw. die Zahlung von Übergangsgeldern einschließlich der exakten Zeitraumbestimmung Aufgabe des LfF ist und in die Entscheidung auch die für die Beendigung des Arbeitsverhältnisses maßgebenden Gründe einzubeziehen sind, habe ich keine Einwendungen, wenn das LfF in diesen Fällen die vollständigen Unterlagen erhält. Insoweit habe ich meine Auffassung (gegenüber Abschnitt 5.1.10 meines 1. Tätigkeitsberichts) geändert.

5.1.8 Beihilfebearbeitung im Landesamt für Finanzen

Dem Landesamt für Finanzen (LfF) ist neben anderen Aufgaben auch die Bearbeitung der Beihilfeangelegenheiten und der Unfallfürsorge für die Landesbeamten, Richter und Staatsanwälte Sachsens übertragen worden. Es unterhält sowohl in Dresden als auch in den Außenstellen Chemnitz und Leipzig Beihilfestellen. Die in § 118 Abs 1 Satz 2 SächsBG geforderte organisatorische Trennung der Beihilfebearbeitung von der übrigen Personalverwaltung ist damit gewährleistet.

Im Berichtszeitraum habe ich mich über die Beihilfebearbeitung im LfF Dresden informiert und das Landesamt bei dieser Gelegenheit in datenschutzrechtlichen Fragen beraten. Erfreulich war die Aufgeschlossenheit des SMF und des LfF für datenschutzrechtliche Belange.

Als nicht datenschutzgerecht habe ich insbesondere folgendes angesehen:

Posteingang / Postausgang
Die Antragsteller senden ihre Beihilfeanträge unmittelbar an das LfF bzw. die örtlich zuständige Außenstelle. Ich habe bemängelt, daß die Briefumschläge der eingehenden Beihilfeanträge, denen Arztrechnungen mit Diagnosedaten, Rezepte usw. beiliegen, in der zentralen Poststelle generell geöffnet werden - also auch dann, wenn sie den Zusatz "Beihilfestelle" tragen. Dies ist inzwischen geändert worden. Für die Beihilfepost wurde eine eigene Poststelle eingerichtet. Außerdem weist das LfF die Antragsteller durch Merkblätter darauf hin, daß Beihilfepost an die Beihilfestelle zu adressieren ist. Leider konnte mein Vorschlag, für Beihilfeanträge jeweils ein bedrucktes (nicht frankiertes) Kuvert für die Rücksendung zur Verfügung zu stellen, angeblich aus Kostengründen nicht verwirklicht werden.

Beihilfebearbeitung für Angehörige des LfF in herausgehobener Position sowie des Personals der Beihilfestellen
Ich habe auf die Problematik hingewiesen, die sich aus der Beihilfebearbeitung für die Angehörigen des LfF in herausgehobener Position (z. B. Präsident, Abteilungsleiter) sowie für das Personal der Beihilfestellen ergibt.

Die Anträge dieses Personenkreises sollten auf Wunsch in einer Beihilfestelle des LfF bearbeitet werden, die nicht zugleich Beschäftigungsstelle des Beihilfeberechtigten ist.

Besoldungsdaten für die Beihilfestelle
Als Arbeitsunterlage erhält jede Beihilfestelle eine *monatlich* aktualisierte Namensliste aller Beamten zur Feststellung der Beihilfeberechtigung. Diese Listen enthielten auch die für die Beihilfebearbeitung nicht benötigte Besoldungsgruppe. Auf deren Ausdruck ist inzwischen verzichtet worden.

Belege zum Beihilfeantrag
Als Belege werden neben den Originalen auch Rechnungszweit- und Rechnungsdurchschriften anerkannt. Bei Rezepten reicht eine Fotokopie mit Originalstempel der Apotheke. Damit entfällt für Sachsen das Problem anderer Bundesländer, in denen die Beihilfestellen nur *beglaubigte* Zweitschriften oder Kopien anerkennen, mit der Folge, daß die Beglaubigungen von dazu befugten Amtsangehörigen - zumeist Kollegen des beihilfeberechtigten Antragstellers - vorgenommen werden, die dadurch zwangsläufig von den Diagnosedaten des Beihilfeberechtigten und dessen Familienangehörigen Kenntnis erhalten.

Die eingereichten Belege werden auch nicht für die Beihilfeakte kopiert. Ferner sind aus den in den Akten vorhandenen Zusammenstellungen über die geltend gemachten Aufwendungen keine Rückschlüsse auf den behandelnden Arzt oder die Art der Erkrankung möglich.

Anträge von Angehörigen des Beihilfeberechtigten
Obwohl die Angehörigen eines Beamten gesetzlich kein eigenes Antragsrecht haben (entsprechende Initiativen anderer Datenschutzbeauftragter waren erfolglos), haben SMF und LfF versichert, Problemfälle (z. B. bei getrennt lebenden Ehegatten) pragmatisch zu lösen. Ich finde das gut und werde die Handhabung beobachten.

5.1.9 Beihilfebearbeitung durch den Kommunalen Versorgungsverband Sachsen (KVS)

Die Beihilfegewährung für die Beamten der Gemeinden, Landkreise, Zweckverbände und anderer Körperschaften erfolgt nach dem *Gesetz über den Kommunalen Versorgungsverband Sachsen (SächsGKV)* durch den KVS. Nach sächsischem Datenschutzrecht ist der KVS insoweit eine sächsische öffentliche Stelle, die die Beihilfeakten als Teilakten der Personalakten der Beamten führt. Diese Aufgabe nimmt der KVS mit eigenen Bediensteten derzeit in den Räumen des Kommunalen Versorgungsverbandes Baden-Württemberg in Karlsruhe wahr - datenschutzrechtlich eine nicht unproblematische Organisationsform, auch wenn sie nur für eine Übergangszeit vorgesehen ist.

Der KVS hat mir auf Rückfrage versichert, es sei organisatorisch sichergestellt, daß die Beihilfeanträge der sächsischen Beamten nur durch die Sachbearbeiter des KVS bearbeitet und gesondert aufbewahrt würden. Diese Abschottung muß auch bei aufsichts-, revisions- und datenschutzrechtlichen Überprüfungen gewährleistet bleiben. Ich habe die Datenschutzbeauftragte des Landes Baden-Württemberg entsprechend unterrichtet.

Das Verfahren zur Beantragung der Beihilfe weist noch erhebliche datenschutzrechtliche Mängel auf: So wird der Betroffene aufgefordert, jeden Beihilfeantrag samt Rechnungen (ob verschlossen oder unverschlossen, wird nicht angegeben) in der Personalverwaltung

abzugeben, von wo aus die Unterlagen nach Überprüfung der Personalangaben an den KVS weitergeleitet werden. Die im Sächsischen Beamtengesetz (§ 118) geforderte Abschottung der Beihilfebearbeitung von der übrigen Personalverwaltung wird damit nicht erreicht. Es ist nicht ausgeschlossen, daß Mitarbeiter in der Personalstelle auf diese Weise Kenntnis von den Gesundheitsdaten des Antragstellers und seiner Familienangehörigen erhalten. Auch erhält die Personalstelle davon Kenntnis, wie häufig ein Bediensteter Beihilfeanträge stellt, auch wenn die Belege in verschlossenem Umschlag dem Antrag beigefügt werden. Denn bei jedem Antrag sind alle persönlichen Angaben zu wiederholen und erneut von der Personalstelle zu bestätigen.

Ich werde darauf hinwirken, daß auch der KVS das vom SMF für die Beihilfeangelegenheiten der Staatsbediensteten vorgeschriebene Antragsformular (vgl. SächsABl. 1993, Sonderdruck Nr. 4) verwendet. Dieses ist datenschutzgerecht gestaltet und läßt nach der Bearbeitung keine Rückschlüsse auf die Art der Erkrankung zu. Dagegen sind im Antragsformular des KVS der Name des behandelnden Arztes, der Name des Krankenhauses einschließlich Dauer des stationären Krankenhausaufenthalts und die Art der Behandlung (Strahlenbehandlung, Zahnbehandlung) anzugeben, so daß entgegen § 123 Abs. 2 SächsBG auch nach Rücksendung der Belege die Art der Erkrankung erkennbar bleibt, insbesondere dann, wenn die Behandlung durch Fachärzte oder Spezialkliniken erfolgte.
Der KVS begründet die Erforderlichkeit dieser Angaben damit, daß er erkennen müsse, ob Belege doppelt eingereicht worden seien. Auch wenn die Belege vor der Rücksendung als "für Beihilfezwecke verwendet" gekennzeichnet wurden, sei nicht ausgeschlossen, daß dieselben Aufwendungen erneut geltend gemacht würden; denn es würden auch Kopien, Duplikate und Abschriften von Rechnungen und Rezepten anerkannt.
Ich bin der Auffassung, daß bereits anhand von Datum und Rechnungsbetrag mögliche Doppelanträge erkannt werden können und das Problem eher theoretischer Natur ist, denn anderen Beihilfestellen (z. B. dem Sächsischen Landesamt für Finanzen) genügen diese Angaben. Außerdem ist erfahrungsgemäß nicht davon auszugehen, daß die Antragsteller potentielle Leistungsbetrüger sind.

Der KVS hat zugesagt, die Beihilfeberechtigten künftig darüber aufzuklären, daß sie (entsprechend der Satzung des KVS) Anträge auch direkt beim KVS einreichen können. Außerdem sollen die Antragsvordrucke überarbeitet werden.

Ich werde die Angelegenheit weiterverfolgen.

5.1.10 Kontrolle der Personalstelle einer Stadtverwaltung aufgrund anonymer Eingabe

Einer telefonischen, durchaus sachkundig und plausibel erscheinenden, jedoch anonymen Mitteilung zufolge würden die Personalakten der Beschäftigten unverschlossen und damit für sämtliche Mitarbeiter zugänglich in der Personalstelle der Stadtverwaltung eines sächsischen Fremdenverkehrsortes aufbewahrt. Erfolglos versicherte ich dem Petenten am Telefon, daß für "seine Verschwiegenheit mir gegenüber" kein Grund bestehe, da ich bei datenschutzrechtlichen Ermittlungen (Aufforderung an Behörden zur Stellungnahme, Kontrollbesuche etc.) Namen und Anschrift der Petenten *ohne Einverständnis nicht offenbaren* würde. Gemäß § 23 Abs. 6 SächsDSG bin ich

nämlich zur Verschwiegenheit hinsichtlich der bei meiner Tätigkeit bekanntgewordenen Daten verpflichtet. Der Anrufer machte einen verängstigten Eindruck.

Trotzdem habe ich aufgrund des Hinweises eine datenschutzrechtliche Kontrolle bei der Stadtverwaltung durchgeführt. Der Sächsische Datenschutzbeauftragte ist nämlich nach Art. 57 SächsVerf "zur Wahrung des Rechts auf Datenschutz berufen" und hat gemäß § 24 SächsDSG bei den sächsischen öffentlichen Stellen die Einhaltung datenschutzrechtlicher Vorschriften zu kontrollieren. Anders als beispielsweise ein Rechtsanwalt bin ich bei meiner Tätigkeit also nicht an einen Auftrag eines Petenten gebunden, sondern ich habe auch *von Amts wegen* Datenschutzverstöße zu ermitteln und darauf hinzuwirken, daß eine datenschutzgerechte Datenverarbeitung stattfindet. Dies bedeutet, daß ich auch anonymen Hinweisen - sofern die Ernstlichkeit dieser Hinweise nicht angezweifelt werden muß - nachzugehen habe, wenn sie plausibel sind.

Der anonyme Vorwurf erwies sich allerdings - ich hatte es anders erwartet - nicht als gerechtfertigt. Die Kontrolle ergab, daß die Mitarbeiter der Stadtverwaltung gegenüber den Belangen des Datenschutzes aufgeschlossen waren und die datenschutzrechtlichen Vorschriften (z. B. Sächsisches Beamtengesetz, Sächsisches Meldegesetz, Sächsisches Datenschutzgesetz) beachten. Aber vielleicht wollte der kluge Anrufer auch nur, daß eine Prüfung mit gutem Ergebnis erfolgte.

Meinen gesetzlichen Auftrag nehme ich ernst. Ich werde jedoch in Zukunft bei anonymen Eingaben die Ernstlichkeit der Hinweise *besonders prüfen* und bei den "angeschwärzten" öffentlichen Stellen den Sachverhalt mit Zurückhaltung ermitteln. Meine Dienststelle darf keine "Anlaufstelle für Denunzianten" werden, die unter dem Deckmantel der Anonymität öffentlichen Stellen völlig aus der Luft gegriffene Datenschutzverstöße vorwerfen.

5.1.11 Meldungen gem. § 31 Abs. 7 SächsDSG zur automatisierten Verarbeitung von Beschäftigtendaten

Gem. § 31 Abs. 7 SächsDSG darf eine automatisierte Verarbeitung von Beschäftigtendaten durch öffentliche Stellen in Sachsen nur im Benehmen mit dem Sächsischen Datenschutzbeauftragten eingeführt, angewendet, geändert oder erweitert werden.

Da mir im Berichtszeitraum einige Hundert dieser Systeme gemeldet worden sind (einschließlich Verfahrens- und Datensatzbeschreibungen, Anwenderhandbüchern und ggf. Dienstvereinbarungen), war es mir nicht in jedem Fall möglich, zeitnah die erbetenen Stellungnahmen abzugeben. War ich anfangs von einer überschaubaren Anzahl der eingesetzten Systeme ausgegangen, mußte ich bald feststellen, daß kaum ein System dem anderen gleicht, zumal außer gekaufter Software auch Eigenentwicklungen eingesetzt werden, insbesondere bei Personalinformationssystemen. Selbst bei identischen Systemen war die Anwendung unterschiedlich, weil die öffentlichen Stellen die Möglichkeiten desselben Systems unterschiedlich nutzten.

Den vorliegenden Meldungen zufolge werden Beschäftigtendaten im wesentlichen automatisiert verarbeitet durch

- ISDN-Telekommunikationsanlagen,
- Personalinformations-, Stellenverwaltungs- bzw. Stellenbewirtschaftungssysteme,
- elektronische Arbeitszeiterfassung,
- EDV-gestützte Lohn- und Gehaltsabrechnung,
- EDV-gestützte Wohnungsfürsorge,
- EDV-gestützte Verwaltung von Reisekosten- und Umzugskostenangelegenheiten.

Sobald automatisierte Verfahren nicht der reinen Personalverwaltung dienten, haben sich Probleme ergeben. So war zweifelhaft, ob auch der Einsatz automatisierter Systeme zur Unterstützung der Tätigkeit der Beschäftigten (z. B. Textverarbeitung, automatisierte Abrufverfahren, Nutzung automatisierter Dateien), bei dem ja zwangsläufig Beschäftigtendaten (mindestens für die Zugangsberechtigung und Zugriffskontrolle) gespeichert werden - also die *sachbezogene* Speicherung von Beschäftigtendaten -, meldepflichtig sei. Ebenso zweifelhaft war, ob die zu Organisationszwecken gespeicherten Beschäftigtendaten (z. B. Registrierung von Schlüsselausgaben bzw. ausgegebener Code-Karten für die Zugangskontrolle, Bibliotheksausleihen) gemeldet werden müßten.

Ich habe mir dazu folgende Auffassung gebildet:

Gem. § 31 Abs. 1 SächsDSG darf eine öffentliche Stelle die Daten der Beschäftigten nur verarbeiten, soweit dies zur Eingehung, Durchführung oder Beendigung des Dienst- oder Arbeits*verhältnisses* erforderlich ist oder ein Gesetz (auch das Sächsische Datenschutzgesetz) bzw. eine Rechtsverordnung, ein Tarifvertrag oder eine Dienstvereinbarung dies vorsehen. Ein *Dienstverhältnis* ist das zwischen einem Beamten und seinem Dienstherrn bestehende öffentlich-rechtliche Dienst- und Treueverhältnis mit den sich daraus ergebenden gegenseitigen Rechten und Pflichten. Ein *Arbeitsverhältnis* ist das zwischen einem sonstigen Arbeitnehmer und der öffentlichen Stelle bestehende Rechtsverhältnis, dessen Grundlage der Arbeitsvertrag, Tarifverträge und die sonstigen arbeitsrechtlichen Vorschriften bilden.

Ob Beschäftigtendaten zur Eingehung, Durchführung oder Beendigung des Dienstverhältnisses verarbeitet werden, läßt sich deshalb nur anhand des *Verarbeitungszwecks* entscheiden:

Werden die Daten im Rahmen der (klassischen) Personalverwaltung verarbeitet, besteht immer der Zusammenhang mit dem Dienst- oder Arbeitsverhältnis. Werden sie jedoch bei der dem Beschäftigten übertragenen Aufgabe oder im Rahmen EDV-gestützter Organisationsmaßnahmen verarbeitet - also sachbezogen -, geschieht dies *nicht* zur Durchführung des Dienst*verhältnisses*, sondern des Dienstes selbst. Erst wenn die Datenverarbeitung mit der Zielrichtung durchgeführt wird, Aufschlüsse über das Verhalten oder die Leistung des Beschäftigten zu erhalten oder den Beschäftigten - nicht aber den bearbeiteten Vorgang - zu kontrollieren, handelt es sich um die Verarbeitung von Personaldaten zur Durchführung des Dienstverhältnisses, mit der Folge, daß sich die betreffende öffentliche Stelle nach § 31 Abs. 7 SächsDSG mit mir ins Benehmen zu setzen hat.

Die Frage, ob gespeicherte Daten für eine Leistungs- und Verhaltenskontrolle geeignet sind, berührt die Mitbestimmung der Personalvertretung. Ob und ggf. in welchem Umfang und unter welchen Voraussetzungen sie auch für eine Leistungs- und Verhaltenskontrolle genutzt werden dürfen, bestimmt die Dienstvereinbarung. Erlaubt sie nicht, daß die Daten für eine Verhaltens- und Leistungskontrolle des Beschäftigten genutzt werden, ist die Verarbeitung insoweit gemäß § 31 Abs. 1 SächsDSG unzulässig.

Daraus folgt, daß sach- oder organisationsbezogene EDV-Verfahren wie z. B. *Textverarbeitungssysteme* nur dann anzuzeigen sind, wenn sie tatsächlich für eine Leistungs- und Verhaltenskontrolle des Verfassers bzw. der Schreibkraft *genutzt* werden (wer hat wieviel und wie gut geschrieben?).

Für *Zugangskontrollsysteme* gilt, daß sie mir anzuzeigen sind, wenn die aufgezeichneten Beschäftigtendaten nicht nur unter Sicherheitsgesichtspunkten, sondern (auch) zur Verhaltens- oder Leistungskontrolle der Beschäftigten ausgewertet werden. Beschäftigtendaten, die für Zwecke der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebs einer Datenverarbeitungsanlage gespeichert wurden, dürfen gem. § 12 Abs. 4 SächsDSG nicht für eine Leístungs- und Verhaltenskontrolle verwendet werden.

Ich beabsichtige, die sich zu § 31 SächsDSG stellenden Fragen demnächst in einer Bekanntmachung darzustellen und zu klären.

5.1.12 Zum Begriff "Dienstvereinbarung" im Sinne von § 31 Abs. 1 SächsDSG

Gemäß § 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. Im Berichtszeitraum wurden mir häufig mit "Dienstvereinbarung" überschriebene Absprachen zwischen Dienststellen und Personalräten mit der Bitte um datenschutzrechtliche Bewertung zugesandt. Ich hatte daher vor allem zu klären, wie diese "Dienstvereinbarungen" grundsätzlich datenschutzrechtlich einzuordnen sind.

Dienstvereinbarungen werden definiert als allgemeine, das Dienstverhältnis der Beschäftigten betreffende Regelungen durch Übereinkunft zwischen Dienststellenleiter und Personalrat. Denkbar sind solche Vereinbarungen in vielen Bereichen (z. B. Vereinbarung über Datensicherungsmaßnahmen). Mit dem Begriff "Dienstvereinbarung" in § 31 Abs. 1 SächsDSG sind allerdings nur Dienstvereinbarungen gemeint, welche die in §§ 80 Abs. 3, 81 Abs. 3 SächsPersVG abschließend aufgeführten Regelungstatbestände betreffen (z. B. Einführung technischer Einrichtungen zur Leistungskontrolle der Beschäftigten). Dies ergibt sich daraus, daß gemäß § 4 Abs. 1 Nr. 1 SächsDSG eine Datenverarbeitung ohne Einwilligung des Betroffenen nur zulässig ist, soweit sie durch das Datenschutzgesetz selbst oder eine andere *Rechtsvorschrift* erlaubt ist. Nur Dienstvereinbarungen aufgrund der oben genannten Vorschriften des Sächsischen Personalvertretungsgesetzes haben nämlich die Qualität von Rechtsvorschriften. Diese gehen als Spezialvorschriften dem allgemeinen Sächsischen Datenschutzgesetz vor (vgl. § 2 Abs. 4 SächsDSG), müssen aber die für alle

verbindlichen (§ 31 BVerfGG) tragenden Gründe der verfassungsgerichtlichen Rechtsprechung und die Verfassung beachten.

Hieraus ergeben sich für die datenschutzrechtliche Bewertung folgende Konsequenzen:

Werden mir Dienstvereinbarungen i. S. v. § 31 Abs. 1 SächsDSG (also Rechtsvorschriften) mit der Bitte um datenschutzrechtliche Stellungnahme zugesandt, habe ich die darin enthaltenen Regelungen auf Vereinbarkeit mit Art. 33 SächsVerf (Recht auf informationelle Selbstbestimmung), konkretisiert durch das Volkszählungsurteil (BVerfGE 65, 1 ff.) zu prüfen. Dienstvereinbarungen mit Rechtsnormqualität müssen nämlich - wie jede Rechtsvorschrift - mit der Verfassung in Einklang stehen. Die Kernsätze der zitierten Entscheidung habe ich bereits in meinem 1. Tätigkeitsbericht (1.1.2) dargestellt und erläutert.

Dienstvereinbarungen außerhalb der Regelungstatbestände des Sächsischen Personalvertretungsgesetzes habe ich demgegenüber unmittelbar an den Vorschriften des Sächsischen Datenschutzgesetzes zu messen. Insbesondere ist zu fragen, ob gegebenenfalls getroffene Vereinbarungen über die Verarbeitung von Beschäftigtendaten zur Eingehung, Durchführung oder Beendigung des Dienst- oder Arbeitsverhältnisses erforderlich sind (vgl. § 31 Abs. 1 S. 1 Fall 1 SächsDSG).

Wegen der unterschiedlichen Qualität von "Dienstvereinbarungen" sollten die öffentlichen Stellen diejenigen Übereinkünfte, die *nicht* unter §§ 80 Abs. 3, 81 Abs. 3 SächsPersVG fallen, nicht als "Dienstvereinbarungen", sondern z. B. als "*Dienstabsprachen*" bezeichnen.

5.1.13 Personaldatenverarbeitung für Lehramtsbewerber

Mit der Meldung zur Ersten Staatsprüfung für das Lehramt beginnen die Prüfungsämter, die Daten der Betroffenen zu speichern. Im Zuge der weiteren Ausbildung (Vorbereitungsdienst/Referendariat, Zweite Staatsprüfung) werden die Daten ergänzt, so daß sich nach der Zweiten Staatsprüfung alle Einzelheiten der Ausbildung anhand der Daten nachvollziehen lassen. So werden die nach der Prüfungsordnung geforderten Voraussetzungen, wie beispielsweise Nachweise in Sprachkenntnissen, Bescheinigungen über Schulpraktika, Teilnahme an den vorgeschriebenen Kursen, Übungen, Seminaren und Exkursionen sowie sonstige Leistungsnachweise ebenso gespeichert wie die in den einzelnen Prüfungsfächern erzielten Noten.

Das SMK hat mich um eine Stellungnahme zu dem Verfahren gebeten. Der Umfang der gespeicherten Daten entspricht (bis auf das Merkmal "geleisteter Wehr-, Ersatzdienst oder freiwilliges soziales Jahr") dem Erforderlichkeitsgrundsatz und war deshalb im wesentlichen nicht zu beanstanden. Im Hinblick auf die Schutzbedürftigkeit dieser Daten und den großen Personenkreis, den die Dateien erfassen, habe ich die Erstellung eines technisch-organisatorischen Konzepts zur Gewährleistung der Datensicherheit gefordert. Außerdem habe ich es als zwingend angesehen, den zum Vorbereitungsdienst zugelassenen und zu Beamten auf Widerruf ernannten Lehramtsanwärtern gem. § 124 Abs. 5 SächsBG die über sie gespeicherten Daten mitzuteilen und von wesentlichen Änderungen zu unterrichten.

5.1.14 Zeiterfassung mittels Stempelkarte

In vielen Verwaltungen wird die geleistete Arbeitszeit noch im herkömmlichen Stempelkartenverfahren erfaßt. Oftmals sind die Stempelkarten mit dem Namen bzw. einer Personalnummer versehen (personenbezogene Daten). Ebenso häufig befinden sich die Karteikästen an unbeaufsichtigten Stellen im Bereich des Behördeneingangs. Einsicht oder Zugriff Unbefugter sowie eine mißbräuchliche Benutzung ist dann leicht möglich.

Nach § 9 Abs. 1 SächsDSG haben die öffentlichen Stellen unter Berücksichtigung des Verhältnismäßigkeitsgrundsatzes alle personellen, technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um eine datenschutzgerechte Verarbeitung der Zeiterfassungsdaten zu gewährleisten. Insbesondere sind Maßnahmen zu treffen, die geeignet sind,

1. Unbefugten den Zugang zu den Stempelkarten und den Stempelgeräten zu verwehren (§ 9 Abs. 2 Nr. 1 SächsDSG),

2. zu verhindern, daß die Stempelkarten unbefugt gelesen, kopiert, verändert oder entfernt werden können (§ 9 Abs. 2 Nr. 2 SächsDSG),

3. die unbefugte Stempelung sowie die unbefugte Kenntnisnahme oder Löschung (z. B. Vernichtung) gespeicherter Daten zu verhindern (§ 9 Abs. 2 Nr. 3 SächsDSG) und

4. die innere Organisation (z. B. durch Dienstanweisung) so zu gestalten, daß sie den besonderen Anforderungen des Datenschutzes gerecht wird (§ 9 Abs. 2 Nr. 10 SächsDSG).

Oftmals werden nach meinen Erfahrungen die herkömmlichen Zeiterfassungsverfahren vorstehenden Grundsätzen nicht gerecht.
Es liegt sowohl im Interesse der Behörde als auch der Bediensteten, daß behördenfremden Personen der räumliche Zugang zur Stempelkartenanlage versperrt wird (z. B. durch Installation der Stempelkartenanlage in der Pförtnerloge oder an einer Stelle, die ständig unter der Aufsicht des Pförtnerpersonals steht).

Außerdem sollte anstelle des Namens eine Code-Kartennummer treten und geregelt werden, daß es den Bediensteten aus Gründen des Datenschutzes *freigestellt* ist, die Stempelkarte bei sich zu tragen, ein Deponieren der Karte im Karteikasten also *freiwillig* geschieht.

Auf das Erfordernis, auch das Zeiterfassungsverfahren ins Dateien- und Geräteverzeichnis aufzunehmen (siehe § 10 SächsDSG), erlaube ich mir hinzuweisen.

Ersetzt eine öffentliche Stelle ein Stempelkartenverfahren durch ein automatisiertes System, hat sie sich gemäß § 31 Abs. 7 SächsDSG mit dem Sächsischen Datenschutzbeauftragten ins Benehmen zu setzen.

Ich wiederhole mich (1. Tätigkeitsbericht, 5.1.12.3): Eine elektronische Zeiterfassung ist nur in wenigen Behörden (nämlich bei großen, unübersichtlichen Arbeitseinheiten)

erforderlich. Im Hinblick auf die Arbeitsmoral ist sie unzweckmäßig, weil diese zu einer "Arbeitszeit-Moral" degradiert wird. Hinzu kommen mannigfache datenschutzrechtlich problematische Fallgestaltungen, die entweder rechtswidrig gehandhabt werden oder viel Arbeitskraft binden.

5.1.15 Umgang mit Personalakten in Großstädten

Glaubhafte Beschwerden über "alte Strukturen", "Machenschaften" und "Seilschaften" in Personalämtern veranlaßten mich, bei Großstädten im Freistaat den Umgang mit Personalakten zu kontrollieren: Die Personalakten der Beschäftigten werden zu einem großen Teil nicht im Personalamt, sondern in den jeweiligen Fachämtern geführt. Hier sind sog. "Personalsachbearbeiter" oder "Sachbearbeiter für allgemeine Verwaltungsangelegenheiten" beschäftigt, die Zugang zu den Personalakten haben. Sie beraten und betreuen ("Sorge ist Herrschaft") sämtliche Angehörigen der Dienststelle - teilweise "nebenbei" - in Personalangelegenheiten und bereiten Personalentscheidungen vor. Dienstvorgesetzter ist der jeweilige Amtsleiter und nicht der "Personalchef".

Aus datenschutzrechtlicher Sicht habe ich darauf hingewiesen, daß eine solche *dezentrale* Personalaktenführung eine erhebliche Gefahr für das Persönlichkeitsrecht des Einzelnen darstellt, da nur mit großem Aufwand geprüft werden kann, ob mit den Akten datenschutzgerecht umgegangen wird, insbesondere, ob hinreichende Maßnahmen zur Gewährleistung des Datenschutzes (vgl. § 9 SächsDSG) getroffen worden sind und ggf. eingehalten werden. Außerdem dürfen zur Personalakte nur solche Beschäftigten Zugang haben, die im Rahmen der *Personalverwaltung* mit der Bearbeitung von Personalangelegenheiten beauftragt sind. Die Personalverwaltung in Großstädten hat grundsätzlich ausschließlich durch die Personalämter zu erfolgen. Es entspricht einem allgemein anerkannten Grundsatz, alle personellen Aufgaben einer größeren Behörde in einer besonderen organisatorischen Einheit zusammenzufassen (vgl. auch: Empfehlung des Sächsischen Städte- und Gemeindetages vom September 1993). Das auf dem Gebiet des Personalwesens anzuwendende Beamten-, Tarif-, Haushalts- und in Rechtsstreitigkeiten zu beachtende Prozeßrecht sind ausgesprochen schwierige Rechtsgebiete. Die Arbeit im Personalamt erfordert daher regelmäßig ein hohes Maß an Sachkenntnis und Vorbereitung und darf deshalb nicht "nebenbei" in den Fachämtern erledigt werden. Darüber hinaus muß sichergestellt werden, daß die Mitarbeiter einer Behörde in personalrechtlicher Hinsicht *gleich behandelt* werden (der Gleichheitsgrundsatz gilt auch innerhalb einer Behörde). Dies kann nur erreicht werden, wenn die Personalbearbeitung und Personalstellenbewirtschaftung "in einer Hand" liegen. Allerdings bedeutet dies nicht, daß *sämtliche* Personalentscheidungen auch zentral *getroffen* werden müssen. In einem vom Personalamt "vorgegebenen Rahmen" können Bereiche, die nicht das *Grundverhältnis*, sondern die "eigentliche Amtstätigkeit" betreffen (z. B. Regelungen über die Vertretung, Anordnung von Dienstreisen, Genehmigung von Urlaub) weiterhin auf Fachamtsebene entschieden werden.

Im einzelnen habe ich gefordert:

1. Sofortige Überprüfung der "Personalsachbearbeiter" auf eine möglicherweise vorliegende Mitarbeit für das MfS/AfNS der ehemaligen DDR, soweit noch nicht geschehen.

2. Nach Möglichkeit *zentrale Personalaktenführung* im Personalamt.
3. Soweit dies aus Raummangel nicht möglich sein sollte: "Organisatorische Überführung" der "Außenstellen" in den Zuständigkeitsbereich des Personalamtes, damit nicht mehr der jeweilige Amtsleiter, sondern allein das Personalamt für den Umgang mit den Personalakten und für alle das Grundverhältnis betreffende Regelungen verantwortlich ist.

Dies werde ich in nächster Zeit bei den Stadtverwaltungen überprüfen. Gemeinsam mit ihnen soll erarbeitet werden, welche Entscheidungen dem Personalamt vorbehalten werden müssen.

5.1.16 Verleihung des Verdienstordens der Bundesrepublik Deutschland

Vor der Ordensverleihung wird die Ordenswürdigkeit der betreffenden Person geprüft. Zu diesem Zweck erheben die Vorschlagsberechtigten (Ministerpräsidenten der Länder oder Bundesminister) Daten beim Bundeszentralregister, bei der Gauck-Behörde und für Jahrgänge vor 1926 zusätzlich beim Document-Center in Berlin. Dies geschieht natürlich ohne Kenntnis des Betroffenen. Außerdem werden allgemeine Angaben zur Person wie die Staatsangehörigkeit, Eckdaten aus dem Lebenslauf, das bisherige verdienstvolle Wirken, schon erhaltene Auszeichnungen, Vorstrafen und Wohnorte zwischen 1945 und 1950 erfragt - für im öffentlichen Dienst Beschäftigte beim Dienstherrn (der die Auskünfte anhand der Personalakte erteilt), für andere Personen unter Einschaltung der Regierungspräsidien bei Nachbarn oder Arbeitskollegen. Auch dies geschieht ohne Wissen des Betroffenen, denn sonst könnte ihn die Ehrung nicht überraschen.

Die Stadt Dresden hat Zweifel an der datenschutzrechtlichen Zulässigkeit dieser Verfahrensweise an mich herangetragen, die sich als durchaus berechtigt herausgestellt haben:

Das *Gesetz über Titel, Orden und Ehrenzeichen* (Ordensgesetz) enthält weder Datenverarbeitungsregelungen noch Kriterien für die Ordenswürdigkeit einer Person. Lediglich die Ausführungsbestimmungen zum Statut des Verdienstordens der Bundesrepublik Deutschland regeln die Verleihung (oder Nichtverleihung) der Auszeichnung bei Gesetzesverstößen des Betroffenen. Diese Ausführungsbestimmungen sind jedoch keine ausreichende Rechtsgrundlage, die zu einer Daten*erhebung* über Gesetzesverstöße berechtigen könnte. Außerdem sind die gesetzlichen Grundlagen für die Daten*übermittlungen* nicht immer in der gebotenen Eindeutigkeit vorhanden (z. B. behilft man sich Auskünften des Document-Centers mit einer analogen Anwendung von § 5 Abs. 2 i. V. m. Abs. 5 BArchG). Sogar eindeutig unzulässig ist die Weitergabe von Personalaktendaten eines im öffentlichen Dienst Beschäftigten, der nicht in die Datenweitergabe eingewilligt hat (für Beamte gemäß § 121 SächsBG, für Arbeiter und Angestellte aufgrund des Zweckänderungsverbots gemäß § 12 SächsDSG).

Das Argument, die Einwilligung des Betroffenen nicht einzuholen, um ihn vor verfrühten Hoffnungen und einer nachfolgenden Enttäuschung zu bewahren, wiegt sicher schwer. Da ein Betroffener auch die Möglichkeit haben muß, diese eingehende Prüfung einer Ordenswürdigkeit abzulehnen, sollte er trotzdem frühzeitig in das Verfahren

eingebunden werden.

Auf jeden Fall darf die - unklare und vertrackte - rechtliche Situation nicht dazu führen, daß eine Prüfung der Ordenswürdigkeit unterbleibt. Bei Ordens-Kandidaten, die im öffentlichen Dienst beschäftigt sind, halte ich es deshalb für vertretbar, daß der Dienstherr solche Personaldaten mitteilt, die einer Behörde bzw. sonstigen öffentlichen Stelle ohnehin (z. B. nach § 29 Abs. 1 SächsMG) übermittelt werden dürften. Auch gegen Angaben über Eckdaten des dienstlichen Werdegangs und eine Beurteilung ganz allgemeiner Art habe ich keine Bedenken. Lebenslaufdaten dürfen jedoch wegen ihres ganz persönlichen Charakters nicht mitgeteilt werden. Eine Abgrenzung ist schwierig; ich bin gern bereit, im Einzelfall meinen Rat zu erteilen.

Der Bundesbeauftragte für den Datenschutz sowie mehrere Länder-Datenschutzbeauftragte unterstützen meine Forderung nach einer eindeutigen Regelung der Datenverarbeitung im Ordensgesetz. Der Bundesbeauftragte für den Datenschutz hat zwischenzeitlich beim Bundesminister des Innern eine entsprechende Gesetzesänderung angeregt.

5.2 Personalvertretung

5.2.1 Keine Schwangerschaftsübersichten für den Personalrat

Der Personalrat einer größeren Stadt hat von der Dienststelle eine Liste aller Erzieherinnen (Krippenerzieherinnen, Kindergärtnerinnen und Hortnerinnen) mit Angabe der jeweiligen Vergütungsgruppe angefordert und gebeten, auch bestehende Schwangerschaften und die voraussichtlichen Entbindungstermine auszuweisen. Die Dienststelle war unter Berufung auf das Sächsische Datenschutzgesetz nur bereit, einen mit den Namen der Stelleninhaber versehenen Stellenplan zu erstellen und diesen durch den Personalrat jederzeit in der Personalstelle einsehen zu lassen. Da sich Dienststelle und Personalrat in dieser Frage nicht einigen konnten, bin ich vor der beabsichtigten Anrufung der Einigungsstelle um Stellungnahme gebeten worden.

Ich habe empfohlen, dem Personalrat aktuelle Listen mit den Grunddaten der Erzieherinnen (Name, Tätigkeit und Vergütungsgruppe) zur Verfügung zu stellen, dazu auch den mit den Namen versehenen Stellenplan, allerdings *ohne Schwangerschaftsdaten*, und dies wie folgt begründet:

Die Personalvertretung muß sich zur Wahrnehmung der allgemeinen Aufgaben jederzeit einen Personal-Überblick verschaffen können, und zwar zusätzlich zu den anlaßbezogenen Einzelfallinformationen und ohne stets die Personalstelle einschalten zu müssen. Da eine Liste mit den Grunddaten der Beschäftigten Informationen enthält, die dem Personalrat jederzeit ohne Einwilligung des Betroffenen von der Dienststelle gegeben werden müßten, bestehen insoweit keine datenschutzrechtlichen Bedenken.

Die Mitteilung von Schwangerschaftsdaten darf ohne Einwilligung oder gar gegen den Willen einer Beschäftigten nicht erfolgen. Denn die Weitergabe von Daten über Lebenssachverhalte aus der Privat- oder Intimsphäre - wie das Bestehen einer

Schwangerschaft - ohne Einwilligung der Betroffenen stellt eine Beeinträchtigung des Persönlichkeitsrechts dar (vgl. BVerwG, Beschluß vom 29.8.1990, NJW 1992, 373).

5.2.2 Telekommunikationsanlagen (TK-Anlagen) und das Mitbestimmungsrecht der Personalvertretung

Die Einführung und Anwendung des Telefonverbundes der Sächsischen Staatsregierung im Zusammenhang mit der Beteiligung der Personalräte hat zu Irritationen geführt: Gemäß § 77 Nr. 4 SächsPersVG hat der Personalrat ein Mit*wirkung*srecht 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". Dagegen steht der Personalvertretung ein Mit*bestimmung*srecht gemäß § 80 Abs. 3 Nr. 16 SächsPersVG zu bei der "Einführung und Anwendung technischer Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Beschäftigten zu überwachen".

Während ich mit dem Bundesverwaltungsgericht (BVerwGE v. 16. Dezember 1987, Nr. 6 P 32.84) davon ausgegangen bin, daß die Einführung und Anwendung der TK-Anlage mit*bestimmungs*pflichtig ist, hielt das SMI lediglich die Mit*wirkung* des Personalrats für ausreichend. An die Stelle von Dienstvereinbarungen mit den Personalvertretungen war eine für alle Ressorts geltende Verwaltungsvorschrift vorgesehen.

Ich habe darauf hingewiesen, daß es nach der vorgenannten Entscheidung für die Mitbestimmung der Personalvertretung bereits ausreicht, wenn die technische Einrichtung objektiv für eine Überwachung von Verhalten und Leistung der Beschäftigten geeignet ist. Da dies nach meinem Dafürhalten bei modernen Informations- und Kommunikationsanlagen, die den "Arbeitsbereich der Mitarbeiter" betreffen, stets der Fall sein dürfte und solche Einrichtungen damit auch stets der Mitbestimmung unterliegen, habe ich mich für die Streichung des § 77 Nr. 4 SächsPersVG eingesetzt. Dies insbesondere auch vor dem Hintergrund, daß mir Sinn und Anwendungsbereich dieser Vorschrift nicht einmal nachvollziehbar erläutert werden konnten. Das SMI beabsichtigt nun, bei einer Novellierung des Sächsischen Personalvertretungsgesetzes auf eine Streichung hinzuwirken.

5.2.3 Vorlage von Bewerbungsunterlagen an den Personalrat trotz Widerspruchs des Bewerbers

Ein Staatsministerium bat um Klärung, ob Bewerbungsunterlagen auch dann dem Personalrat vorzulegen seien, wenn der Bewerber dies ausdrücklich *nicht* wünsche.

Ich habe dazu folgende Auffassung vertreten:

Nach § 72 Abs. 2 SächsPersVG hat die Dienststelle dem Personalrat sämtliche Bewerbungsunterlagen (aller Bewerber), die er für eine sachliche und behördenbezogene Entscheidung benötigt, vorzulegen. Bewerbungsunterlagen sind sämtliche vom Bewerber zur Person gemachten Angaben sowie beigebrachten Unterlagen (Zeugnisse,

Lebenslauf, Lichtbild usw.). *Nicht* zu den Bewerbungsunterlagen gehören nach herrschender Meinung der Arbeitsvertrag, das Führungszeugnis sowie das Ergebnis der Einstellungsuntersuchung (LAG Hamm DB 75, 360; LAG Düsseldorf EzA 11 zu § 99 BetrVG 1972; LAG Hamburg BB 75, 1016). Der Dienstherr ist nicht verpflichtet, aber auch nicht berechtigt, diese Unterlagen dem Personalrat vorzulegen.

Hat ein Bewerber um "Vertraulichkeit" gebeten oder sogar ausdrücklich darauf hingewiesen, daß er die Vorlage seiner Bewerbungsunterlagen an den Personalrat nicht wünscht, ändert das nichts an der gesetzlichen Vorlagepflicht der Dienststelle. Ein Bewerber, der sich um eine bestimmte Stelle bewirbt, muß damit rechnen, daß der Arbeitgeber bei seiner Einstellung das durch das Sächsische Personalvertretungsgesetz vorgeschriebene Verfahren einzuhalten hat, also den Personalrat einschalten muß. Insoweit liegt ein rechtlich zulässiger Eingriff in das informationelle Selbstbestimmungsrecht vor. Denn nach Art. 33 SächsVerf darf in das informationelle Selbstbestimmungsrecht nur durch Gesetz oder aufgrund eines Gesetzes eingegriffen werden. Das Sächsische Personalvertretungsgesetz ist ein solches Gesetz, dessen Vollzug nicht der Disposition des Bewerbers unterliegt. Ich habe geraten, den Bewerber auf die Rechtslage hinzuweisen, um ihm Gelegenheit zu geben - sofern er seine Meinung nicht ändert -, von seiner Bewerbung zurückzutreten.

5.3 Meldewesen

5.3.1 Entwicklung des Einwohnermeldewesens

Das Sächsische Meldegesetz vom 21. April 1993 hat Bewegung in das Einwohnermeldewesen gebracht. In zunehmendem Maße wird das Meldewesen von den Landratsämtern auf die gemäß § 2 Abs. 1 SächsMG zuständigen Gemeinden übertragen, ohne daß die bis zum 31. Dezember 1995 laufende Übergangsfrist (§ 38 Abs. 1 SächsMG) ausgeschöpft wird. Mit Ausnahme eines Landkreises, wo die Software zur Übernahme der Meldedaten durch die Gemeinden zu fehlerhaften Ergebnissen geführt haben soll, sind mir keine Probleme mit dem Vollzug des § 38 Abs. 1 SächsMG bekanntgeworden.

Probleme gab es jedoch im Zusammenhang mit der Verarbeitung von Meldedaten im Auftrag durch Private. Soweit die Meldebehörden selbst dazu nicht in der Lage sind, dürfen mit der automatisierten Führung des Melderegisters nur andere sächsische Gemeinden oder sonstige juristische Personen des öffentlichen Rechts, die der Aufsicht des Freistaates Sachsen unterstehen, beauftragt werden (§ 3 SächsMG). Für eine Übergangszeit wurden nach § 38 Abs. 2 SächsMG bestehende Auftragsdatenverarbeitungsverhältnisse mit Privaten bis zum 31. Dezember 1993 geduldet. Eine große Zahl sächsischer Meldebehörden läßt bei den ehemaligen DVZ - also bei Privaten - u. a. das Einwohnermeldewesen im Wege der Auftragsdatenverarbeitung rechnen.

Aufgeschreckt durch diese rechtliche Situation suchten die ehemaligen DVZ und insbesondere der Sächsische Städte- und Gemeindetag (SSG) das Gespräch mit dem SMI und mit mir, um ohne den durch § 38 Abs. 2 SächsMG entstandenen Zeitdruck

eine sachgerechte Lösung zu erwirken.

Gegen meine grundsätzlichen Bedenken wurden inzwischen drei Zweckverbände zur kommunalen Datenverarbeitung gegründet und genehmigt. Diesen Zweckverbänden (juristischen Personen des öffentlichen Rechts) soll von den Meldebehörden gemäß § 3 SächsMG die automatisierte Führung des Melderegisters übertragen werden. Die Zweckverbandssatzungen sehen übereinstimmend die Beauftragung privater Subauftragnehmer vor, was nicht per se unzulässig sein muß. Nach Auffassung des SMI kann die Einbeziehung Privater in die Verarbeitung von Meldedaten im Wege eines Unterauftragsverhältnisses dann zugelassen werden, wenn der Datenschutz sowohl in rechtlicher wie auch in technisch-organisatorischer Hinsicht gewährleistet wird. Die mir vorliegenden Zweckverbandssatzungen bieten jedenfalls diese Gewähr nicht. Für rechtswidrig halte ich die Formulierung in den Satzungen, wonach die Verantwortung für die Einhaltung der Datenschutzbestimmungen (allein) dem Zweckverband obliegt. Dem steht § 7 Abs. 1 SächsDSG entgegen (siehe insbesondere Nrn. 8 und 9 der Bekanntmachung des Sächsischen Datenschutzbeauftragten zur Datenverarbeitung im Auftrag vom 3. November 1993, nachstehend abgedruckt unter 16.1.4), wonach insbesondere der Auftraggeber als "Herr der Daten" für die Einhaltung des Datenschutzes verantwortlich ist.

Aus den Satzungen ist auch nicht ersichtlich, ob die Zweckverbände selbständige Stellen oder lediglich Auftragnehmer sind. Wäre ersteres der Fall, schiede eine Datenübermittlung von den Mitgliedsgemeinden an die Zweckverbände mangels verfassungsrechtlich gebotener Rechtsgrundlage (Art. 33 SächsVerf) aus. Sollten die Zweckverbände dagegen als Auftragnehmer fungieren, müßten sie sich einer permanenten Überwachung durch die Mitgliedsgemeinden als Auftraggeber unterwerfen (§ 7 Sächs DSG).
Erhebliche Meinungsverschiedenheiten zwischen dem SMI und mir müssen in diesen Fragen noch ausgeräumt werden.

Jedenfalls hat der Gesetzgeber Ende des Jahres 1993 mit meiner Zustimmung durch Verlängerung der in § 38 Abs. 2 SächsMG enthaltenen Übergangsfrist um ein Jahr (also bis zum 31.12.1994) den Zeitdruck verringert und so zu einer wesentlichen Entspannung der Situation beigetragen. Ich gehe davon aus, daß mich das Thema "Zweckverbände und private Subauftragnehmer" auch 1994 beschäftigen wird.

Ich erwarte eine möglichst weitgehende Dezentralisierung, einen - ohnehin durch das Haushaltsrecht gebotenen - Leistungswettbewerb und eine jederzeitige bestimmende Kontrolle der Einzelgemeinde in Bezug auf die Datenverarbeitung.

5.3.2 Erlaß der Ersten Verordnung des SMI zur Durchführung des Sächsischen Meldegesetzes (Meldevordruckverordnung - MVVO) vom 6. September 1993

Am 1. November 1993 ist die Meldevordruckverordnung in Kraft getreten, die u. a. die im Meldewesen zu verwendenden Formulare inhaltlich vorschreibt. An der Entstehung der MVVO wurde ich gemäß § 13 Abs. 5 Satz 4 der Geschäftsordnung der Sächsi-

schen Staatsregierung *rechtzeitig* beteiligt.

Allerdings sind die meisten meiner Änderungsvorschläge nicht übernommen worden.

Beispielsweise habe ich mich erfolglos dagegen ausgesprochen, daß in einer Meldevordruckverordnung Datenübermittlungsvorschriften (§§ 1 Abs. 5, 3 Abs. 2 MVVO) aufgenommen werden.
Auch mein Hinweis, daß § 4 MVVO mit der in ihm vorgesehenen Aufbewahrungsfrist und Löschungsverpflichtung im Widerspruch zu den Aufbewahrungs- und Löschungsbestimmungen des § 26 SächsMG stehen, wurde ignoriert.

Weil Anmeldebescheinigungen (Anlage 1 a zur MVVO) vielfach zur Vorlage bei anderen öffentlichen Stellen oder bei Privaten (z. B. Vermieter) dienen, habe ich empfohlen, lediglich zu bescheinigen, wann sich wer mit welcher Wohnung gemeldet hat. Die übrigen Daten sollten geschwärzt werden. Auch diesem Vorschlag ist der Verordnungsgeber nicht gefolgt. Durch Vorlage der Meldebescheinigung bei Behörden oder Privaten werden nun weitaus mehr Daten als erforderlich offenbart.

Bei den Erläuterungen zum Ausfüllen des Meldescheins (Anlage 1 b zur MVVO) habe ich ohne Erfolg darum gebeten, eine Auskunftssperre bei Gefahr für Leben, Gesundheit, persönliche Freiheit oder ähnliche schutzwürdige Belange von einer Gebührenpflicht auszunehmen (siehe auch nachfolgend unter 5.3.3).

Auch den Religionsschlüssel "VD" (ursprünglich "keine öffentlich-rechtliche Religionsgesellschaft"; jetzt "verschiedene") habe ich erfolglos bemängelt. Als Erläuterung der Bedeutung des Schlüssels "VD" habe ich vorgeschlagen: "keine *dieser* öffentlich-rechtlichen Religionsgesellschaften". Es gibt nämlich niemanden, der verschiedenen (also mehreren) Religionsgesellschaften angehört.

Gefolgt ist der Verordnungsgeber meinem Vorschlag, auf die (überflüssige) Frage nach der Wehrüberwachung zu verzichten.

Im übrigen wird mit dem An- und Abmeldeformular bei Geschiedenen und Verwitweten unzulässigerweise das Datum "Familienstand seit" erhoben. § 5 Abs. 1 Nr. 14 SächsMG sieht lediglich bei Verheirateten den "Tag der Eheschließung" vor. Die Meldeformulare sind insoweit rechtswidrig.
Die Meldebehörden wären gut beraten, das Datum "Familienstand seit" bei Geschiedenen und Verwitweten nicht mehr zu erheben und bisher unzulässigerweise erhobene Daten zu löschen.

5.3.3 Melderechtliche Auskunfts- und Übermittlungssperren; diesbezügliche Kostenregelung

Anfragen zur Speicherung melderechtlicher Auskunfts- und Übermittlungssperren haben die Schwierigkeiten deutlich gemacht, welche die Meldebehörden mit den entsprechenden Regelungen im Sächsischen Meldegesetz haben. So war vielfach nicht bekannt, daß es im Melderecht nachstehende *acht* Auskunfts- und Übermittlungssperren gibt, die bei

Auskunftsersuchen, insbesondere aber auch verfahrenstechnisch im automatisierten Meldewesen berücksichtigt werden müssen:

1. Auskunftssperre nach § 1758 Abs. 2 BGB (Adoptionspflegeverhältnis),
2. Auskunftssperre nach § 61 Abs. 2 bis 4 PStG (insbesondere Erwachsenenadoption, Transsexuelle),
3. Auskunftssperre wegen Gefahr für Leben, Gesundheit, persönliche Freiheit oder ähnliche schutzwürdige Belange,
4. Auskunftssperre nach § 21 Abs. 6 MRRG (Sperrung der sogenannten erweiterten Melderegisterauskunft),
5. Übermittlungssperre nach § 19 Abs. 2 Satz 3 MRRG, § 30 Abs. 2 Satz 3 SächsMG (Widerspruch gegen Datenübermittlungen an öffentlich-rechtliche Religionsgesellschaften),
6. Auskunftssperre nach § 33 Abs. 1 und 4 SächsMG (Widerspruch bei Auskünften an Parteien, Wählergruppen und andere Träger von Wahlvorschlägen),
7. Auskunftssperre nach § 33 Abs. 2 und 4 SächsMG (Widerspruch bei Alters- und Ehejubiläumsauskünften),
8. Auskunftssperre nach § 33 Abs. 3 und 4 SächsMG (Widerspruch gegen Veröffentlichungen im Adreßbuch).

Eine zusätzliche *neunte* Auskunftssperre, die von Amts wegen gelten muß, halte ich im Hinblick auf den nachstehenden Abschnitt 5.3.4 bei Personen, die in Justizvollzugsanstalten, in Krankenhäusern, Pflegeheimen oder ähnlichen Einrichtungen i. S. v. § 20 Abs. 1 SächsMG gemeldet sind, wegen des Aussagegehaltes der ja regional durchaus bekannten Anstaltsanschriften für geboten (und zwar nicht etwa erst de lege ferenda).

Außer in den Fällen des § 30 Abs. 2 SächsMG (Widerspruch gegen Datenübermittlungen an öffentlich-rechtliche Religionsgesellschaften) und des § 33 SächsMG (Widerspruch gegen Auskünfte an politische Parteien, Veröffentlichung von Jubiläumsdaten, Adreßbuchverlage) kann ein Betroffener nach § 34 Abs. 1 SächsMG bei der Meldebehörde die Eintragung einer Auskunftssperre im Melderegister beantragen, soweit er ein berechtigtes Interesse an der Auskunftsverweigerung *glaubhaft macht.*
Welche der oben unter Nrn. 1 bis 4 genannten Auskunftssperren *beantragt* werden müssen, geht aus § 34 Abs. 1 SächsMG nicht hervor. Ich vertrete die Auffassung, daß die unter 1 (Adoptionspflegeverhältnis) und 2 (Erwachsenenadoption, Transsexuelle) genannten Auskunftssperren aufgrund standesamtlicher Mitteilungen von *Amts wegen* einzutragen sind. Demnach kommt eine Beantragungspflicht nach § 34 Abs. 1 SächsMG nur in den Fällen 3 (Gefahr für Leben, Gesundheit, persönliche Freiheit oder ähnliche schutzwürdige Belange) und 4 (Sperrung der sog. erweiterten Melderegisterauskunft) in Betracht.

Ein vom SMI herausgegebenes vorläufiges Kostenverzeichnis sieht allgemein für Auskunftssperren nach § 34 SächsMG eine Gebühr von 30,- DM vor. Dem Vernehmen nach ist beabsichtigt, diese Gebühr auch im endgültigen Kostenverzeichnis festzuschreiben. Ich habe das SMI und SMF wiederholt in aller Deutlichkeit darauf hingewiesen, daß Betroffene, denen durch eine Melderegisterauskunft eine Gefahr für Leben, Gesundheit, persönliche Freiheit oder ähnliche schutzwürdige Belange drohen würde, nicht durch eine Gebührenpflicht von der Geltendmachung eines Schutzrechts abgehal-

ten werden dürfen. Die Gebührenerhebung kommt daher nur für die unter 4 aufgeführte Auskunftssperre (Sperrung der sog. erweiterten Melderegisterauskunft) in Betracht. Ich erwarte, daß meiner Forderung auf Gebührenverzicht im endgültigen Kostenverzeichnis Rechnung getragen wird.

5.3.4 Darf die Meldebehörde Auskunft über Anschriften von Häftlingen, Pflege-heimbewohnern oder Patienten in psychiatrischen Krankenhäusern usw. an Private erteilen?

Ein Einwohnermeldeamt fragte, ob es zulässig sei, die Anschrift eines in einer Justizvollzugsanstalt (JVA) gemeldeten Betroffenen einem Inkassobüro bekanntzugeben. Ähnliche Anfragen könnten Betroffenen gelten, die beispielsweise in Pflegeheimen oder psychiatrischen Krankenhäusern untergebracht sind.

Hierzu vertrete ich folgende Auffassung:

Wer in ein Krankenhaus, ein Pflegeheim oder eine ähnliche Einrichtung, die der Betreuung pflegebedürftiger oder behinderter Menschen oder der Heimerziehung dient, aufgenommen wird, unterliegt der Meldepflicht, solange er nicht für eine andere Wohnung in der Bundesrepublik Deutschland gemeldet ist (vgl. § 20 Abs. 1 SächsMG). Gleiches gilt für Personen, die aufgrund richterlicher Entscheidung in eine Justizvollzugsanstalt aufgenommen worden sind (vgl. § 16 Abs. 1 Nr. 3 und Abs. 3 SächsMG).
In den genannten Fällen wird als Anschrift der Ort, die Straße und die Hausnummer der Einrichtung bzw. der Justizvollzugsanstalt im Melderegister gespeichert. Zusätze, die das "besondere Aufenthaltsverhältnis" betreffen (z. B. JVA), dürfen im Melderegister nicht gespeichert werden. Trotzdem können durch die Übermittlung dieser Anschriften an Dritte sehr wohl schutzwürdige Belange der Betroffenen beeinträchtigt werden. In der Regel sind nämlich die Anschriften der Einrichtungen i. S. v. § 20 Abs. 1 SächsMG regional, Anschriften von Justizvollzugsanstalten sogar zumeist überregional bekannt.

Daher bin ich der Auffassung, daß die Einwohnermeldeämter die Vorschrift des § 22 SächsMG (Berücksichtigung schutzwürdiger Interessen des Betroffenen bei der Datenverarbeitung) bei ihrer Ermessensentscheidung, ob Auskunft aus dem Melderegister erteilt wird, in diesen Fällen *besonders* beachten müssen. Die Meldebehörden handeln meines Erachtens nur dann nicht ermessenfehlerhaft, wenn sie zwischen dem Geheimhaltungsinteresse des Betroffenen und dem Auskunftsinteresse des Antragstellers abwägen. Hierzu müssen sie vor Auskunftserteilung den Zweck der Auskunft beim Auskunftssuchenden erfragen und den Betroffenen (ggf. seinen gesetzlichen Vertreter) anhören.
Die Vorschrift des § 32 Abs. 4 SächsMG, wonach eine Melderegisterauskunft *unterbleibt*, wenn dem Betroffenen oder einer anderen Person hierdurch eine Gefahr für Leben, Gesundheit, persönliche Freiheit oder ähnliche schutzwürdige Belange erwachsen kann, stellt hierbei eine Ermessens*grenze* dar. Liegt eine dieser Voraussetzungen vor, dürfen die Einwohnermeldeämter unabhängig von einem ggf. geltend gemachten berechtigten Interesse des Auskunftssuchenden *zwingend keine* Auskunft erteilen.
In den genannten Fällen ist es zweckmäßig, entweder eine Auskunftssperre von Amts wegen einzutragen oder zumindest dem Betroffenen nahezulegen, eine Auskunftssperre

nach § 34 Abs. 1 SächsMG zu beantragen, damit sichergestellt ist, daß seine Belange bei der Frage der Auskunftserteilung berücksichtigt werden (vgl. § 34 Abs. 2 SächsMG). Keinesfalls darf das Einwohnermeldeamt jedoch die Prüfung der Belange des Betroffenen mit der Begründung unterlassen, er habe es versäumt, eine Auskunftssperre zu beantragen. Eine solche Auslegung wiederspräche dem Gebot, Gesetze so auszulegen, daß ein möglichst effektiver Grundrechtsschutz gewährleistet wird.

Nach meiner Auffassung wird das Auskunftsinteresse grundsätzlich dann überwiegen, wenn der Antragsteller glaubhaft macht, daß er die Anschrift und ggf. weitere Daten des Betroffenen benötigt, um *Rechtsansprüche* gegen diesen geltend zu machen. Denn es läßt sich mit der verfassungsmäßigen Rechtsschutzgarantie (Art. 19 Abs. 4 GG) nicht vereinbaren, dem Antragsteller den Rechtsweg abzuschneiden, indem man ihm die Anschrift seines Schuldners verheimlicht.

5.3.5 Verwendung von Meldescheinvordrucken und Antragsformularen zur Einrichtung von Auskunfts- und Übermittlungssperren, die mit dem Sächsischen Meldegesetz nicht vereinbar sind

Vor Inkrafttreten der Meldevordruckverordnung am 1. November 1993 (oben 5.3.2) habe ich bei einer Stadt die Verwendung von Meldescheinvordrucken festgestellt, die mit dem Sächsischen Meldegesetz nicht in Einklang gebracht werden konnten.

Meinen Feststellungen zufolge wurden im Bereich des Einwohnermeldewesens Formulare verwendet, mittels deren auch unzulässige Daten erhoben, gespeichert und möglicherweise im Vollzug der 1. und 2. BMeldDÜV an andere Stellen übermittelt wurden. Sämtliche im Anmeldevordruck angegebenen Rechtsgrundlagen (Vorder- und Rückseite) galten in Sachsen nicht (die Formulare stammten wohl aus Baden-Württemberg). Gleichwohl wurden die Betroffenen unter Hinweis auf diese Rechtsgrundlagen verpflichtet, das Formblatt "wahrheitsgemäß" und "lückenlos" auszufüllen. Folge war, daß die Meldepflichtigen Angaben machen mußten, die weder durch § 2 MRRG noch durch § 5 SächsMG gedeckt waren. Im einzelnen waren dies die Fragen nach
- dem Beruf
- der Seriennummer des Personalausweises, des vorläufigen Personalausweises, des Reisepasses/Paßersatzes
- Familienstand seit (es darf nur das Eheschließungsdatum erfragt werden)
- Ausbildung als Krankenpfleger, Röntgen- oder med.-techn. Laborpersonal.

Unter Hinweis auf §§ 7 Nr. 3, 10 MRRG, 23 Abs. 1 Nr. 3, 26 SächsMG bat ich zu veranlassen, daß die unzulässigerweise erhobenen Daten sowohl im Melderegister (falls sie dort gespeichert wurden) als auch in den gesammelten Meldeformularen (z. B. durch Schwärzen) gelöscht wurden. Außerdem waren in den noch vorhandenen (leeren) Vordrucken die unzulässigen Fragen nach Beruf, Seriennummer und medizinischem Personal für Eingaben zu sperren (z. B. Durchkreuzen der Eingabefelder). Im übrigen habe ich die übergangsweise Weiterverwendung der Formulare bis zum Inkrafttreten des Sächsischen Meldegesetzes bzw. bis zum Vorliegen eines amtlich vorgeschriebenen Meldescheins geduldet.

Weiter habe ich festgestellt, daß der "Antrag auf Einrichtung einer Auskunftssperre bzw. Übermittlungssperre" in verschiedener Hinsicht mängelbehaftet war.
Ich habe mich wie folgt geäußert:

1. Das Antragsformular ist wenig bürgerfreundlich.
   Die Hinweise auf Bestimmungen des MRRG, auf § 61 Abs. 2 und 3 PStG und § 1758 BGB sind ohne nähere Erläuterungen für den Antragsteller unverständlich.
2. Auskunftssperren nach § 1758 BGB (Adoptionspflege) werden nicht beantragt, sondern sind von Amts wegen zu speichern.
   Mit der Annahme als Kind (Adoption) sind *sämtliche* Hinweise, die auf eine Adoption schließen lassen (z. B. der bisherige Name des Kindes), sowie die Auskunftssperre zu *löschen*. Eine Auskunftssperre nach § 61 Abs. 2 PStG scheidet aus, da sie mehr offenbaren als schützen würde. Ein adoptiertes Kind ist melderechtlich wie ein eheliches Kind zu behandeln.
3. Der Vordruck ist so gestaltet, daß der Antragsteller bei jeder der acht verschiedenen Auskunftssperren von einer Begründungspflicht ausgehen muß. Tatsächlich gibt es eine Pflicht zur Begründung des Antrags nur bei den Auskunftssperren nach § 21 Abs. 5 und 6 MRRG (bzw. nach § 34 Abs. 1 SächsMG).
4. Eine Auskunftssperre betreffend "Gruppenauskünfte nach § 21 Abs. 3 MRRG" ist melderechtlich *nicht* vorgesehen.
5. Eine Auskunftssperre für Transsexuelle (§ 61 Abs. 4 PStG) wird nicht eröffnet. Das Formular sieht lediglich die Fälle des § 61 Abs. 2 und 3 PStG vor.
6. Die Hinweise, daß der Antragsteller über die Entscheidung der Meldebehörde schriftlich Bescheid erhält, sind irreführend.
   Die Betroffenen haben einen Rechtsanspruch auf Eintragung folgender Auskunftssperren:
   - Adoptionspflege (§ 1758 BGB)
   - § 61 Abs. 2 - 4 PStG
   - Kirchen
   - politische Parteien
   - Adreßbuchverlage u. ä.
   - Alters- und Ehejubiläen.

   Für die Meldebehörde besteht insoweit *kein* Ermessensspielraum.

   Über die Ablehnung der Auskunftssperren nach § 21 Abs. 5 und Abs. 6 MRRG (§ 34 Abs. 1 SächsMG) ist ein Bescheid zu erteilen, um dem Betroffenen den Verwaltungsrechtsweg zu eröffnen.

Die von mir kritisierte Meldebehörde hat prompt reagiert und datenschutzgerechte Vordrucke eingeführt.

5.3.6 Anwendbarkeit der technisch-organisatorischen Datenschutzbestimmungen bei Online-Anschlüssen an das Melderegister

Insbesondere in den größeren Stadtverwaltungen besteht Bedarf, einzelne Fachämter im Online-Verfahren auf bestimmte Daten des Melderegisters zugreifen zu lassen. Automatisierte Abrufverfahren zwischen verschiedenen, organisatorisch getrennten Behörden werden melderechtlich grundsätzlich als "*regelmäßige* Datenübermittlung" behandelt.

Sie sind gemäß § 29 Abs. 5 SächsMG nur zulässig, *soweit dies durch Bundes- oder Landesrecht* unter Festlegung des Anlasses und des Zwecks der Übermittlungen, der Empfänger und der zu übermittelnden Daten bestimmt ist.
Soll die regelmäßige Meldedatenübermittlung jedoch *innerhalb* der Gemeinde, die ja Meldebehörde ist (§ 2 Abs. 1 SächsMG), erfolgen, ist dies nach meiner Auffassung gemäß § 29 Abs. 7 SächsMG *nicht* von einer bundes- oder landesrechtlichen Ermächtigung abhängig. Gleichwohl darf für regelmäßige Meldedatenübermittlungen im Online-Verfahren innerhalb der Gemeinde kein datenschutzfreier Raum entstehen. Da § 4 Abs. 2 SächsMG das Sächsische Datenschutzgesetz ausdrücklich für anwendbar erklärt, falls im Meldegesetz entsprechende Datenschutzbestimmungen fehlen, sind Online-Anschlüsse innerhalb der Gemeindeverwaltung an § 8 Abs. 2 SächsDSG zu messen. § 8 Abs. 2 SächsDSG schreibt nämlich speziell für solche Fälle vor, daß ein automatisierter Datenabruf innerhalb der Gemeindeverwaltung nur zulässig ist, wenn dieses Verfahren unter Berücksichtigung der schutzwürdigen Interessen der Betroffenen (Einwohner) und der Aufgaben der öffentlichen Stelle angemessen ist und eine mindestens stichprobenweise Abrufkontrolle gewährleistet ist. Außerdem ist *vor* Aufnahme des Abrufverfahrens schriftlich festzulegen:
1. der Anlaß und der Zweck des Abrufverfahrens,
2. die Datenempfänger,
3. die abrufbaren Daten,
4. die Maßnahmen zur Gewährleistung des Datenschutzes (§ 9 SächsDSG).

Nach § 8 Abs. 3 SächsDSG ist der Sächsische Datenschutzbeauftragte *vor* der Einrichtung eines solchen innergemeindlichen Abrufverfahrens zu unterrichten.

Die vom SMI in dieser Frage bisher vertretene Ansicht, § 8 Abs. 2 SächsDSG sei für behördeninterne Online-Anschlüsse ans Melderegister *nicht* anwendbar, wird dem Vernehmen nach *nicht* aufrechterhalten. Meine Überzeugungsbemühungen werden andernfalls fortgesetzt.
Jedenfalls werde ich Online-Anschlüsse innerhalb der Gemeinde, welche die Voraussetzungen des § 8 Abs. 2 SächsDSG nicht erfüllen, nach § 26 SächsDSG beanstanden müssen.

5.3.7 Meldedatenübermittlung an Hochschulen bzw. an Hochschulinstitute zum Zwecke der wissenschaftlichen Forschung

Meldedatenübermittlungen an Hochschulen bzw. an Hochschulinstitute sind grundsätzlich nach § 29 Abs. 1 SächsMG zulässig; jedoch sind sie an folgende Auflagen zu binden (vgl. auch § 30 SächsDSG):
1. Der Datenempfänger ist auf den Zweckbindungsgrundsatz (§ 29 Abs. 6 SächsMG) hinzuweisen. Die Daten dürfen nur für das Forschungsvorhaben verwendet werden, für das sie übermittelt wurden.
2. Der Datenempfänger hat die Betroffenen schriftlich darauf hinzuweisen, daß die Befragung *freiwillig* ist. Erfolgt der Hinweis zusammen mit anderen Erklärungen, so ist er deutlich hervorzuheben. Auf die Folgen einer Verweigerung der Einwilligung muß ebenfalls schriftlich hingewiesen werden.
3. Die Betroffenen sind vom Datenempfänger über Inhalt und Zweck der Befragung sowie über die Auswertung und die weitere Verwendung der Daten zu informieren.

4. Daten von Personen, die die Teilnahme an der Befragung verweigern, sind unverzüglich beim Datenempfänger zu löschen.
5. Die übermittelten Daten sind gegen unberechtigten Zugriff zu sichern.
6. Nach Abschluß des Projekts sind die Daten unverzüglich zu löschen.
7. Zusammenstellungen von Ergebnissen dürfen keine Angaben enthalten, die auf bestimmte oder bestimmbare Personen hinweisen; d. h. sie müssen anonymisiert sein.

Es wäre wünschenswert, wenn vorstehende Hinweise in die noch nicht vorhandene Vollzugsbekanntmachung zum Sächsischen Meldegesetz aufgenommen würden.

5.3.8 Veröffentlichung von Jubiläumsdaten

Nach § 33 Abs. 2 SächsMG darf die Meldebehörde Namen, Doktorgrad, Anschriften, Tag und Art des Jubiläums von Alters- und Ehejubilaren veröffentlichen und an Presse, Rundfunk oder andere Medien zum Zwecke der Veröffentlichung übermitteln. Dies gilt nicht, soweit die Betroffenen für eine Justizvollzugsanstalt, für ein Krankenhaus, Pflegeheim oder eine ähnliche Einrichtung im Sinne von § 20 Abs. 1 SächsMG gemeldet sind, eine Auskunftssperre besteht oder die Betroffenen der Auskunftserteilung, der Veröffentlichung oder der Datenübermittlung widersprechen (§ 33 Abs. 4 Satz 1 SächsMG).

Wiederholt habe ich beim Studium der Presse festgestellt, daß auch die Daten von Jubilaren, die in *Pflegeheimen* gemeldet sind, veröffentlicht wurden. Die betreffenden Meldebehörden habe ich auf die Unzulässigkeit hingewiesen.

Meine Feststellungen unterstreichen die Notwendigkeit, in den automatisierten Einwohnerverfahren durch eine besondere Auskunftssperre die zumindest regional bekannten Anschriften von Justizvollzugsanstalten, Krankenhäusern, Pflegeheimen oder ähnlichen Einrichtungen i. S. v. § 20 Abs. 1 SächsMG so zu kennzeichnen, daß Melderegisterauskünfte jedweder Art - so auch an Adreßbuchverlage oder an politische Parteien - *grundsätzlich* (siehe dazu oben unter 5.3.4) unterbleiben.

5.3.9 Organisation des Eingangs und Abgangs der Meldeamtspost

Zur Frage, ob die Entscheidung des Bürgermeisters (Behördenleiter gem. § 53 SächsGemO) oder des Hauptamtleiters einer Gemeinde, die Meldeamtspost im Abteilungssekretariat oder in der zentralen Poststelle öffnen zu lassen, gegen datenschutzrechtliche Bestimmungen verstößt, habe ich wie folgt Stellung genommen:

Meldedaten sind ihrem Wesen nach heikle Daten, was u. a. auch in § 9 SächsMG (Meldegeheimnis) zum Ausdruck kommt. Die Kenntnisnahme von Meldedaten durch *nicht* mit dem Vollzug des Sächsischen Meldegesetzes beauftragte Bedienstete ist geeignet, das Recht der Betroffenen auf informationelle Selbstbestimmungs (vgl. Art. 33 SächsVerf, § 1 SächsDSG, § 22 SächsMG) unzulässig zu beeinträchtigen. Innerhalb einer Gemeindeverwaltung sollte daher der Personenkreis, der Kenntnis von Meldedaten erhalten darf, möglichst klein gehalten werden. Eindeutig an die Meldebehörde adressierte Post sollte nach meinem Dafürhalten *nicht* durch Personal der *zentralen*

Poststelle geöffnet werden dürfen. Auch ein Öffnen der Meldeamtspost im Sekretariat des Hauptamtsleiters halte ich für bedenklich, zumal das Hauptamt keine Aufgaben der Meldebehörden (§ 1 SächsMG) zu erfüllen hat.

Soweit dem Bürgermeister in kleinen Gemeinden durch Gemeinderatsbeschluß bzw. durch Hauptsatzung das Einwohnermeldewesen zur Aufgabenerledigung übertragen wurde, habe ich keine Bedenken, wenn das Öffnen der Meldeamtspost in seinem Sekretariat erfolgt und er sie nach Kenntnisnahme und unter Beachtung von § 9 Abs. 4 SächsDSG an das Meldeamt weiterleitet.

Eine besondere Bestimmung, wie sie beispielsweise § 22 der Dienstanweisung für die Standesbeamten und deren Aufsichtsbehörden (DA) für die Standesamtspost vorsieht, halte ich im Hinblick auf § 4 Abs. 2 SächsMG für nicht unbedingt erforderlich. Die ergänzende Anwendbarkeit des Sächsischen Datenschutzgesetzes verpflichtet nämlich die Gemeinden, alle zur Gewährleistung des Datenschutzes nötigen personellen, technischen und organisatorischen Maßnahmen zu treffen. Insbesondere ist die innere Organisation so zu gestalten, daß sie den besonderen Anforderungen des Datenschutzes gerecht wird (vgl. § 9 Abs. 2 Nr. 10 SächsDSG). Dazu gehört auch die Organisation einer das Persönlichkeitsrecht des Einzelnen berücksichtigenden Posteingangs- und -abgangsbearbeitung innerhalb der Gemeinde (nicht nur bezüglich der Meldeamtspost). Entsprechende Hinweise in einer Verwaltungsvorschrift des SMI würde ich begrüßen.

5.3.10 Aufbewahrung der alten Kreismeldestellenkartei

Eine Kontrolle bei einer Stadtverwaltung ergab, daß dort die alte Kreismeldestellenkartei der DDR nicht nur für Bedienstete des Einwohnermeldeamts, sondern auch für Mitarbeiter anderer Ämter zugänglich war. Ich habe dies nachdrücklich kritisiert:

Die Kreismeldestellenkartei der DDR enthält u. a. melderechtsfremde Daten mit besonders starkem Persönlichkeitsbezug, und zwar z. B. über
- Haftzeiten,
- Ein- und Ausreisen,
- Anträge auf Verlassen der DDR,
- die Personenkennzahl.

Gemäß § 38 Abs. 3 i. V. m. § 26 Abs. 4 SächsMG muß die alte Kreismeldestellenkartei *gesondert aufbewahrt* und durch *technische und organisatorische Maßnahmen* besonders gesichert werden. Ich habe daher verlangt, daß die Kartei unverzüglich in einem Raum untergebracht wird, der diesen Anforderungen entspricht. Insbesondere habe ich gefordert, die Tür mit einem einbruchsicheren Schloß zu versehen. Darüber hinaus habe ich darauf hingewiesen, daß die in der Kartei enthaltenen melderechtsrelevanten Daten unverzüglich in den EDV-Bestand des Einwohnermeldeamts übernommen werden. Anschließend (bis spätestens zum 31.12.1995) ist die alte Kreismeldestellenkartei an das zuständige Archiv abzugeben. Diese Verfahrensweise ist mit dem SMI abgestimmt.

Die Stadtverwaltung hat mir inzwischen mitgeteilt, daß die Kreismeldestellenkartei in einem durch eine Stahltür gesicherten Raum mit vergitterten Fenstern gesondert

aufbewahrt wird. Der Schlüssel zu diesem Raum befindet sich beim Leiter des Einwohnermeldeamts.

Ich werde die Angelegenheit weiter im Auge behalten und gegebenenfalls durch eine erneute Kontrolle feststellen lassen, ob das oben geschilderte Verfahren eingehalten wird.

5.3.11 Übermittlung von Meldedaten an die Gebühreneinzugszentrale der Rundfunkanstalten (GEZ)

Im 1. Tätigkeitsbericht (5.3.3) habe ich mich ausführlich zur Problematik regelmäßiger Meldedatenübermittlungen an die GEZ geäußert. An meiner seinerzeitigen Auffassung, die von der überwiegenden Mehrzahl der Datenschutzbeauftragten des Bundes und der Länder geteilt wird, hat sich im wesentlichen nichts geändert. Der (mit Ausnahme des Bayerischen Datenschutzbeauftragten) gemeinsam vertretene Standpunkt wurde von der Datenschutzkonferenz in einer (im Anhang unter 16.2.1 abgedruckten) "Entschließung zu regelmäßigen Datenübermittlungen an die öffentlich-rechtlichen Rundfunkanstalten und die Gebühreneinzugszentrale (GEZ)" deutlich.

Auf Bitte der Staatskanzlei, ein für die Einwohner am wenigsten belastendes Verfahren zu finden, das gleichzeitig dem Anliegen der GEZ nach einem aktuellen Datenbestand Rechnung trägt, machte ich folgenden Vorschlag:

"Die öffentlich-rechtliche Rundfunkanstalt/GEZ übergibt der Meldebehörde einen Datenträger mit dem bisherigen Rundfunkteilnehmer-Datenbestand. Die Meldebehörde gleicht die Daten mit dem Melderegister ab und teilt der öffentlich-rechtlichen Rundfunkanstalt/GEZ Abweichungen mit (z. B. Wegzugsadressen, Sterbedatum). Für solche Maßnahmen würde es keiner Meldedatenübermittlungsverordnung bedürfen."

Es wird sich weisen, ob die GEZ sich damit zufrieden gibt, oder ob sie in Wahrheit das Interesse verfolgt, einen umfassenden Überblick über den Meldebestand zu erhalten.

5.4 Wahlrecht

5.4.1 Entwurf einer Landeswahlordnung

Zum Entwurf der Landeswahlordnung (LWO) habe ich ausführlich Stellung genommen. Einige Schwerpunkte möchte ich herausgreifen.

1. Für Patienten, Pflegebedürftige, Personen, die in sozialtherapeutischen Anstalten oder in Justizvollzugsanstalten untergebracht sind, sollen "bewegliche Wahlvorstände" und "Sonderwahlbezirke" eingerichtet werden. Da dieser Personenkreis ein besonderes Interesse daran hat, daß der Aufenthalt in solchen Einrichtungen nicht unnötigerweise bekannt wird, habe ich vorgeschlagen, zum Schutz des informationellen Selbstbestimmungsrechts für die Betroffenen *generell* Briefwahlen vorzusehen.

2. Nach §§ 32 Abs. 4, 34 SächsMG besteht die Möglichkeit, eine *Auskunftssperre* wegen einer Gefahr für Leben, Gesundheit, persönliche Freiheit und andere schutzwürdige Belange im Melderegister zu vermerken. Die Meldebehörde darf in einem solchen Fall keine Melderegisterauskunft über den Betroffenen an Private erteilen.

   Das *öffentlich auszulegende* Wählerverzeichnis erfüllt den melderechtlich vorgesehenen Schutzzweck der Auskunftssperre nicht mehr in ausreichendem Maße. Aus diesem Grunde wäre es zu begrüßen, wenn in der Landeswahlordnung deutlich zum Ausdruck käme, daß auch die *Einsichtnahme* in das Wählerverzeichnis (manuell und automatisiert) nur durch *Wahlberechtigte* (der jeweiligen Gemeinde) zulässig ist, soweit dies im Zusammenhang mit der Prüfung des Wahlrechts einzelner bestimmter Personen steht. Diese Voraussetzungen wären vom zuständigen Personal insbesondere dann zu prüfen, wenn im Melderegister die o. a. Auskunftssperre gespeichert ist.

   Bei Verstößen gegen den vorgesehenen Zweckbindungsgrundsatz, der auch für die *Einsichtnahme* ins Wählerverzeichnis gelten muß, und das Verbot der Weitergabe der Auszüge aus dem Wählerverzeichnis an Dritte, sind (erforderliche) Sanktionen nicht vorgesehen. Bußgeld- und Strafbewehrung sollten im Landeswahlrecht geregelt werden. Zumindest sollte auf die entsprechende Anwendbarkeit der §§ 32 f. SächsDSG hingewiesen werden.

3. Die Möglichkeit, noch am Wahltag bis $15.^{00}$ Uhr bei *"nachgewiesener"* plötzlicher Erkrankung einen Wahlschein beantragen zu dürfen, darf nicht von der Vorlage einer ärztlichen Diagnose oder Anamnese abhängig gemacht werden. Anstelle des Wortes "nachgewiesen" sollte "glaubhaft gemacht" verwendet werden. Jedenfalls reicht ein (ärztliches) Zeugnis darüber, daß (und nicht: warum) der Wähler nicht transportfähig ist.

4. Die Gemeindebehörde darf für jeden Wahlberechtigten die Bescheinigung des Wahlrechts nur *einmal* zu *einem* Wahlvorschlag erteilen; dabei darf sie nicht festhalten, für *welchen* Wahlvorschlag die erteilte Bescheinigung bestimmt ist.

   In den alten Bundesländern wurde immer wieder festgestellt, daß sich die Wahlbehörden zum Nachweis der erteilten Bescheinigungen Kopien der bescheinigten Wahlvorschläge anfertigten. Deshalb sollte die entsprechende Bestimmung wie folgt gefaßt werden:
   "dabei darf sie nicht festhalten (auch nicht durch Kopien des bescheinigten Wahlvorschlags), für welchen Wahlvorschlag die erteilte Bescheinigung bestimmt ist."
   Zum Nachweis, daß eine Unterschrift bereits bescheinigt wurde, könnte die Wahlbehörde die Unterzeichner in eine manuell geführte Liste oder Kartei eintragen oder besser noch in einem alphabetischen Verzeichnis aller Wahlberechtigten (z. B. durch Abhaken) kennzeichnen.

   Ein zwingendes Gebot des Datenschutzes ist es außerdem, daß nach Ablauf der Frist für die Einreichung der Unterstützungslisten beim Landeswahlleiter *alle* Aufzeichnungen in der Gemeinde *gelöscht* werden.

Falls nicht in der Landeswahlordnung selbst, so sollten diese Gesichtspunkte zumindest in einer für die Wahlbehörden bestimmten Wahlanweisung deutlich herausgestellt werden.

5. Die Landeswahlordnung sieht vor, daß lediglich der *Name* (= Familienname) der gewählten Bewerber öffentlich bekanntgegeben werden muß. Nach einer weiteren Bestimmung ist öffentlich bekanntzugeben, *welcher* Bewerber in den Sächsischen Landtag eingetreten ist.
   Ich habe vorgeschlagen, die öffentlich bekanntzugebenden Daten *abschließend* in der Landeswahlordnung aufzuzählen.

Ich hoffe, daß sich der Verordnungsgeber von diesen Argumenten überzeugen läßt.

5.4.2 Überprüfung von Wahlrechtsdaten

Im Hinblick auf die kommenden Wahlen stehen in den neuen Bundesländern die zuständigen Wahlbehörden vor dem Problem, Ausschlüsse vom Wahlrecht oder der Wählbarkeit anhand ihrer Unterlagen nur unvollständig feststellen zu können.
Hintergrund ist, daß die Meldebehörden der neuen Bundesländer ihre Einwohnerdaten ohne Hinweise darüber bekommen haben, ob jemand aufgrund vor dem 3. Oktober 1990 ergangener gerichtlicher Entscheidung vom aktiven oder passiven Wahlrecht ausgeschlossen war. Nach diesem Termin wurden gerichtliche Entscheidungen über Wahlrechtsausschlüsse seitens der Justizverwaltungen den Meldebehörden nach Nummer 12 a der Mitteilungen in Strafsachen (MiStra) nur unzureichend mitgeteilt. Daher fehlen in den neuen Bundesländern genaue Angaben über aktuelle Wahlrechtsausschlüsse. Daraus könnten sich bei den kommenden Wahlen 1994 Wahlanfechtungen und Wahlwiederholungen ergeben.

Eine sicherere Beurteilung könnte nur anhand der im Bundeszentralregister eingetragenen Vorstrafen der Wahlberechtigten vorgenommen werden. Das Bundeszentralregistergesetz (BZRG) in seiner geltenden Fassung bietet allerdings keine ausreichende Rechtsgrundlage für die Übermittlung der Führungszeugnisse *aller* Wahlberechtigten. Nur im Einzelfall kann einer Behörde nach § 31 BZRG das Führungszeugnis übermittelt werden, soweit die Behörde es zur Erledigung ihrer hoheitlichen Aufgaben benötigt und eine Aufforderung an den Betroffenen, ein Führungszeugnis vorzulegen, nicht sachgemäß ist oder erfolglos bleibt. § 31 BZRG kommt somit als Rechtsgrundlage für einen Abgleich der Melderegister nicht in Betracht.
Aus diesem Grunde sah ein aus der Mitte des Bundestages kommender Gesetzentwurf zur Änderung des Bundeszentralregistergesetzes vom 8. November 1993 vor, daß die Innenministerien der fünf neuen Bundesländer und Berlins beim Bundeszentralregister Führungszeugnisse der wahlberechtigten Bürger anfordern können. Gegen diesen Gesetzentwurf wurden seitens des Bundesbeauftragten und der Landesbeauftragten für den Datenschutz erhebliche Bedenken erhoben, weil er ihrer Auffassung nach gegen das verfassungsmäßige Gebot der Verhältnismäßigkeit verstieß: Der Millionenzahl der den Innenressorts der Länder zu erteilenden Registerauskünfte stünden eine kleine Zahl von Auskünften mit Wahlrechtsrelevanz gegenüber. Auch mußte bezweifelt werden, ob die Innenressorts die ihnen zugedachte Filterfunktion in dem vom Gesetzentwurf

vorgesehenen Umfang überhaupt leisten könnten oder - unter dem Gesichtspunkt des Persönlichkeitsschutzes noch bedenklicher - auf die örtliche Ebene (Landratsämter) verlagern dürften. Aufgrund dieser Kritik wurde durch den Bundesbeauftragten für den Datenschutz, das Bundesministerium der Justiz und den Generalbundesanwalt - Dienststelle Bundeszentralregister - ein neuer Vorschlag zur BZRG-Änderung erarbeitet. Dieser sieht vor, bereits beim Bundeszentralregister diejenigen Informationen herauszufiltern, die einen Wahlrechtsbezug haben. Besteht ein Ausschluß des *aktiven* Wahlrechts nach § 45 Abs.5 StGB, wird allein dieses Datum vom Bundeszentralregister übermittelt. Seitens des Bundeszentralregisters ist dies technisch möglich, da der Ausschluß des aktiven Wahlrechts richterlich angeordnet wird (§ 45 StGB) und der Ausschluß als Nebenfolge im Tenor eines Urteils erscheint. Nach dem Entwurf werden die Auskünfte sodann vom Bundeszentralregister direkt an die zuständigen Meldebehörden weitergeleitet. Der Verlust des *passiven* Wahlrechts tritt automatisch bei einer Verurteilung wegen eines Verbrechens zu einer Freiheitsstrafe von mehr als einem Jahr ein. Diese strafrechtliche Nebenfolge erscheint nicht in allen Fällen im Urteilstenor und kann somit nicht als Einzeldatum übermittelt werden. Um zu vermeiden, daß die Meldebehörden umfassende Bundeszentralregisterauszüge erhalten, sollen diese von den Innenministerien auf bestehende Wahlausschlüsse überprüft werden. Bei Vorliegen eines Ausschlusses wird dann nur dieses Datum an die Meldebehörden übermittelt.
Der neue Gesetzentwurf soll noch im März 1994 im Bundesrat beraten werden.

5.5 Kommunale Selbstverwaltung

5.5.1 Verpflichtung von Gemeinderatsmitgliedern auf das Datengeheimnis

Wiederholt wurde gefragt, ob Gemeinderatsmitglieder auf das Datengeheimnis nach § 6 SächsDSG zu verpflichten sind.
Hierzu vertrete ich folgende Auffassung: Gemeinderatsmitglieder sind zwar nicht Beschäftigte im Rahmen eines Dienstverhältnisses, sondern Mandatsträger, deren Rechtsstellung sich grundsätzlich von der Rechtsstellung aller Angehörigen des öffentlichen Dienstes unterscheidet. Nach § 35 Abs. 3 SächsGemO üben sie ihr Mandat nach dem Gesetz und ihrer freien, dem Gemeinwohl verpflichteten Überzeugung aus. Sie sind an Aufträge und Weisungen, durch die diese Freiheit beschränkt würde, nicht gebunden. Sie schulden damit rechtlich keine Dienste, sondern nehmen unabhängig ihr Mandat wahr (so das Bundesverfassungsgericht in seiner Entscheidung in BVerfGE 40, 296, 316 in Bezug auf Abgeordnete). § 6 Abs. 1 SächsDSG stellt jedoch nicht auf ein arbeits- oder dienstrechtliches Beschäftigungsverhältnis ab, sondern auf die faktische Beschäftigung bei der Datenverarbeitung. Der Gesetzeswortlaut macht deutlich, daß sämtliche Personen erfaßt sein sollen, deren Aufgabengebiet sie mit personenbezogenen Daten in Verbindung bringt.

Gemeinderatsmitglieder, die in vielen Fällen zudem Ausschüssen angehören, erfahren häufig schutzwürdige personenbezogene Daten. Sie müssen deshalb nach § 6 Abs. 2 SächsDSG über ihre Pflicht zur Verschwiegenheit nach §§ 41 Abs. 5, 43 Abs. 3 i. V. m. § 37 Abs. 2 SächsGemO belehrt werden.

Eine Belehrung der Gemeinderatsmitglieder nach § 6 Abs. 1 SächsDSG steht nicht ihrer

Unabhängigkeit nach § 35 Abs. 3 SächsGemO entgegen, da sie ihr Mandat nach dem Gesetz ausüben müssen und ihnen durch die Belehrung keine neuen Pflichten auferlegt, sondern sie nur auf ihre kraft Gesetzes bestehenden Pflichten hingewiesen werden.

Ich halte es für sinnvoll, wenn die Verpflichtung auf das Datengeheimnis vom Bürgermeister vorgenommen wird. Dies hätte gegenüber einer Verpflichtung durch Bedienstete der Gemeindeverwaltung den Vorteil, daß der Eindruck vermieden wird, es werde in die Unabhängigkeit der Gemeinderatsmitglieder eingegriffen. Die Verpflichtung auf das Datengeheimnis durch den Bürgermeister könnte gleichzeitig mit der Verpflichtung der Gemeinderäte auf die gewissenhafte Erfüllung ihrer Pflichten nach § 35 Abs. 1 SächsGemO erfolgen.

5.5.2 Weitergabe der Privatanschriften von Kreistagsmitgliedern an Dritte

Eine Anfrage, ob die Weitergabe und damit das Bekanntwerden der Privatanschriften von Kreisräten eine Verletzung des Datenschutzes darstellt, konnte ich nicht ohne weiteres bejahen.
Soweit z. B. wahlrechtliche Vorschriften eine Veröffentlichung von Wahlbewerberdaten einschließlich der Wohnanschrift vorsehen, wird dies nicht zu beanstanden sein. Das gleiche gilt auch für die Veröffentlichung der Wahlergebnisse. Jeder Interessent hat natürlich die Möglichkeit, sich aus diesen öffentlichen Quellen mit den Informationen zu versorgen, um sie später für seine Zwecke (z. B. Versand von Werbesendungen) zu nutzen.
Für unzulässig und mit Art. 33 SächsVerf sowie mit § 1 SächsDSG nicht vereinbar halte ich es aber, wenn sächsische Behörden durch die Übermittlung wahlrechtlicher Daten an Dritte für kommerzielle oder sonstige Zwecke an einer *Zweckentfremdung* der Wahlbewerberdaten beziehungsweise der Daten von Gewählten durch Bekanntgabe der *Privatanschriften* mitwirken würden. Auch kommunale Mandatsträger (und ihre Familien) haben ein Recht, zu Hause in Ruhe gelassen zu werden.
Eine solche Datenübermittlung wäre nur mit Einwilligung der Betroffenen zulässig (vgl. § 4 Abs. 1 Nr. 2 und Abs. 2 und 3 SächsDSG). Dies gilt auch für Broschüren (sog. Behördenführer), in denen nach meinen Erfahrungen außer den Anschriften von Behörden und öffentlichen Einrichtungen oftmals auch Namen und Wohnanschriften der Kreis- und Gemeinderäte enthalten sind.
Bezüglich der *Namen* der kommunalen Mandatsträger tritt aber m. E. das Recht auf informationelle Selbstbestimmung zurück. Kreisräte sind nämlich Persönlichkeiten des öffentlichen Lebens mit einem "verkürzten" Persönlichkeitsschutz. In ihrer politischen Funktion müssen sie auch für die Bürger und ihre Wähler erreichbar sein. Hierzu ist allerdings die Privatadresse nicht erforderlich, weil die Kreisräte über die Anschrift des Landratsamtes erreichbar sind.

5.5.3 Veröffentlichung von Grundeigentümerdaten in gemeindlichen Mitteilungs-blättern bei Straßenumbenennungen

In einem Mitteilungsblatt einer Gemeinde im Freistaat wurden im Zuge der Straßenumbenennung "zur besseren Orientierung im Ortsgebiet" u. a. die Namen der Grundeigentümer veröffentlicht.

Diese Datenübermittlung an die Leser des kommunalen Mitteilungsblatts war unzulässig, weil die Gemeinde es unterlassen hatte, von den Betroffenen zuvor eine schriftliche Einwilligung einzuholen. Gemäß § 4 Abs. 2 SächsDSG hätten die Betroffenen darüber hinaus vor der Veröffentlichung auf den Zweck der Datenübermittlung sowie auf das Recht zur Verweigerung der Einwilligung hingewiesen werden müssen. Ich habe die Gemeinde auf die Unzulässigkeit der Veröffentlichung hingewiesen.

5.5.4 Bildung eines Bewertungsausschusses aus der Mitte des Kreistages zur Überprüfung der Kreistagsmitglieder und der Landkreisbediensteten auf "Stasi"-Vergangenheit

Zur Frage, ob und gegebenenfalls unter welchen Voraussetzungen aus der Mitte des Kreistages ein Bewertungsausschuß zur Überprüfung der Kreistagsmitglieder und der Landkreisbediensteten auf "Stasi"-Vergangenheit gebildet werden darf, habe ich wie folgt Stellung genommen:

Die Sächsische Landkreisordnung läßt in § 39 die Bildung eines beratenden Ausschusses durch den Kreistag zu, dem u. a. die *Vorberatung* für Personalentscheidungen im Hinblick auf eventuelle "Stasi"-Belastungen auch der Kreisbediensteten übertragen werden kann. Der Landrat hat das Recht, an den Sitzungen des Ausschusses teilzunehmen, sofern er nicht selbst den Vorsitz führt. Die Sitzungen des Ausschusses sind nichtöffentlich.

Der Kreistag (mindestens 1/4 der Kreisräte) kann verlangen, daß der Landrat dem Ausschuß *Akteneinsicht* gewährt (§ 24 Abs. 4 LKrO). Die Ausschußmitglieder sind (wie alle Kreisräte und der Landrat) gemäß § 33 Abs. 2 LKrO zur Verschwiegenheit über alle im Ausschuß behandelten Angelegenheiten so lange verpflichtet, bis der Kreistag sie im Einvernehmen mit dem Landrat von der Schweigepflicht entbindet. Die Personalentscheidung selbst (Entlassung, Abstufung, Nichtentlassung) erfolgt dann durch den Kreistag im Einvernehmen mit dem Landrat (§ 24 Abs. 3 LKrO) beziehungsweise durch besondere Regelungen im Rahmen der Hauptsatzung.

Es ist deutlich zu machen, daß der Kreistag *aus seiner Mitte* den Bewertungsausschuß bildet. Z. B. wäre ein Beschluß "...bestehend aus je einer Person einer jeden Partei und Bürgerbewegung ..." rechtswidrig, da Ausschußmitglieder nur Mitglieder des Kreistages sein können (§§ 39 Abs. 2, 38 Abs. 1 LKrO).

Auch ein etwa vorgesehenes "Öffnen" und "Bekanntgeben" der zu erwartenden Antworten würde den Bestimmungen der Landkreisordnung widersprechen. Aktenverwaltende Stelle ist der Landrat (§ 49 LKrO). Er muß dem Bewertungsausschuß

allerdings unter den oben angegebenen Voraussetzungen *Akteneinsicht* gewähren (§ 24 Abs. 4 LKrO). Das Abholen oder Entgegennehmen der Überprüfungsergebnisse von der Gauck-Behörde, das "Öffnen" sowie die "Bekanntgabe" sind ausschließlich Angelegenheiten der Kreisverwaltung, die vom Landrat geleitet wird.

Wegen der Veröffentlichung eventuell aufgrund "Stasi"-Belastung entlassener Personen verweise ich auf Nr. 5.5.3 meines 1. Tätigkeitsberichts.

5.6 Baurecht / Wohnungswesen

5.6.1 Unterrichtung des Bauherrn durch die Bauaufsichtsbehörde über einen eingelegten Widerspruch gegen die Baugenehmigung

Auf Grund einer Eingabe hatte ich mich mit der Frage zu befassen, ob eine Bauaufsichtsbehörde berechtigt ist, dem Bauherrn Namen und Anschrift des Widerspruchsführers (Nachbar) mitzuteilen.

Grundsätzlich ist hierzu zu sagen, daß die Bauaufsichtsbehörde Nachbarn, d. h. Eigentümer von Grundstücken in unmittelbarer Nähe zum Baugrundstück, im Genehmigungsverfahren gemäß § 13 Abs. 2 Satz 2 VwVfG (anwendbar gemäß § 1 des vorläufigen Verwaltungsverfahrensgesetzes des Freistaats Sachsen) *notwendig hinzuziehen* muß. Nach der Beiladung sind die "Hinzugezogenen" *Beteiligte am Verwaltungsverfahren* mit allen Verfahrensrechten (z. B. Recht zur Antragstellung, Anhörung). In diesem Fall werden selbstverständlich Name und Anschrift der Beteiligten bekannt.
Legt ein am Verfahren bislang nicht Beteiligter (z. B. weil seine "Hinzuziehung" unterblieben ist) gegen eine Baugenehmigung Widerspruch ein, ist die Bauaufsichtsbehörde zur nochmaligen Überprüfung der Sach- und Rechtslage verpflichtet, um entscheiden zu können, ob sie die erteilte Baugenehmigung aufgrund des Widerspruchs ändert, aufhebt (also abhilft) oder ob sie den Vorgang der Widerspruchsbehörde vorlegt. Bevor die Behörde eine solche Entscheidung trifft, hat der Bauherr gemäß § 71 VwGO ein Anhörungsrecht (vgl. zum Umfang von Anhörungsrechten 1. Tätigkeitbericht, 5.1.9), da die erneute Entscheidung der Bauaufsichtsbehörde für ihn ungünstig sein kann (z. B. Aufhebung der erteilten Baugenehmigung). Im Anhörungsverfahren soll dem Bauherrn Gelegenheit gegeben werden, sich zu dem eingelegten Widerspruch in tatsächlicher und rechtlicher Hinsicht zu äußern. Es dient also "der Verteidigung". Die Bauaufsichtsbehörde muß daher dem Bauherrn *alle* Tatsachen mitteilen, die *entscheidungserheblich* sein könnten. Hierzu gehört unter anderem auch die Bekanntgabe des Namens und der Anschrift des Widerspruchsführers: Die Kenntnis des genauen Wohnorts eines Widerspruchsführers hat Bedeutung für die Frage, ob dieser überhaupt *befugt* war, Widerspruch zu erheben. Dies ist nämlich nur dann der Fall, wenn der Widerspruchsführer durch das Bauvorhaben *unmittelbar betroffen* ist, er also wirklich Eigentümer eines Grundstücks "in der Nachbarschaft" ist. Verwaltungsverfahren sind grundsätzlich *offene* Verfahren. Nur so wird Art. 19 Abs. 4 GG (Art. 38 SächsVerf), also die Rechtsschutzgarantie, mit Leben erfüllt.

5.6.2 Stellungnahme zum Entwurf eines Sächsischen Architektengesetzes

Wieder einmal wurde ich entgegen § 13 Abs. 5 Satz 4 GeschoSReg nicht rechtzeitig am Gesetzgebungsverfahren beteiligt. Der Entwurf des Sächsischen Architektengesetzes wurde mir erst zugeleitet, als die erste parlamentarische Beratung unmittelbar bevorstand. Daher war ich gezwungen, meine Stellungnahme sehr rasch zu erarbeiten und direkt den mit dem Entwurf befaßten Ausschüssen für Bau und Verkehr sowie Wirtschaft und Arbeit zuzuleiten. Die weiteren Beratungen, an denen ich teilnehmen werde, sind derzeit noch nicht abgeschlossen.

Aus meiner datenschutzrechtlichen Stellungnahme möchte ich drei Änderungsvorschläge hervorheben:

Für unverhältnismäßig habe ich eine Regelung gehalten, wonach die Eintragung eines Bewerbers in die Architekten- oder Stadtplanerliste zu versagen ist, wenn er rechtskräftig wegen einer Straftat verurteilt worden ist und sich aus dem zugrundeliegenden Sachverhalt die Nichteignung zum Architekten- oder Stadtplanerberuf ergibt. Das Gericht hat nämlich die Frage, ob ein Berufsverbot ausgesprochen werden soll (was der Versagung der Eintragung in die Liste gleichkommt), bereits geprüft und entschieden. Ich vermag nicht einzusehen, warum die Architektenkammer eine erneute Prüfung des Sachverhalts im Hinblick auf die Zuverlässigkeit des betroffenen Bewerbers vornehmen soll.

Des weiteren enthielt der Gesetzentwurf keine Regelung darüber, auf welche Weise die im einzelnen aufgeführten Versagungstatbestände ermittelt werden sollen. Beispielsweise war vorgesehen, einem Architekten oder Stadtplaner die Eintragung zu versagen, solange er krankheitsbedingt einzelne Angelegenheiten, die die Berufsausübung betreffen, ganz oder teilweise nicht besorgen kann. Wie diese Voraussetzung festgestellt werden sollte, war nicht geregelt. Ich habe darauf hingewiesen, daß die zur Eignungsprüfung erforderlichen personenbezogenen Daten grundsätzlich beim Betroffenen selbst zu erheben sind und durch konkrete Formulierungsvorschläge zum Ausdruck gebracht, die Offenbarung welcher Daten ich im einzelnen für erforderlich halte (z. B. Vorlage eines ärztlichen Attests).

Außerdem sah der Entwurf für alle Mitarbeiter der Kammer die sogenannte "Gauck-Überprüfung" vor, um feststellen zu können, ob die Mitgliedschaft oder Beschäftigung wegen einer möglicherweise vorliegenden "Stasi-Vergangenheit" *unzumutbar* ist. Die Vorschrift gewährte dem Betroffenen kein *Anhörungsrecht* zu der Frage, welche Konsequenzen aus dem Ergebnis der Überprüfung gezogen werden sollen (z. B. Kündigung, Ausschluß der Wiederwahl). Da nach meiner Auffassung *Anhörungsrechte* unverzichtbarer Bestandteil eines rechtstaatlichen Verfahrens sind und der Sachaufklärung dienen (vgl. 1. Tätigkeitsbericht, 5.1.9), habe ich die Aufnahme eines Anhörungsrechts für die Betroffenen in den Gesetzentwurf angeregt.

5.6.3 Unterrichtung von Anzeigenerstattern im Verfahren nach dem Wohnungsbelegungsgesetz

Nach § 9 Abs. 1 Wohnungsbelegungsgesetz, der nach dem Einigungsvertrag in den

neuen Ländern anzuwenden ist, dürfen kommunale Wohnungen ohne Genehmigung des Wohnungsamtes nicht zu Zwecken einer dauernden Fremdenbeherbergung verwendet oder anderen als Wohnzwecken zugeführt werden. Die Wohnungsämter haben von amtswegen die Einhaltung dieser Vorschrift zu überwachen. Wie mir mitgeteilt wurde, werden den Wohnungsämtern vielfach Hinweise aus der Bevölkerung über eine mögliche Zweckentfremdung gegeben.

Bei einem Besuch in einem Wohnungsamt wurde ich mit der anscheinend gängigen Praxis konfrontiert, Anzeigenerstatter über das weitere Verfahren zu unterrichten (z. B. Verhängung eines Bußgeldes wegen Zweckentfremdung). Diese Verfahrensweise ist gemäß § 15 Abs. 1 Nr. 1, 2 SächsDSG (Übermittlung personenbezogener Daten an nicht-öffentliche Stellen) unzulässig, weil die Unterrichtung des Anzeigenerstatters über das weitere Verfahren weder zur Aufgabenerfüllung des Wohnungsamtes erforderlich ist (Nr. 1) noch anzunehmen ist, daß der Betroffene kein schutzwürdiges Interesse am Unterbleiben der Übermittlung hat (Nr. 2).

Das Wohnungsamt hat zugesagt, die Anzeigenerstatter in Zukunft nicht mehr über den weiteren Verlauf des Verwaltungsverfahrens zu informieren.

5.7 Statistikwesen

Der aus der Sicht des Datenschutzes erfreuliche Verlauf der Vorarbeiten zum Sächsischen Statistikgesetz, über den ich in meinem 1. Tätigkeitsbericht unter 5.7 berichten konnte, hat sich bei der Beratung des Regierungsentwurfes im Innenausschuß fortgesetzt. Dieser hat sämtliche von mir in diesem Stadium des Gesetzgebungsverfahrens zusätzlich gemachten Verbesserungsvorschläge - einstimmig - übernommen, die dann auch in das Gesetz Eingang gefunden haben, das am 15. Juni 1993 in Kraft getreten ist.

Aufgrund des Gesetzes wird sich der Schwerpunkt meiner Arbeit auf den Bereich der *Kommunalstatistiken* verlagern. Gemäß § 8 Abs. 3 SächsStatG ist der Sächsische Datenschutzbeauftragte 'bei der Vorbereitung von Kommunalstatistik-Satzungen *zu beteiligen*'. Ab dem 15. Juni 1995 dürfen auch bereits vor Inkrafttreten des Sächsischen Statistikgesetzes bestehende Kommunalstatistiken nicht mehr ohne eine Satzung als Rechtsgrundlage weitergeführt werden (§§ 25, 8 Abs. 1 SächsStatG). Ich habe ein Muster für eine *'Statistik-Mutter-Satzung'* in Zusammenarbeit mit der Stadt Dresden erarbeitet. (Auf der Grundlage einer solchen Mutter-Satzung können dann in vergleichsweise knapp gefaßten 'Tochter-Satzungen' jeweils die einzelnen kommunalen Statistiken angeordnet werden.) Der Text soll demnächst in geeigneter Form *zur Diskussion gestellt* werden.

5.8 Archivwesen

5.8.1 Gesetzgebung

Am 15. Juni 1993 ist das Archivgesetz für den Freistaat Sachsen in Kraft getreten.
Erfreulicherweise sind die von mir *zugunsten*
- des Schutzes der Belange Betroffener (§ 5 Abs. 7; vgl. auch §§ 6 Abs. 1 und 2,

9 Abs. 2 Nr. 2, 10 Abs. 4 SächsArchG),
- der Möglichkeit der Erforschung des Archivgutes der Rechtsvorgänger des Freistaates Sachsen sowie aus der Zeit vom 8. Mai 1945 bis zum 2. Oktober 1990 (dies bedeutet, daß auch sehr junges Archivmaterial ohne Einhaltung von Schutzfristen ausgewertet werden kann, §§ 10 Abs. 2 S. 2 und 3 i. V. m. 4 Abs. 2 S. 2 und 3 SächsArchG) und
- des Einzelnen, der die ihn betreffenden Archivalien aus dieser Zeit nutzen kann (§ 6 Abs. 3 SächsArchG),

gemachten Vorschläge, die ich ausführlicher im 1. Tätigkeitsbericht unter 5.8 dargestellt habe, in das Gesetz aufgenommen worden.

5.8.2 Archivierung von Altdaten

So erfreulich die Erarbeitung des Sächsischen Archivgesetzes - vor allem am Ende - verlaufen ist, so unbefriedigend sind, wie bereits erwähnt (oben 1.3), bisher die Sonderregelungen in die Wirklichkeit umgesetzt worden, die der Gesetzgeber im Anschluß an § 35 SächsDSG in §§ 4 Abs. 2 S. 2 und 3 sowie 5 Abs. 2 SächsArchG für die Daten aus der Zeit zwischen dem 8. Mai 1945 und dem 2. Oktober 1990 vorgesehen hat.

Ein erster, gemeinsam mit Vertretern des staatlichen Archivwesens und des SMI als dessen oberster Aufsichtsbehörde durchgeführter Besuch bei einem großen Unternehmen der Stahlbranche, von dem Teile privatisiert worden sind und das im übrigen von der Treuhandanstalt abgewickelt wird, hat die Berechtigung meines Drängens bestätigt: Es stellte sich heraus, daß Unterlagen § 35 SächsDSG und dem Archivgesetz zuwider vernichtet oder in Teilen geschwärzt wurden. Außerdem wurde zum Teil der archivrechtlich wichtige Entstehungs- und Überlieferungszusammenhang zerstört.

Hier muß ein Ausgleich mit handels- und steuerrechlichen sowie sozial- und arbeitsrechtlichen Aufbewahrungspflichten der Unternehmen, der Liquidatoren und insbesondere der Treuhandanstalt gefunden werden, die in Dresden solche Unterlagen abgewickelter Unternehmen im sogenannten 'Depot Sachsen' zusammengefaßt hat und, soweit ich erkennen konnte, in Anbetracht der Schwierigkeit der Aufgabe und der begrenzten Mittel zu ihrer Bewältigung vorbildlich verwaltet.

Ich bin weiterhin bereit, das SMI an dieser 'Schnittstelle' zwischen der Altdaten-Sicherung nach § 35 SächsDSG und der Sonderregelung für die Archivierung von Altdaten nach dem Archivgesetz zu unterstützen, erwarte aber, daß die Leitung des Ministeriums dieser Aufgabe größere Aufmerksamkeit als bisher widmet - zumal sich neue Probleme auf diesem Gebiet schon abzeichnen: Der Verbleib der in Kreisarchiven oder noch unarchiviert in den Landratsämtern gelagerten Altdaten im Zuge der Kreisreform. Mit Recht hat der Sächsische Landesbeauftragte für die Unterlagen des Staatssicherheitsdienstes der ehemaligen Deutschen Demokratischen Republik sich dieserhalb bereits an die Staatskanzlei gewandt.

5.8.3 Datenerhebung im Zusammenhang mit der Erteilung von Erlaubnissen zur Benutzung eines kommunalen Archivs

Im Zuge der Überprüfung eines Entwurfes einer Archiv- und Archivbenutzungsordnung

für ein Kreisarchiv ergab sich die Frage, welche Daten von einem Interessenten im Zusammenhang mit der Erteilung der Erlaubnis zur Archivbenutzung erhoben (und gespeichert) werden dürfen.

Entsprechend dem verfassungsrechtlichen Grundsatz der Verhältnismäßigkeit bestimmt § 11 Abs. 1 SächsDSG, daß das Erheben personenbezogener Daten nur zulässig ist, wenn ihre Kenntnis zur Erfüllung der Aufgaben der erhebenden Stelle erforderlich ist. Maßgebend für die Regelung der Benutzung eines Kreisarchivs ist die in § 13 Abs. 1 SächsArchG ausgesprochene Pflicht des Archivs, das Archivgut zu verwahren, zu erhalten und zur allgemeinen Nutzung zu erschließen. Die letztgenannte Aufgabe wird durch § 13 Abs. 3 S. 1 i. V. m. § 9 SächsArchG dahin näher bestimmt, daß jedermann, der ein berechtigtes Interesse glaubhaft macht, das Recht hat, das Archivgut des kommunalen Archivs zu nutzen. Dabei ist gemäß § 9 Abs. 2 S. 1 und 2 SächsArchG die Benutzung einzuschränken oder zu versagen, wenn einer der in der Vorschrift benannten oder sonst ein wichtiger Grund vorliegt.
Mithin dürfen Daten des Benutzers nur insoweit erhoben werden, als dies zur Entscheidung über eine Einschränkung oder Versagung der Benutzung erforderlich ist. Darüber hinaus können gegebenenfalls weitere Daten auf der Grundlage der - als Satzung, § 13 Abs. 3 S. 2 SächsArchG - zu erlassenden Archivordnung erhoben werden, soweit dies zur Erfüllung einer sich aus dieser Archivordnung ergebenden Aufgabe erforderlich und diese mit dem Gesetz und allgemeinen verfassungsrechtlichen Grundsätzen vereinbar ist.

Gegen die Erhebung und gegebenenfalls Speicherung der Daten
- Name, Vorname, evtl. Geburtsname,
- Wohnanschrift,
- Thematik/Zweck der Archivbenutzung sowie
- des Identitätsnachweises

bestehen keine datenschutzrechtlichen Bedenken. Die Erhebung dieser Daten ist erforderlich, um im Einzelfall die Identität des Antragstellers feststellen und aufgrund dessen über eine Einschränkung oder Versagung der Benutzung entscheiden zu können.

Die Erhebung und gegebenenfalls Speicherung des *Geburtstages* wird in den Fällen, in denen dieses Datum nicht schon durch die Führung des Identitätsnachweises (z. B. durch Vorlage des Personalausweises) miterhoben wird, in aller Regel nicht erforderlich und daher aus datenschutzrechtlichen Gründen unzulässig sein: Fälle, in denen sowohl Namens- als auch Anschriftengleichheit zweier verschiedener Benutzer vorliegen, werden äußerst selten sein. Benutzer, von deren kindlichem Alter eine Gefahr für den Erhaltungszustand des Archivgutes ausgehen könnte, sind auch ohne Erhebung des Geburtstages von der Benutzung ausschließbar.

Unzulässig - weil nicht erforderlich - wäre die Erhebung des Merkmales "Tätigkeit", "Beruf" oder ähnliches. Im Falle einer in der Archivordnung vorgesehenen Gebührenbefreiung für nicht Erwerbstätige ist lediglich die Erhebung dieses Merkmals bzw. seines Gegenteils ("erwerbstätig") erforderlich und auch ausreichend.

Es gibt, namentlich in Baden-Württemberg, Archivbenutzungsordnungen, die zusätzlich nach einem gegebenenfalls vorhandenen *Auftraggeber* des Nutzers fragen.
Ich halte diese Frage für im Regelfall unzulässig. Aus dem Gebührenrecht ergibt sich

keine Rechtfertigung einer solchen Datenerhebung. Es gibt keine Veranlassung, die für die Archivbenutzung anfallenden Gebühren in dem Falle eines für einen Auftraggeber tätigen Benutzers statt bei diesem bei dem Auftraggeber zu erheben. Gebührenschuldner ist ausschließlich der unmittelbare Benutzer, nicht dessen Auftraggeber. Es ist nach allgemeinen gebührenrechtlichen Regeln nicht Sache des Archivs, als einer Behörde, sich um das finanzielle Innenverhältnis zwischen Benutzer und Auftraggeber zu kümmern. Darüber hinaus würde die Frage nach einem Auftraggeber des Benutzers womöglich zur Offenlegung eines evtl. aus rechtlichen Gründen gerade geheimzuhaltenden Auftragsverhältnisses veranlassen.

Anderes kann nur in den seltenen Ausnahmefällen gelten, in denen der Benutzer nicht in seiner Person, sondern nur in derjenigen seines Auftraggebers ein berechtigtes Interesse an der Nutzung des Archivgutes (§ 9 Abs. 1 i. V. m. § 13 Abs. 2 S. 1 SächsArchG) nachweisen kann. Nur in diesen Fällen sollte dann dem Benutzer *Gelegenheit gegeben* werden, durch Nennung seines Auftraggebers und Nachweis der tatsächlichen Beauftragung das notwendige berechtigte Interesse nachzuweisen.

5.8.4 Nutzung kommunaler Archive durch den Internationalen Suchdienst Arolsen (ISD)

Die Aufgabe des ISD besteht darin, personenbezogene Informationen über Verfolgte des nationalsozialistischen Regimes zu sammeln. Aufgrund der gesammelten Unterlagen erteilt der ISD Auskünfte über Vermißte, Bestätigungen über Haft, Zwangsarbeit oder Verschleppung der Betroffenen. Die ehemals Verfolgten, ihre nächsten Familienangehörigen oder Rechtsnachfolger sowie die Wiedergutmachungsbehörden benötigen die Auskünfte, um Ansprüche auf Rente oder Entschädigungen geltend machen zu können.

Im Berichtszeitraum fragten wiederholt Kommunen an, ob sie berechtigt seien, dem ISD Ablichtungen von Unterlagen aus dem Kommunalarchiv (z. B. über verfolgte Fremdarbeiter) zu übermitteln oder ob Bedenken dagegen bestünden, daß Mitarbeiter des ISD die Unterlagen vor Ort auswerten.

Die Anfragen habe ich wie folgt beantwortet:

Gemäß § 13 Abs. 3 i. V. m. § 9 SächsArchG hat jedermann, der ein *berechtigtes Interesse* glaubhaft macht, das Recht, das Archivgut des kommunalen Archivs zu nutzen. Angesichts der Aufgaben des ISD, Schicksale von Verfolgten aufzuklären, ist ein berechtigtes Interesse zu bejahen. Allerdings dürfen gemäß § 9 Abs. 2 Nr. 2 SächsArchG für eine uneingeschränkte Nutzung des Archivs keine schutzwürdigen Belange Dritter entgegenstehen. Es bestehen daher keine Bedenken gegen eine Übermittlung der vom ISD gewünschten Unterlagen (Ablichtungen), sofern diese keine personenbezogenen Daten über andere Personen als möglicherweise Verfolgte enthalten. Auch gegen die Auswertung der Unterlagen durch Mitarbeiter des ISD vor Ort ist aus datenschutzrechtlicher Sicht nichts einzuwenden, wenn sichergestellt ist, daß den Mitarbeitern keine Daten anderer Personen als Verfolgter zur Kenntnis gelangen (z. B. Vorhandensein einer eigenen Kartei).

5.9 Fortentwicklung des Landessystemkonzeptes

Das Landessystemkonzept bildet die Grundlage für die Planung und Koordinierung der Informations- und Kommunikationstechnik (IuK) der Ressorts unter Beachtung ressortübergreifender IuK-Verfahren. Die wirtschaftliche Beschaffung (und Wartung) von Hard- und Software und die Festlegung ressortübergreifender Schnittstellen soll den sparsamen Einsatz der Mittel gewährleisten. Dazu muß der IuK-Bedarf für ressortübergreifende Verfahren ermittelt und anhand einer Kosten-Nutzen-Analyse entschieden werden, ob ein landesweites Datennetz installiert werden soll.
Bereits im 1. Tätigkeitsbericht (1.1.5 und 5.9) habe ich meine schwerwiegenden Bedenken gegen flächendeckende Vernetzungen der Verwaltung angekündigt. Zu diesem Zeitpunkt wurde der Gesellschaft für Mathematik und Datenverarbeitung (GMD) der Auftrag für eine Studie zum Landessystemkonzept (später als IT-Rahmendefinition bezeichnet) übertragen.
Im April 1993 stellte die GMD den Entwurf dieser Studie vor. Wesentliche Schwerpunkte der Studie waren:
- Analyse der Ausgangssituation,
- Schwachstellenanalyse,
- Erarbeitung von Empfehlungen,
- Entwurf einer "Richtlinie für die Koordination des Einsatzes und der Planung von IuK-Anwendungen in der Landesverwaltung des Freistaates Sachsen".

Die endgültige Fassung der GMD-Studie vom Juli 1993 analysierte die Planung und den Einsatz der IuK-Technik und gab Empfehlungen für das weitere Vorgehen. Sie kam zwar zu dem Ergebnis, daß nur eine ressortübergreifende Koordinierung von IuK-Planung und -Einsatz Fehlinvestitionen verhindern könne, gab aber keine ausreichenden Vorgaben, um ein Landessystemkonzept entwickeln zu können.
In meiner Stellungnahme zu der Studie bemerkte ich folgendes:

° Die Kommunikationsbezüge zwischen den jeweiligen Ressorts und ihren nachgeordneten Dienststellen sind nur bruchstückhaft erfaßt.

° Die Studie gibt keine Auskunft über die Datenmengen, Häufigkeit der Übertragungen und Sensitivität der Daten (Eingriffstiefe in das Persönlichkeitsrecht). Folglich ist der aktuelle und der zu erwartende Informationsbedarf nicht analysiert. Damit fehlt die grundlegende Voraussetzung zur Entscheidungsfindung für ein landesweites Datennetz.

° Es wird nicht ausreichend beachtet, daß jeder Informationsaustausch personenbezogener Daten einer gesetzlichen Grundlage bedarf.

° Der Entwurf weist zwar auf die Problematik der IT-Sicherheit hin, er fordert aber kein Datenschutz- und Datensicherheitskonzept.

° Die Aufstellung einer Risikoanalyse zur Informationssicherheit wird im Entwurf nicht gefordert. Sie muß aber unabhängig davon, ob ein Landesnetz oder ressortinternes Netz geplant ist, erstellt werden, denn nur eine Analyse möglicher Gefährdungen bildet die Voraussetzung, konkrete Sicherheitsmaßnahmen festlegen zu können.

° Aus Sicht des Datenschutzes ist vom SMI ein Datenschutz- und Datensicherheitskonzept für ein landesweites Datennetz oder für ressortübergreifende Datennetze in Auftrag zu geben.

Weil die GMD-Studie keine tragfähigen Aussagen zur Entwicklung eines Landessystemkonzeptes enthielt, wurde ein Arbeitsstab unter Leitung des Abteilungsleiters 1 im SML gebildet, der einen Bericht für den weiteren Ausbau und Einsatz der Informationstechnologie (IT), die alle Formen der Informationsverarbeitung, Kommunikation und Nachrichtentechnik einschließt, erarbeitet hat. Dieser Bericht stellt fest, daß in den Bereichen der Planung, des Einsatzes der Informationstechnik, der Bearbeitung von Grundsatzfragen, der Einbeziehung neuer Entwicklungen sowie der Schulung der Bedarf an ressortübergreifender Koordinierung nicht durch die geringen personellen Ressourcen der Landesverwaltung gedeckt werden könne. Dafür sei eine ressortunabhängige Beratungsstelle für Informationstechnik einzurichten. Wesentliche Aufgaben dieser Beratungsstelle sollten sein :

°Entwicklung und Fortschreibung der IT-Rahmendefinition in Zusammenarbeit mit den Ressorts und Beratung durch den Sächsischen Datenschutzbeauftragten,
°Definition von Standards für Hard- und Software,
°Beratung der Ressorts bei Planung und Durchführung von IT-Vorhaben,
°Registrierung der laufenden und geplanten IT-Vorhaben,
°Erarbeitung von Empfehlungen und Richtlinien zur Privatisierung der IT und
°Erstellung eines jährlichen Berichts über die Informationstechnik.

Dieser Bericht wurde der Staatsregierung als Vorschlag "zur Entwicklung von Rahmendefinitionen zum Einsatz der Informationstechnik in der Verwaltung des Freistaates Sachsen" vorgelegt. Die Staatsregierung nahm diesen Vorschlag auf und beschloß:

°Für den weiteren Aufbau einer leistungsfähigen und wirtschaftlichen Verwaltung moderne Informationstechnik zur Bearbeitung von Verwaltungsabläufen einzusetzen,
°einen Koordinierungsausschuß für die wirtschaftliche Beschaffung und Wartung von Hard- und Software und für einen effektiven Datenaustausch einzurichten,
°eine Beratungsstelle für Informationstechnik einzusetzen, die den Koordinierungsbedarf bei ressortübergreifenden Verfahren feststellen und Standardisierungsrichtlinien für die Informationstechnik und Datenaustauschformate festlegen soll,
°Ist- und Soll-Bedarfspläne für Informationstechnik durch die Ressorts unter Beachtung vorgegebener Vertragsmuster und Definitionen erstellen zu lassen,
°den Bedarf und die Kosten für ein "Landesdatennetz" zu ermitteln und Modellversuchsnetze innerhalb der Telekommunikations-Anlage (TK-Anlage) der Sächsischen Staatsregierung durch das SMI errichten zu lassen. Dabei sollen schon bestehende Kommunikationswege genutzt werden. Ein Modellversuchsnetz soll die Datenübermittlung zwischen der TK-Anlage der Sächsischen Staatsregierung und den drei Regierungspräsidien realisieren, ein weiterer Modellversuch soll die TK-Anlage zur Datenübermittlung zwischen den obersten Landesbehörden nutzen, um Dienste wie Electronic Mail (mit dem Protokoll X.400), dpa-Informationen, JURIS und statistische Informationssysteme nutzen zu können. Die Rahmenbedingungen für diese Modellnetze sollen mit mir beraten werden.

Zur Zeit befinden sich diese Modellversuche in der Testphase, so daß erst im nächsten Tätigkeitsbericht darüber informiert werden kann, ob sie erforderlich, effektiv, billig und erfolgreich waren. Ich habe dazu erhebliche Bedenken.

Der Einsatz moderner IuK-Technik zur Verbesserung der Verwaltungstätigkeit muß sich an den rechtlichen Vorgaben orientieren und Forderungen des Datenschutzes und der Datensicherheit beachten. Ressortübergreifende Netze dürfen nur dann eingerichtet werden, wenn sie zur Erfüllung konkreter Aufgaben erforderlich sind und eine klare gesetzliche Grundlage besteht. Allerdings bestehen bei mir noch grundlegende Zweifel an der Sinnhaftigkeit und am "angedachten" Volumen eines Landesdatennetzes. Entscheidungen im Bereich der Informationstechnologie haben wesentlich größere Auswirkungen als selbst die Beteiligten gemeinhin annehmen. Die finanziellen, organisatorischen und gesellschaftspolitischen Folgelasten sind immens. Dementsprechend sorgfältig müssen Entscheidungen begründet sein. Dies ist allerdings für mich noch nicht sichtbar: Eine Bedarfsanalyse, für die das SMI verantwortlich ist, liegt bisher nicht vor und ist auch in Ansätzen nicht erkennbar. Der Ist-Stand und der von den Ressorts angegebene Soll-Stand stellen dafür keine ausreichende Grundlage dar. Auch ein Datenschutz- und Datensicherheitskonzept fehlt.
Ich werde immer wieder diese grundlegenden Voraussetzungen und Forderungen anmahnen.

5.10 Polizei

5.10.1 Polizeigesetz

Über die Entwurfsarbeiten zur Novellierung des Sächsischen Polizeigesetzes, die in erster Linie in der Ergänzung um bereichsspezifische Datenverarbeitungsregelungen besteht, habe ich in meinem 1. Tätigkeitsbericht (unter 5.10.1) eingehend berichtet.

Inzwischen liegt ein Gesetzentwurf der Staatsregierung vor, zu dem der Innenausschuß des Sächsischen Landtages am 1. März 1994 Sachverständige unter meiner Beteiligung öffentlich angehört hat.

Trotz frühzeitiger Beteiligung meiner Dienststelle an der Diskussion vorausgegangener Arbeitsentwürfe weist der Entwurf der Staatsregierung aus datenschutzrechtlicher Sicht noch Änderungsbedarf auf:

- Der Entwurf zählt den Schutz der freiheitlichen demokratischen Grundordnung zu den polizeilichen Aufgaben. Dies ist jedoch weniger Aufgabe als *Zweck* polizeilichen Handelns. Ansonsten bestünde Kongruenz mit der Aufgabenzuweisung für das Landesamt für Verfassungsschutz. Eine derartige Aufgabenüberschneidung sollte vom Gesetzgeber nicht gewollt sein, zumal nur polizeitypische Aufgabenbereiche in den folgenden Rechtsvorschriften des Entwurfs aufgeführt sind und die Sächsische Verfassung dem Verfassungsschutz als Geheimdienst polizeiliche Befugnisse verwert. Ich warne vor der Tendenz, polizeiliche und geheimdienstliche Aufgaben oder gar Befugnisse zu vermischen.

- Der Entwurf enthält eine generelle Verweisung auf die Anwendbarkeit des Sächsischen Datenschutzgesetzes für die Polizei. Die damit verbundene Absicht wird von mir grundsätzlich unterstützt; sie macht deutlich, daß die Polizei an die gleichen

Grundregeln gebunden ist wie alle anderen Behörden des Landes.

Gerade im Bereich polizeilicher Datenverarbeitung, die an sich voneinander getrennte Aufgaben, nämlich die Gefahrenabwehr, die vorbeugende Bekämpfung von Straftaten und die Verfolgung begangener Straftaten abzudecken hat, ist es aber notwendig, differenzierte Erhebungs- und Nutzungsbefugnisse zu schaffen, die dem *verfassungsrechtlichen Zweckbindungsgebot* entsprechen: Polizeiliche Daten dürfen nur dann für einen veränderten Zweck genutzt werden, wenn sie auch für den neuen Zweck mit *denselben Methoden erhoben* werden dürften. Weder der Entwurf noch das durch Verweisung anzuwendende Sächsische Datenschutzgesetz berücksichtigen diese Besonderheit polizeilicher Datenverarbeitung.

- Die Begriffsbestimmungen des Entwurfs sehen eine Anzahl unbestimmter Rechtsbegriffe vor, wie z. B. "geeignet, den Rechtsfrieden zu stören", "bedeutende fremde Sachwerte" und "sonst organisiert begangen". Aus datenschutzrechtlicher Sicht wäre es wünschenswert, hier Konkretisierungen vorzunehmen. Zu berücksichtigen ist jedoch, daß ein genauer Straftatenkatalog und eine genaue Begriffsbestimmung des "organisierten Verbrechens" kaum möglich und sachdienlich sein dürften. Denn jede Straftat ist eine schwerwiegende Störung des Rechtsfriedens. Aus Täterpersönlichkeit, Organisation der Täter, Opferpersönlichkeit, Tathäufigkeit, Art der Ausführung und der Art des gefährdeten Rechtsgutes ergibt sich die Bedeutung einer Straftat.

  Keinesfalls darf aber die Verunsicherung der Bevölkerung durch alltägliche Massenkriminalität dazu führen, den Begriff des "organisierten Verbrechens" zu verschleißen und ihn auf jede Absprache von Tätern im Sinne einer Bandenkriminalität anzuwenden. Ich rate deshalb dazu, von "organisierter Kriminalität" nur dann zu sprechen, wenn "der Arm, der Straftaten verhütet und bekämpft, gelähmt wird", wenn also Organe der Polizei, anderer Sicherheitsbehörden oder der Justiz sich systematisch an Straftaten oder ihrer Vertuschung beteiligen. Davon kann in der Bundesrepublik Deutschland nicht die Rede sein. Deshalb ist mit dem Begriff des "organisierten Verbrechens" nur zurückhaltend umzugehen; die derzeitige Unsicherheit der Bevölkerung darf nicht zur schrankenlosen Erweiterung polizeilicher Eingriffsinstrumentarien mit der Begründung mißbraucht werden, Banden - die es seit jeher gibt - seien mit der Mafia gleichzusetzen.

- Der Entwurf eröffnet der Polizei die Möglichkeit, durch verdeckten Einsatz technischer Mittel Aufnahmen und Bildaufzeichnungen in oder aus Wohnungen anzufertigen sowie das gesprochene Wort abzuhören und aufzuzeichnen. Zu diesem in der Öffentlichkeit als "großer Lauschangriff" bezeichneten besonderen Erhebungsmittel bemerke ich folgendes:

  Es ist ein Grundelement des Rechtsstaates, daß es keine Straftatenbekämpfung um jeden Preis gibt; der Zweck heiligt nicht die Mittel. Die Verfassung gebietet es, sowohl den *Kernbereich* (Wesensgehaltsgarantie, Art. 19 Abs. 2 GG) der Grundrechte unangetastet zu lassen als auch bei jedem staatlichen Eingriff in die informationelle Selbstbestimmung und die Privatsphäre den verfassungsimmanenten *Verhältnismäßigkeitsgrundsatz* zu beachten:

- Zur Menschenwürde im Rechtsstaat gehört die Gewißheit, daß die staatliche Gewalt das *Beicht-, Arzt- und Anwaltsgeheimnis* sowie andere gesetzlich geschützte Berufs- und Amtsgeheimnisse, *unangetastet* läßt.
- Staatliche Organe sind ohne Änderung des Grundgesetzes nicht befugt, Straftaten zu begehen: Deshalb dürfen Abhörgeräte (Wanzen) durch Hausfriedensbruch oder Sachbeschädigung nicht installiert werden, es sei denn, es liegt ein übergesetzlicher Notstand im Sinne des § 34 StGB vor. Werden Abhörgeräte in anderer, lediglich auf Täuschung angelegter Weise installiert, dürfte dies nur selten zu dem gewünschten Erfolg führen. (Stichwort: "Hier ist der Gasmann ...")
- Straftätern, um deren Absprachen und Verhalten es meist geht, fällt es leicht, die Wohnung oder den Treffpunkt kurzfristig zu wechseln oder sich außerhalb von Räumen oder auch mit Hilfe von Sprechcodes (meist technisch unterstützt) zu verabreden. Schon für 3000,- DM kann man Geräte erwerben, mit denen sich schnell feststellen läßt, ob im Raum ein Abhörgerät installiert ist.

Aus den vorgenannten Gründen ist deshalb vor der Fehleinschätzung zu warnen, die Erhebung in oder aus Wohnungen sei ein überaus erfolgreiches polizeiliches Mittel. Allerdings werden die potentiellen Straftäter verunsichert. Dies allein rechtfertigt bereits die Befugnis zum Abhören.

Die anderen Bundesländer haben überwiegend Regelungen in ihren Polizeigesetzen, die die heimliche Erhebung von Daten in oder aus Wohnungen lediglich bei Gefahr für Leib oder Leben rechtfertigen. Dies scheint mir wegen der modernen Kooperationsformen von potentiellen Straftätern nicht ausreichend zu sein. Dies bedeutet aber nicht, daß die Wohnung im Sinne des Art. 13 GG insgesamt zur Disposition gestellt werden dürfte. Auch hier ist ein Kernbereich bis auf extreme Ausnahmefälle unangetastet zu lassen. Das Bundesverfassungsgericht betont, daß selbst überwiegende Interessen der Allgemeinheit einen Eingriff in den absolut geschützten Kernbereich privater Lebensgestaltung nicht rechtfertigen können (BVerfGE 34, 238 [245]). Diese Entscheidung gibt nicht nur wertvolle Hinweise zum absolut geschützten Bereich privater Lebensgestaltung, sondern auch zur Abwägung bei der Entscheidung über das heimliche Abhören außerhalb dieses Bereichs. In ihren tragenden Gründen ist die Entscheidung für alle Verfassungsorgane verbindlich, § 31 Abs. 1 BVerfGG.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat daher vorgeschlagen, den in der obergerichtlichen Rechtsprechung weit gefaßten Wohnungsbegriff aufzulösen: Wenn bisher unter diesem Wohnungsbegriff Segelschiffe, Jagdhütten, Tiefgaragen, Gaststätten, Billardräume, Büros, Hotelzimmer etc. erfaßt wurden, so ist dies unbefriedigend: Um einen angemessenen Ausgleich zu schaffen zwischen der Aufgabe des Staates, *Straftaten effizient* vorzubeugen, und dem Schutzanspruch des Bürgers auf Unverletzlichkeit *seines höchst privaten Bereiches*, darf das Abhören und Aufzeichnen des gesprochenen Wortes nur für solche Räume zugelasssen werden, die allgemein zugänglich sind oder beruflichen oder gesellschaftlichen Tätigkeiten dienen und nicht dem besonderen Schutz von Berufs- oder Amtsgeheimnissen unterliegen. Lediglich die *Privatwohnung* sollte *unantastbar* mit der Ausnahme bleiben, daß auch dort der Einsatz besonderer Mittel möglich ist, wenn eine konkrete Gefahr für Leib oder Leben besteht.

Werden "Privatwohnungen" lediglich aus dem Grunde angemietet oder vorgehalten, um dort nicht etwa ein Privatleben zu entfalten, sondern "Verbrechertreffs" abzuhalten, so sind auch derartige *konspirative Wohnungen* ein *geeignetes und erlaubtes Terrain* für die heimliche Datenerhebung durch die Polizei.

Die zur Anordnung der Datenerhebung berufenen Richter bedürfen einer Vorschrift, die es ihnen ermöglicht, ihre Entscheidung am Verhältnismäßigkeitsgrundsatz zu orientieren.

Der Entwurfstext normiert im Regelfall den Richtervorbehalt für die heimliche Datenerhebung. Ohne hinreichenden Grund weicht der Entwurf hiervon ab, wenn das besondere Mittel ausschließlich zum Schutz der bei einem polizeilichen Einsatz tätigen Personen eingesetzt wird. Hierzu ist festzustellen, daß der Richtervorbehalt notwendiges Korrektiv des gravierenden Grundrechtseingriffes durch die staatliche Gewalt ist. Dieser Grundrechtseingriff wird in seiner Intensität nicht geringer, wenn die Maßnahme zum Schutz einer eingesetzten Person durchgeführt wird. Es ist konsequent, auch in diesem Fall grundsätzlich den Richtervorbehalt auszusprechen.

- Im Zusammenhang mit der Ausschreibung von Personen zur polizeilichen Beobachtung erlaubt der Entwurf die zu lang bemessene Befristung der Ausschreibung auf ein Jahr. Kontrollmeldungen im Bereich polizeilicher Beobachtung stellen für sich genommen einen schwerwiegenden Eingriff in das Recht auf informationelle Selbstbestimmung dar. Sie bezwecken und ermöglichen die Erstellung eines Bewegungsbildes über eine Person. Deshalb sollte in möglichst kurzen Fristen die Erforderlichkeit der Aufrechterhaltung einer solchen Maßnahme zu überprüfen sein. Eine Frist von sechs Monaten für die erste Anordnung und die jeweilige Verlängerung ist angemessen. Diese Frist ist auch in anderen Gesetzen üblich und hat sich in der polizeilichen Praxis bewährt.

- Wesentliche Grundlage für die Bewertung der Erforderlichkeit der weiteren Speicherung von Daten ist der Ausgang der jeweiligen polizeilichen Aktionen und eventuell nachfolgender Verfahren. Vor allem Freispruch, endgültige Verfahrenseinstellung oder Nichtbestätigung ursprünglicher Verdachtsmomente sollten deshalb dokumentiert werden. Datenschutzrechtliche Kontrollen in anderen Bundesländern haben ergeben, daß diese Informationen häufig nicht zu den Akten oder zu den Dateien genommen werden. Deshalb ist eine besondere Regelung erforderlich.

- Eine bereichsspezifische Regelung der Datenübermittlung des Polizeivollzugsdienstes an andere öffentliche Stellen fehlt im Entwurf. Offenbar soll hier § 13 SächsDSG greifen.

Es muß bezweifelt werden, daß die pauschale Verweisungsregelung dem besonderen Charakter polizeilicher Datenverarbeitung gerecht werden kann:

Wichtigster Grund der Übermittlung der Daten an andere öffentliche Stellen wird in der Praxis sein, daß die Übermittlung zur eigenen polizeilichen Aufgabenerfüllung erforderlich ist. Darüber hinaus kommt auf der Empfängerseite in erster Linie die

Erfüllung von Aufgaben auf dem Gebiet der Gefahrenabwehr in Betracht. Diese beiden Fallgestaltungen sollten in einer gesonderten Vorschrift normiert werden, die im übrigen absichern müßte, daß gesetzliche Vorschriften, die dem Schutz des Betroffenen dienen, durch die Datenübermittlung nicht unterlaufen werden. So hat auch die Polizei den im Bundeszentralregistergesetz konkretisierten Resozialisierungsgedanken zu beachten. Demgemäß darf die Polizei keinesfalls Auskünfte an Behörden übermitteln, die nicht für die Strafverfolgung zuständig sind, wenn die der Auskunft zugrunde liegende Information aus dem Bundeszentralregister nicht oder nicht mehr zu erhalten wäre.

Auch dürfen durch die Datenübermittlung polizeiliche Aufbewahrungsfristen nicht faktisch unterlaufen werden, indem die empfangende Stelle selbständig eigene, längere Aufbewahrungsfristen festlegt.

Schon aus Gründen der polizeiinternen Fachaufsicht sollte das Gesetz die übermittelnde Stelle dazu verpflichten, jede Übermittlung personenbezogener Daten aktenkundig zu machen.

5.10.2 Bereinigung der DDR-Kriminaldatenbestände

Wie in den anderen neuen Bundesländern hat die Polizei auch im Freistaat Sachsen eine zusätzliche Aufgabe zu bewältigen: Die rechtsstaatlich gebotene Bereinigung der zu DDR-Zeiten angelegten Kriminalakten, die zur Erfüllung aktueller polizeilicher Aufgaben noch weitergeführt werden müssen.

Bei der Anpassung des noch 1989 und 1990 in der DDR eingeführten kriminalpolizeilichen automatisierten "dialogorientierten Recherche- und Auskunftssystems" (DORA) waren zunächst als wichtigste Schritte einzuleiten:
- Löschung der Informationen über "ungesetzlichen Grenzübertritt", Demonstrationsteilnahme im Oktober/November 1989, Antrag auf Übersiedlung,
- Löschung von Datensätzen zu Personen, die aufgrund von Handlungen registriert waren, die nach dem Strafgesetzbuch der Bundesrepublik Deutschland keine Straftatbestände darstellen (z. B. "Verleitung zu asozialer Lebensweise", "Zusammenrottung", "Verfehlung zum Nachteil sozialistischen Eigentums"),
- Löschung der Datensätze, deren Speicherungsgrund kein Strafverfahren war,
- Löschung der Datensätze, denen kein Aktenrückhalt zugrunde lag.

Nach der Planung der sächsischen Polizei sollen die Auskunfts- und Recherchefunktionen des Systems DORA künftig vom "Polizeilichen Auskunftssystem Sachsen" (PASS) übernommen werden, das sich seit dem 1. April 1993 im Probebetrieb befindet. Über die Anwendung dieses Landessystems, das auch in Teilen an das bundesweite INPOL-Verbundsystem angeschlossen ist, habe ich mich anläßlich meines Kontrollbesuchs bei einer Polizeidirektion informiert (vgl. 5.10.5). Bis zur vollständigen Einführung von PASS wird als Übergangslösung zum Nachweis der bereinigten Kriminalakten das PC-Projekt "Erfassung rechtmäßiger Personalien, Unterlagen und Straftaten" (ERPUT) betrieben.

Im Gegensatz zur automatisiert - und daher effektiv und flächendeckend -

durchführbaren Bereinigung des DORA-Bestandes bereitet die Überprüfung der diesem zugrunde liegenden Kriminalaktenbestände Probleme, weil diese Akten nunmehr dezentral bei den Polizeidirektionen gelagert sind und die dortige Personalsituation eine zügige Bereinigung nicht zuläßt, wie ich feststellen mußte.

Aus datenschutzrechtlicher Sicht kommt jedoch der beschleunigten Bereinigung dieser Aktenbestände höchste Priorität zu, waren doch nach den einschlägigen DDR-Bestimmungen Informationen in die Akten aufzunehmen, die rechtsstaatlichen Grundsätzen eklatant zuwiderliefen. Als Beispiele seien erwähnt: Beurteilungen von Hausvertrauensleuten, Beurteilungen des Rates des Bezirks oder des Kreises zur Feststellung der Persönlichkeit des Betroffenen, Straftaten ohne gesetzliche Grundlage (z. B. "Asozialität") sowie Angaben zu "Westfernsehen" sowie zu Hobys und Freizeitinteressen. Akteninhalte dieser Art sind im Hinblick auf die Rehabilitationsinteressen der Betroffenen grundsätzlich nicht zu vernichten; sie sind den Kriminalakten zu entnehmen und sodann zu archivieren.

Das SMI habe ich auf die Dringlichkeit der Bereinigungsarbeiten hingewiesen und als einschlägige Arbeitshilfe für die Polizeidirektionen die umfassenden Richtlinien des Landeskriminalamts Sachsen-Anhalt empfohlen.

Den Fortgang der Aktenbereinigung werde ich überprüfen.

5.10.3 Bereinigung der Fingerabdruckblätter

Seit Dezember 1993 befindet sich das automatisierte Fingerabdruckidentifizierungssystem (AFIS) des Bundeskriminalamtes als bundesweites Netzwerk mit Arbeitsstationen bei den Landeskriminalämtern im Wirkbetrieb. Im Rahmen der Aufbereitung des AFIS-Bestandes waren die vorhandenen bei den Ländern angelegten Sammlungen der Fingerabdruckblätter (FaBl.) durch das Bundeskriminalamt rückwirkend zu erfassen. Hierbei entstanden bei den Landeskriminalämtern der neuen Länder Schwierigkeiten, deren Ursachen in dem noch nicht bereinigten, aus der DDR stammenden Bestand der FaBl. lagen.

Das Landeskriminalamt Sachsen führte zunächst (bis März 1992) eine erste Bereinigung der für den Freistaat Sachsen übernommenen 32.000 FaBl. anhand eines Straftatenkataloges und der Bundes-Richtlinien für die kriminalpolizeilichen Sammlungen durch. Dabei hat es nicht geprüft, ob den FaBl. auch Kriminalakten zugrunde lagen ("Aktenrückhalt").

Die nach dieser ersten Maßnahme übriggebliebenen FaBl. (etwa 15.000) übersandte das Landeskriminalamt im Oktober 1992 dem Bundeskriminalamt.

Veranlaßt durch Zweifel des Bundeskriminalamts an der Qualität der ersten Bereinigungsaktion habe ich das Landeskriminalamt gebeten, zu überprüfen, ob zu jedem FaBl. ein Aktenrückhalt besteht, sowie anhand dieses Kriminalaktenbestandes festzustellen, ob die weitere Speicherung der erkennungsdienstlich erhobenen Information der FaBl. zulässig ist.

Daraufhin nahm das Landeskriminalamt im Oktober 1993 drei Viertel des dem Bundeskriminalamt übersandten FaBl.-Bestandes zur manellen Sichtung wieder zurück. Nach Angaben des Landeskriminalamtes hat diese im November 1993 im wesentlichen abgeschlossene Maßnahme gezeigt, daß nur etwa die Hälfte der zurückgenommenen FaBl. (etwa 6.000) rechtmäßig vorgehalten wird und deren AFIS-Erfassung zur kriminalpolizeilichen Aufgabenerfüllung erforderlich ist.

Wenn auch diese umfangreichen und mit großem Arbeitseinsatz verbundenen Bemühungen des Landeskriminalamtes, die in AFIS einzustellenden Datensätze eingehend zu überprüfen, anzuerkennen sind, so haben meine letzten Stichprobenkontrollen doch gezeigt, daß in Einzelfällen noch immer unzulässig lang bemessene Speicherfristen festgelegt sind. Ich werde deshalb die notwendigen weiteren Bereinigungen aufmerksam verfolgen.

5.10.4 Entwurf eines Ausländerzentralregistergesetzes

Das Bundesministerium des Innern hat einen Entwurf zum Ausländerzentralregistergesetz erarbeitet, damit das bestehende Ausländerzentralregister beim Bundesverwaltungsamt auf die verfassungsrechtlich gebotene gesetzliche Grundlage gestellt wird. Den Entwurf hat das Bundesministerium des Innern im Dezember 1993 den Innenministerien der Länder zur Stellungnahme zugeleitet. Leider hat mich das SMI über den Gesetzentwurf nicht informiert; erst durch eine entsprechende Benachrichtigung des Bundesbeauftragten für den Datenschutz erhielt ich Kenntnis von diesem Gesetzesvorhaben mit ausgeprägtem Datenschutzbezug.

In Stellungnahmen an den Sächsischen Ausländerbeauftragten und das SMI habe ich folgende datenschutzrechtliche Probleme des Gesetzentwurfs hervorgehoben:

Der Entwurf erweitert den Kreis der für eine Speicherung in Frage kommenden Straftatbestände. Speicherungen mit diesem strafrechtlichen Hintergrund waren bislang im Ausländerzentralregister nicht vorgenommen worden. Ausweislich der Gesetzesbegründung soll damit nicht einem ausländerrechtlichen Informationsbedarf, sondern der Kriminalitätsbekämpfung Rechnung getragen werden. Die dafür zuständigen Polizeibehörden verfügen jedoch bereits über umfangreiche Informationsverbundsysteme.

Dem Entwurf zufolge würde mittelbar ein Informationsverbund der Polizei mit den Verfassungsschutzbehörden hergestellt, wobei Polizei wie Verfassungsschutz jeweils zur Direkteingabe, die Polizei zudem auch uneingeschränkt zum Direktabruf berechtigt wäre. Dies widerspräche dem Grundgedanken des § 6 S. 4 BVerfSchG (kein Online-Zugriff von anderen Stellen als Verfassungsschutzbehörden auf das nachrichtendienstliche Informationssystem). Ein solcher Informationsverbund würde mit dem Gebot zur Trennung von Polizei- und Nachrichtendiensten kollidieren. Dieses "Trennungsgebot" hat nach verbreiteter Auffassung Verfassungsrang; auch aus Art. 83 Abs. 3 S. 1 SächsVerf folgere ich dies. Im übrigen würde eine Vernetzung der polizeilichen und nachrichtendienstlichen Informationssysteme mittels AZR auch eine Diskriminierung von Ausländern darstellen, weil sie nicht die ausländerspezifischen Besonderheiten berücksichtigt und daher ohne zureichenden Sachgrund Ausländer

schlechter stellt als Deutsche. Es gibt zwar Straftaten, die nur von Ausländern begehbar sind (Straftaten nach ausländerrechtlichen Vorschriften). Ich halte es aber nicht für überzeugend, wenn nicht genügend differenziert wird zwischen grenzüberschreitend operierenden Tätern und solchen ausländischen Mitbürgern, die im AZR gespeichert sind.

Die Erweiterung der Straftatbestände, die im AZR gespeichert werden, sollte deshalb gestrichen werden. Sofern diese Informationen abweichend von der Entwurfsbegründung auch speziell für Ausländerbehörden von Interesse sein sollten - was jedenfalls aufgrund des Straftatenkatalogs kaum anzunehmen ist (gerade besonders schwere Verbrechen wie Mord und Totschlag fehlen) -, müßte der Informationszugriff jedenfalls auf diese Stellen begrenzt werden. Ein Zugriff - sei es online, sei es im Wege konventioneller Übermittlungen - durch Polizeien und Nachrichtendienste, die ohnehin gesondert ihre eigenen Informationssysteme haben, müßte dazu ausgeschlossen werden.

Der Gesetzentwurf sieht die Möglichkeit vor, daß die Nachrichtendienste am automatisierten Abrufverfahren des AZR teilhaben. Nach den einschlägigen Gesetzen für das Bundesamt für Verfassungsschutz, den Militärischen Abschirmdienst und den Bundesnachrichtendienst ist jedoch die Einrichtung automatisierter Abrufverfahren für die Nachrichtendienste allgemein ausgeschlossen. Eine spezialgesetzliche Regelung im Ausländerzentralregistergesetz, die die Einrichtung eines automatisierten Abrufverfahrens zugunsten der Nachrichtendienste zuließe, müßte mit ganz außergewöhnlichen Umständen begründet werden können. Hierzu trägt die Begründung des Entwurfs jedoch nichts vor. Bereichsspezifische Besonderheiten für eine derartige Regelung sind nicht ersichtlich. Auch im Vergleichsfall des beim Kraftfahrtbundesamt geführten zentralen Verkehrsinformationssystems (ZEVIS) haben die Nachrichtendienste wohlweislich mit § 36 StVG keinen Online-Zugriff erhalten. Ihr Interesse, die Ermittlungsrichtung aus Geheimschutzgründen gegenüber den ersuchten Stellen nicht preisgeben zu müssen, ist im übrigen durch eine entsprechende Vorschrift des Gesetzentwurfs berücksichtigt. Die Ermöglichung der Zulassung zum Abruf in automatisierten Verfahren ist dazu weder erforderlich noch angemessen.

Ich habe das SMI gebeten, meine datenschutzrechtliche Kritik bei der bevorstehenden Beratung des Gesetzesvorhabens im Rahmen der Länderbeteiligung zu berücksichtigen.

5.10.5 Kontrollbesuch bei einer Polizeidirektion

Bei einer Datenschutzkontrolle einer sächsischen Polizeidirektion habe ich - Dank des dort gut geführten Dateien- und Geräteverzeichnisses nach § 10 SächsDSG - mehrere Dateien festgestellt, die zur Aufgabenerfüllung der Dienststelle nicht erforderlich und damit unzulässig waren. Aufgrund meiner Kritik wurden diese Datensammlungen inzwischen aufgelöst, so daß ich nach § 26 Abs. 2 SächsDSG von einer Beanstandung absehen konnte. Hierbei handelte es sich um folgende Dateien:

- In einer Datei "Erfassung rechtsorientierter Jugendlicher" waren - auf inaktuellem Stand - die Personalien von Jugendlichen erfaßt, die der Polizeidirektion ohnehin über eine Abfrage einer Datei des Landeskriminalamtes zur Verfügung standen.

- Eine Datei über eingeleitete und abgeschlossene Bußgeldverfahren war angelegt worden, weil die zuständigen Bußgeldstellen zunächst nicht arbeitsfähig waren und deren Aufgaben von der Polizeidirektion wahrgenommen wurden.

- Bei einem der Polizeidirektion nachgeordneten Polizeirevier wurden die quartalsweise aktualisierten kleinen Meldedaten in Listenform geführt, um außerhalb der Regelarbeitszeit der Meldebehörde (Landratsamt) auf diesen kompletten Datenbestand zugreifen zu können.
  Eine inzwischen in der Meldebehörde getroffene Regelung gewährleistet, daß der ausschließlich im Einzelfall zulässige polizeiliche Zugriff auf Meldedaten außerhalb der Bürozeiten erfolgen kann.

- Zwei Dateien eines Polizeireviers enthielten die Belegungsdaten eines Aussiedlerheimes. Diese Detailinformationen - Name, Geburtsdatum, Staatsangehörigkeit sowie Ankunfts- und Abreisedatum - wurden weder zum Schutz der Heimbewohner noch für Zwecke der Strafverfolgung benötigt. Die Polizeidirektion hatte die Dateien angelegt, um gemäß einer Weisung ihrer Landespolizeidirektion Einsatzunterlagen zur Bekämpfung fremdenfeindlicher Straftaten zu erstellen. In dieser Weisung waren jedoch nur die *Gesamt*zahlen der Heimbelegung angefordert worden.

Darüber hinaus offenbarte die Kontrolle in einem Fall sorglosen Umgang mit sensiblen personenbezogenen Informationen: In einem offenstehenden Abfallcontainer auf dem Hof der Polizeidirektion fanden sich Schriftstücke (Zeugenaussagen und Täterbeschreibungen), die nur grob zerrissen waren. Diesen Sachverhalt hat die Polizeidirektion zum Anlaß genommen, den Bediensteten unter Hinweis auf disziplinarische Konsequenzen nochmals die einschlägigen Hausverfügungen nahezubringen.

Schließlich gibt die Kontrolle Veranlassung, offenbar bestehende strukturelle Defizite der polizeilichen Fachaufsicht anzusprechen. Weder der Polizeidirektion noch der Landespolizeidirektion waren die "Richtlinien für die Bereinigung von Kriminalakten" des Landeskriminalamts Sachsen-Anhalt bekannt. Damit ist augenscheinlich das an das Sächsische Staatsministerium des Innern gerichtete Schreiben des Landeskriminalamtes Sachsen vom 30. August 1993 nicht umgesetzt worden, in dem angekündigt wurde, den Polizeidirektionen die genannte Richtlinie als "zusätzliche Entscheidungshilfe" bei der Kriminalaktenbereinigung (vgl. 5.10.2) zur Verfügung zu stellen.

5.10.6 Weitergabe von Prostituiertendaten von der Polizei an Gesundheitsämter

Wie ich erfahren habe, wurden in Sachsen in einigen Fällen die Personalien von Prostituierten im Rahmen von Polizeikontrollen nach § 19 SächsPolG erfaßt und dem Gesundheitsamt gemeldet .
Nach § 19 Abs. 1 Nr. 2 SächsPolG ist die Polizei befugt, die Identität einer Person

festzustellen, wenn sie sich an einem Ort aufhält, an dem erfahrungsgemäß Personen der Prostitution nachgehen.
Eine weitergehende Befugnis, die Personalien der kontrollierten Prostituierten an die Gesundheitsämter weiterzuleiten, ergibt sich hingegen aus dieser Vorschrift nicht. Befugnisnorm für die Übermittlung der Personalien von Prostituierten ist § 19 des Gesetzes zur Bekämpfung von Geschlechtskrankheiten. Danach haben die Behörden Personen, die sie *in Verwahrung genommen oder vorläufig festgenommen* haben und bei denen der *hinreichende Verdacht einer Geschlechtskrankheit* und der Weiterverbreitung von Geschlechtskrankheiten begründet ist, vor ihrer Freilassung dem Gesundheitsamt zur Untersuchung zuzuführen.
Für eine Übermittlung der Personalien an das Gesundheitsamt muß somit der hinreichende Verdacht einer Geschlechtskrankheit bestehen. Das Ausüben der Prostitution allein kann nicht den Verdacht einer Geschlechtskrankheit und deren Weiterverbreitung begründen. Den Gesundheitsämtern ist es nicht möglich, an die Personalien von Prostituierten zu gelangen, wenn die Voraussetzungen des Geschlechtskrankheitengesetzes nicht vorliegen. Für die Erfüllung ihrer Aufgaben aus § 2 Abs. 1 i. V. m Abs. 2 GeschlKrG, nämlich die Bekämpfung der Geschlechtskrankheiten, sind die Ämter auf *einzelfallbezogene* Datenübermittlung durch die Polizeibehörden angewiesen. Den Polizeibehörden ist es jedoch verwehrt, den Gesundheitsämtern Daten auf Vorrat zu beschaffen. Die Übermittlung der Personalien von Prostituierten durch Polizeidienststellen an die Gesundheitsämter ist daher nur unter den engen Voraussetzungen des § 19 GeschlKrG zulässig.

Auf diese Rechtslage habe ich das SMI hingewiesen.

5.10.7 "Präventionsrat" zur Kriminalitätsbekämpfung gegründet

Einer Presseveröffentlichung habe ich entnommen, daß sich im November 1993 in einer sächsischen Kreisstadt ein "Präventionsrat" auf Initiative des Landrates und der örtlichen Polizeidirektion unter Beteiligung der Kirche und des Kinder- und Jugendschutzbundes gebildet hatte.

Zur Kriminalitätsbekämpfung auf "gesamtgesellschaftlicher Basis" wollen die Initiatoren neue Wege kommunaler Kriminalprävention gehen, um im Ergebnis das "subjektive Sicherheitsgefühl der Bevölkerung" zu erhöhen. Hierzu ist geplant, Straftaten zu analysieren, polizeiliche Lagebilder auszuwerten und die Idee der "Nachbarschaftswache" ("Neighbourwatch") zu verfolgen - allesamt Vorhaben mit ausgeprägtem Datenschutzbezug. Dabei ist insbesondere von Bedeutung, inwieweit im Rahmen der Tätigkeit des "Präventionsrates" polizeiliche Erkenntnisse an die beteiligten Mitglieder weitergegeben werden.

Zu dieser Frage habe ich das SMI um Stellungnahme gebeten. Schon jetzt weise ich darauf hin, daß eine gesetzliche Grundlage für die Einbeziehung "gesellschaftlicher Kräfte" in die Polizeiarbeit, also auch für eine Datenerhebung, -nutzung und -übermittlung, nicht ersichtlich ist.

5.10.8 "Notfallkartei" bei Polizeidienststellen

Einige Polizeidienststellen in Sachsen führen sogenannte "Notfallkarteien". In diesen sind Name, Anschrift und Telefonnummer der für Gewerbebetriebe verantwortlichen Personen aufgeführt. Die Kartei dient dazu, der Polizei - auch nachts oder am Wochenende - die richtigen Ansprechpartner zu benennen, damit Schäden infolge z. B. von Einbrüchen, Bränden, Wasserschäden möglichst gering gehalten werden können. Die Daten für diese Kartei werden nicht zwangsweise, sondern mit Einwilligung des betroffenen Gewerbetreibenden erhoben. Aus datenschutzrechtlicher Sicht bestehen gegen eine solche Kartei deshalb grundsätzlich keine Bedenken. Zu beachten sind hier jedoch die Anforderungen, die an eine wirksame Einwilligungserklärung nach § 4 Abs. 2 und 3 SächsDSG zu stellen sind. Danach muß der schriftlichen Einwilligung der - ebenfalls schriftliche - Hinweis vorausgehen, zu welchem Zweck die Kartei geführt wird und an welche weiteren Stellen die gespeicherten Daten weitergegeben werden dürfen.

5.11 Verfassungsschutz

Einsicht in Akten anderer Behörden durch das Landesamt für Verfassungs-schutz

Das Personalamt einer sächsischen Großstadt fragte bei meiner Dienststelle an, ob das Landesamt für Verfassungsschutz befugt sei, Einsicht in Personalakten zu nehmen.

Weil die Frage des Akteneinsichtsrechts der Verfassungsschutzbehörde von Interesse für sämtliche öffentlichen Stellen ist, sei an dieser Stelle die Rechtslage dargestellt:

Das Landesamt für Verfassungsschutz ist nach § 11 Abs. 2 SächsVSG grundsätzlich befugt, Akten öffentlicher Stellen und amtliche Register einzusehen, wenn folgende Voraussetzungen vorliegen: Die Einsichtnahme muß für die Erfüllung seiner Aufgaben nach § 2 Abs. 1 und 2 SächsVSG oder zum Schutz seiner Mitarbeiter und "Quellen" gegen Gefahren für Leib und Leben erforderlich sein, und eine andere Art der Informationsübermittlung aus den Akten oder den Registern würde den Zweck der Maßnahme oder das Persönlichkeitsrecht von Betroffenen unverhältnismäßig beeinträchtigen.

Zu den Aufgaben des Landesamtes für Verfassungsschutz gehören nach § 2 Abs. 1 SächsVSG die Sammlung und Auswertung von Informationen über extremistische Bestrebungen, über die Spionagetätigkeit für eine fremde Macht, über terroristische Aktivitäten sowie über fortwährende Strukturen und Tätigkeiten der Nachrichtendienste der ehemaligen DDR. Darüber hinaus obliegt es nach § 2 Abs. 2 SächsVSG dem Landesamt für Verfassungsschutz, an Sicherheitsüberprüfungen und Verfassungstreueüberprüfungen für andere Stellen mitzuwirken.

Das Akteneinsichtsrecht des Landesamtes findet allerdings nach § 13 SächsVSG seine Grenze, wenn für die ersuchte öffentliche Stelle erkennbar ist,
- daß unter Berücksichtigung der Art der in Frage kommenden Informationen und ihrer Erhebung die schutzwürdigen Interessen von Betroffenen das Allgemeininteresse an

der Übermittlung überwiegen oder
- daß Sicherheitsinteressen, Belange der Strafverfolgung oder spezialgesetzliche Übermittlungsregelungen entgegenstehen.

Schließlich hat die ersuchte Stelle zu prüfen, ob das Einsichtsersuchen des Landesamtes für Verfassungsschutz gesetzliche Geheimhaltungspflichten oder Berufs- oder Amtsgeheimnisse berührt.

Wird die Einsicht gewährt, hat das Landesamt für Verfassungsschutz nach § 11 Abs. 2 SächsVSG einen Nachweis zu führen, aus dem der Zweck und die Veranlassung, die ersuchte Behörde und die Aktenfundstelle hervorgehen. Der Nachweis ist gegen ungerechtfertigten Zugriff zu sichern und nach fünf Jahren zu vernichten.

Mit dieser gesetzlichen Protokollierungspflicht des Landesamtes ist eine wichtige Voraussetzung für die effiziente Datenschutzkontrolle geschaffen worden. Sie ermöglicht die rasche und zentrale Überprüfung der Rechtmäßigkeit von Datenerhebungen des Verfassungsschutzes, die wegen ihres heimlichen Charakters prinzipiell von großer Eingriffstiefe für die Betroffenen sind. Erfährt der Sächsische Datenschutzbeauftragte von (Zweifels-)Fällen, wird er den Vorgang auch im Landesamt für Verfassungsschutz kontrollieren.

Von einer Protokollierung der Akteneinsicht auf seiten der ersuchten Stellen ist dagegen strikt abzuraten: Hierdurch entstünden nur überflüssige, für die Aufgabenerfüllung dieser Stellen nicht erforderliche Datensammlungen.

5.12 Sonstiges

5.12.1 Namen und Anschriften von Zeugen auf Bußgeldbescheiden

Wiederholt fragten Behörden an, ob im Bußgeldverfahren auf dem Bußgeldbescheid Namen und Anschrift von Zeugen anzugeben seien.

Die Anfragen geben mir Anlaß, grundsätzlich zu der Frage des Persönlichkeitsschutzes in Verwaltungs-, Ordnungswidrigkeiten- und Strafverfahren Stellung zu nehmen:

1. Verwaltungsverfahren

Nicht selten ergreifen Behörden aufgrund von "Bürgeranzeigen" verwaltungsrechtliche Maßnahmen. Ein Beispiel: Aufgrund der Anzeige, daß sich in einem Naturschutzgebiet ein "Schwarzbau" befinde, erläßt die Bauaufsichtsbehörde nach Ermittlung des Sachverhalts eine Abrißverfügung gegen den Eigentümer.
Es stellt sich die Frage, ob die Behörden in diesen Fällen berechtigt oder sogar verpflichtet sind, dem "Angezeigten" Auskunft über den Anzeigenerstatter zu geben:
In Verwaltungsverfahren gilt anstelle des allgemeinen datenschutzrechtlichen Auskunftsanspruchs (§ 17 SächsDSG) gemäß § 29 VwVfG ein *Akteneinsichtsrecht.* Dieses Recht gewährleistet den am Verwaltungsverfahren Beteiligten (also auch den Betroffenen) ein Einsichtsrecht in die Verfahrensakten, in denen auch Daten über

möglicherweise vorhandene Anzeigenerstatter vermerkt sind. Das Einsichtsrecht gilt allerdings nicht uneingeschränkt: So muß u. a. die Kenntnis der Akten zur Geltendmachung oder Verteidigung der rechtlichen Interessen der Beteiligten *erforderlich* sein. Die Behörde muß also stets eine Einzelfallprüfung vornehmen.
Des weiteren ist die Behörde zur Gestattung der Akteneinsicht nicht verpflichtet, soweit die Vorgänge ihrem Wesen nach, namentlich wegen der berechtigten Interessen dritter Personen, geheimgehalten werden müssen. Liegen der Behörde also z. B. *konkrete und objektive Anhaltspunkte* vor, daß der Beteiligte über das Einsichtsrecht Namen und Anschrift des Anzeigenerstatters nur deswegen in Erfahrung bringen will, um sich bei diesem für die Anzeige "zu rächen", darf (und muß) die Akteneinsicht insoweit verweigert werden. Dies sind jedoch seltene Ausnahmen. In der Regel muß jeder Anzeigenerstatter "mit offenem Visier" argumentieren. Seine Identität ist grundsätzlich dem Betroffenen zugänglich.

2. Ordnungswidrigkeiten- und Strafverfahren

Das Akteneinsichtsrecht in Ordnungswidrigkeiten- und Strafverfahren ist in § 147 StPO geregelt (§ 46 OWiG verweist auf die StPO). Die Einsicht in die Akten oder einzelne Aktenstücke darf nach § 147 Abs. 2 StPO nur versagt werden, wenn sie den Untersuchungszweck gefährden kann. Das Einsichtsrecht ist hier also noch umfassender gewährleistet als in einem Verwaltungsverfahren. Allerdings steht das Akteneinsichtsrecht gemäß § 147 Abs. 1 StPO nicht dem "Beschuldigten" in Person, sondern ausschließlich dem von ihm gewählten oder für ihn bestellten Verteidiger zu. Der Verteidiger ist jedoch berechtigt, dem "Beschuldigten" Ablichtungen des Akteninhalts auszuhändigen. Hierdurch können ihm auch Informationen über möglicherweise vorhandene Anzeigenerstatter bekannt werden.
Das Informationsrecht besteht aber nach allgemeiner Auffassung nicht in Angelegenheiten, die *nicht mehr im Rahmen der Verteidigung* liegen. Der Verteidiger darf also Daten über den Anzeigenerstatter zurückhalten, wenn der "Beschuldigte" die Daten *erkennbar* lediglich dazu verwenden will, den Anzeigenerstatter ausfindig zu machen, um auf ihn in unzulässiger Weise (gegebenenfalls mit Gewalt) einzuwirken. Hier trägt der Verteidiger eine eigene Verantwortung.

Dazu, ob auf einem Bußgeldbescheid im Ordnungswidrigkeitenverfahren oder einer Anklageschrift im Strafverfahren Name und Anschrift von Zeugen anzugeben sind, gilt folgendes:

Gemäß § 66 Abs. 1 Nr. 4 OWiG "enthält" der Bußgeldbescheid die Beweismittel. Eine ähnliche Vorschrift enthält die Strafprozeßordnung für die Anklageschrift: Nach § 200 Abs. 1 Satz 2 StPO sind in der Anklageschrift die Beweismittel "zu bezeichnen". Die Angabe der Beweismittel soll in beiden Verfahren den Betroffenen oder Beschuldigten darüber unterrichten, welche Beweismittel die Beschuldigung tragen sollen. Er muß aus Gründen eines effektiv zu gewährleistenden Rechtsschutzes und wegen des Grundsatzes eines fairen Verfahrens grundsätzlich die Möglichkeit haben, die *Beweisbarkeit* des Vorwurfs auch *aus seiner Sicht* zu beurteilen, damit er über die weitere Vorgehensweise sinnvoll entscheiden kann (z. B. Geständnis, Einspruch). Insoweit muß er beispielsweise im Falle des Zeugenbeweises ermitteln können, ob die Wahrnehmungsfähigkeit der Zeugen zum fraglichen Zeitpunkt beeinträchtigt war (z. B.

Brillenträger?, Gehörschaden?, Alkoholiker? ...). Nur wenn er Namen und Anschrift der Zeugen kennt, kann er dessen Wahrnehmungsfähigkeit überprüfen. Deshalb bin ich mit der Rechtsprechung (vgl. OLG Celle NJW 1970, 880) der Auffassung, daß beim Zeugenbeweis grundsätzlich Name und Anschrift der Zeugen auf dem Bußgeldbescheid oder der Anklageschrift angegeben werden müssen (und nicht nur z. B. "Zeugenaussagen"). Der Datenschutz muß hier also zurücktreten.
Allerdings kann statt der *Wohnanschrift* eine andere Anschrift angegeben werden, über die der Zeuge gegebenenfalls zum Gerichtstermin geladen werden kann, wenn er durch die Bekanntgabe der Wohnanschrift gefährdet würde.

5.12.2 Ordnungsamt übermittelt Listen von Erlaubnisinhabern an Polizeidirektion

Ein Landratsamt versandte an eine Polizeidirektion eine Liste aller Inhaber von Erlaubnissen nach dem Waffengesetz, Bundesjagdgesetz und Sprengstoffgesetz, um bei Trunkenheitsstraftaten Schritte zum Entzug der Erlaubnisse schneller einleiten zu können.

Diese Datenübermittlung war aus datenschutzrechtlicher Sicht unzulässig. Verstößt die listenmäßige Übersendung bereits gegen das verfassungsrechtliche Verhältnismäßigkeitsgebot, weil sie sämtliche Erlaubnisinhaber ohne zugrundeliegendes Trunkenheitsdelikt "auf Vorrat" erfaßt, so wäre selbst eine Einzelauskunft von den einschlägigen Rechtsvorschriften nicht gedeckt:

Nach §§ 47 Abs. 2 Satz 1 i. V. m. 8 Abs. 1, 5 Abs. 2 Satz 1 Buchstabe c WaffG darf die Rücknahme einer Erlaubnis nach dem Waffengesetz nur erfolgen, wenn der Erlaubnisinhaber sich nachträglich als unzuverlässig herausstellt. Dies ist nach der Regelvermutung des § 5 Abs. 2 Satz 1 Buchstabe c WaffG dann anzunehmen, wenn der Erlaubnisinhaber mindestens *zweimal* wegen einer im Zustand der Trunkenheit begangenen Straftat *rechtskräftig verurteilt* worden ist. In einem solchen Fall erhält die zuständige Waffenbehörde Kenntnis durch das Gericht (Nr. 37 Abs. 1 Buchstabe c MiStra). Entsprechendes gilt, soweit es um die Rücknahme von Erlaubnissen nach dem Sprengstoffgesetz und dem Bundesjagdgesetz geht. Die Vollzugspolizei ist im Ermittlungsverfahren vor Abschluß einer rechtskräftigen Entscheidung keineswegs zu solchen Mitteilungen befugt. Die Übermittlung von Erlaubnisinhaberdaten konnte somit nicht der Erfüllung von Aufgaben der Vollzugspolizei dienen und wäre aus diesem Grund rechtswidrig gewesen.

Ich habe das Ordnungsamt aufgefordert, künftig sicherzustellen, daß weder in Listenform noch einzeln Auskünfte der beschriebenen Art vom Landratsamt der Vollzugspolizei erteilt werden.

5.12.3 Weitergabe von Halterdaten durch Zulassungsstellen und Meldebehörden an Brandschutzstellen

Eine Brandschutzstelle fragte bei mir an, ob für den Zweck der Abrechnung von Rettungsdienstleistungen Halterdaten von den Zulassungsstellen und Meldebehörden an die Brandschutzstellen übermittelt werden dürfen.

Für Datenübermittlungen der *Zulassungsstellen* zum Zweck der Abrechnung von Rettungsdienstleistungen gilt § 39 Abs. 1 StVG. Nach dieser Vorschrift sind Name und Anschrift des Halters von der Zulassungsstelle zu übermitteln, wenn die Daten "zur Befriedigung von Rechtsansprüchen im Zusammenhang mit der Teilnahme am Straßenverkehr" benötigt werden. Diese Voraussetzungen liegen vor. Weil die Brandschutzstelle nach § 22 SächsBrandschG berechtigt ist, erbrachte Rettungsdienstleistungen abzurechnen, besitzt sie einen Rechtsanspruch im Sinne des § 39 Abs. 1 StVG. Rettungsdienstleistungen stehen zudem oft im Zusammenhang mit der Teilnahme am Straßenverkehr. Dieser Begriff ist sehr weit auszulegen. Es genügt ein mittelbarer Zusammenhang zum Straßenverkehr. Ein solcher Bezug fehlt nur, wenn das Fahrzeug als bloßer Vermögensgegenstand eine Rolle spielt, z. B. bei Auskunftsersuchen der Sozialämter oder Sozialgerichte, um die Hilfsbedürftigkeit des Betreffenden festzustellen oder bei Auskunftsersuchen von Rundfunkanstalten, um Schuldner von Rundfunkgebühren (Autoradio) ausfindig zu machen. Die Abrechnung von Rettungsdienstleistungen, die im Zusammenhang mit Verkehrsunfällen erbracht werden, hat dagegen einen mittelbaren Bezug zum Straßenverkehr, so daß die Halterdaten von der Zulassungsstelle nach § 39 Abs. 1 StVG zu übermitteln sind, wenn daneben auch die weiteren Voraussetzungen dieser Vorschrift erfüllt sind (Angabe des Kfz-Kennzeichens und plausible Darlegung, warum Auskunft erteilt werden soll).

Die Zulässigkeit der Datenübermittlung durch die *Meldeämter* richtet sich nach dem Sächsischen Meldegesetz. Nach § 29 SächsMG (so sinngemäß auch sämtliche Meldegesetze des Bundes und der Länder) darf die Meldebehörde einer anderen öffentlichen Stelle u. a. Name und Anschrift einer Person übermitteln, wenn dies zur Erfüllung der in der Zuständigkeit des Empfängers liegenden Aufgaben erforderlich ist. Dies ist beim Brandschutzamt der Fall, weil es nach § 22 SächsBrandschG zur Abrechnung von Rettungsdienstleistungen befugt ist.

5.12.4 Sächsisches Aussiedlereingliederungsgesetz

Das Sächsische Gesetz über die Eingliederung von Aussiedlern und zur Durchführung des Bundesvertriebenengesetzes sowie anderer Kriegsfolgengesetze (Sächsisches Aussiedlereingliederungsgesetz) ist inzwischen vom Landtag beschlossen worden. Vom SMI wurde ich - was nicht immer der Fall ist - frühzeitig am Gesetzgebungsverfahren beteiligt. Zu dem Gesetzentwurf habe ich aus datenschutzrechtlicher Sicht Stellung genommen.
Besonders kritisch habe ich mich zu der vorgesehenen Datenübermittlungsvorschrift geäußert, die in mehrfacher Hinsicht nicht den Anforderungen entsprach, die im Volkszählungsurteil aufgestellt sind. Beispielsweise waren die in Betracht kommenden

Datenempfänger nicht hinreichend bestimmt ("mit der Betreuung ... befaßte Stellen"). Des weiteren fehlte eine Regelung zur technisch-organisatorischen Gewährleistung des Datenschutzes. Ich habe gegenüber dem SMI konkrete Formulierungsvorschläge gemacht.
Außerdem enthielt der Entwurf eine Vorschrift, die die Übermittlung von Daten an den kirchlichen Suchdienst regelte. Diese Norm unterlag zwar keinen datenschutzrechtlichen Bedenken, war aber überflüssig, weil bereits das Sächsische Meldegesetz eine entsprechende Regelung enthält. Ich habe daher die Streichung der Vorschrift vorgeschlagen.

Meine Anregungen zu dem Gesetzentwurf sind ganz überwiegend berücksichtigt worden.

5.12.5 Drogenkonsum und Fahrerlaubniswesen

In einigen anderen Bundesländern verpflichten Erlasse der Innenministerien die Polizei, den Führerscheinbehörden Erkenntnisse über Drogenkonsum von Fahrzeugführern oder Fahrerlaubnisinhabern mitzuteilen. Die Führerscheinbehörden werden verpflichtet, bei entsprechenden Mitteilungen des Polizeivollzugsdienstes eine Überprüfung der Fahrtauglichkeit durchzuführen und zu Personen, die noch keine Fahrerlaubnis besitzen, die Erkenntnisse zu speichern.

In einem Schreiben an das Sächsische Staatsministerium des Inneren habe ich dargelegt, welchen datenschutzrechtlichen Anforderungen ein entsprechendes Verfahren im Freistaat Sachsen genügen muß: Nach § 65 Abs. 1 Nr. 1 SächsPolG i. V. m. § 43 Abs. 2 des noch geltenden Polizeiaufgabengesetzes kann die Polizei anderen für die Gefahrenabwehr zuständigen Behörden oder öffentlichen Stellen die bei ihr vorhandenen personenbezogenen Daten übermitteln, soweit die Kenntnis dieser Daten zur Erfüllung der Aufgaben des Empfängers erforderlich erscheint. Zu den Befugnissen der Führerscheinbehörde gehört nach §§ 12, 15 b, 15 c StVZO, daß sie zur Vorbereitung ihrer Entscheidung über eine Entziehung oder Einschränkung der Fahrerlaubnis anordnen kann, daß der Inhaber einer Fahrerlaubnis oder Bewerber um eine solche ein Gutachten beibringt, wenn Anlaß zu der Annahme besteht, daß er ungeeignet zum Führen von Kraftfahrzeugen ist. Liegen diese Voraussetzungen vor, ist eine Datenübermittlung unter Beachtung des Verhältnismäßigkeitsgrundsatzes grundsätzlich zulässig.
Das Bundesverfassungsgericht (Beschl. v. 24.6.1993 - 1 BvR 689/92, NJW 1993, 2365 ff.) hält unter Berücksichtigung des allgemeinen Persönlichkeitsrechts die Anforderung eines medizinisch-psychologischen Gutachtens nur dann für angemessen, wenn sie sich auf die Nachprüfung solcher Mängel bezieht, die bei vernünftiger, lebensnaher Einschätzung die Besorgnis begründen, daß der Betroffene sich als Führer eines Kfz nicht verkehrsgerecht und umsichtig verhalten werde. So kann z. B. der einmalige Cannabiskonsum nach dem Beschluß des Gerichts auf keinen Fall einen Eignungsmangel darstellen. Näher läge es, bei gewohnheitsmäßigem Cannabiskonsum von der Ungeeignetheit des Fahrzeugführers auszugehen. Von dem einmaligen Genuß könne jedoch nicht auf gewohnheitsmäßigen Cannabiskonsum geschlossen werden. Ob dies der Fall sei, müsse, wenn es an sonstigen hinreichend aussagekräftigen Anzeichen

für einen regelmäßigen Konsum fehle, durch eine Erörterung mit dem Betroffenen geklärt werden. Erst wenn sich aus bestimmten (weiteren) Anzeichen Zweifel an der Geeignetheit ergäben, könne anschließend ein fachärztliches Gutachten nach § 15 b Abs. 2 Nr. 1 StVZO angefordert werden.

Die Entscheidung des Bundesverfassungsgerichts berührt mittelbar auch die Frage nach der Zulässigkeit von Datenübermittlungen der Polizei an die Straßenverkehrsbehörden und die Speicherung der Daten bei den Straßenverkehrsbehörden. Entgegen der bisherigen Rechtsprechung des Bundesverwaltungsgerichts (NJW 1990, 2638) genügt nun weder der einmalige Rauschgiftkonsum und erst recht nicht der bloße Besitz einer geringen Menge Haschisch, um Zweifel an der Fahrtauglichkeit des Betroffenen zu begründen. Es müssen vielmehr noch weitere Anzeichen hinzukommen, die auf einen regelmäßigen Rauschgiftkonsum und die damit verbundenen Zweifel an der Geeignetheit zum Führen von Kraftfahrzeugen schließen lassen. Nur wenn diese Voraussetzungen vorliegen, ist eine Datenübermittlung von der Polizei an die Straßenverkehrsbehörde sowie eine Speicherung der Daten bei der Straßenverkehrsbehörde unter der Beachtung des Verhältnismäßigkeitsprinzips zulässig, da sie nur dann zur Aufgabenerfüllung der Straßenverkehrsbehörde erforderlich ist. Nach dem Beschluß des Bundesverfassungsgerichts wird es meines Erachtens nunmehr schwierig, die Datenübermittlung und Speicherung im Erlaßwege zu regeln, da die Gründe, die in Verbindung mit Rauschgiftbesitz oder -konsum Zweifel an der Geeignetheit begründen können, zu sehr vom Einzelfall abhängig sind, um zufriedenstellend und abschließend in einer Verwaltungsvorschrift konkretisiert zu werden. Denn eine Datenübermittlung von der Polizei an die Straßenverkehrsbehörden darf nur unter strikter Beachtung des Verhältnismäßigkeitsgrundsatzes erfolgen. Dieser gebietet es, Personen, die noch nicht im Besitz einer Fahrerlaubnis sind, nur dann den Führerscheinbehörden zu melden, wenn mit einiger Wahrscheinlichkeit damit zu rechnen ist, daß der Rauschgiftkonsument oder -besitzer innerhalb einer gewissen Zeitspanne den Führerschein beantragen wird.

Demnach müßten folgende Punkte beachtet werden:
- Von Personen, die keinen bzw. noch keinen Führerschein besitzen, sollten die Daten nicht
  länger als zwei Jahre aufbewahrt werden, da nach zwei Jahren nicht hinreichend sicher ange-
  nommen werden kann, daß die Person noch immer Drogen konsumiert.
- Personen, die älter als 25 Jahre alt und nicht im Besitz einer Fahrerlaubnis sind, sollten in
  Beachtung des verfassungsmäßigen Übermaßverbotes überhaupt nicht an die
  Straßenverkehrsbehörde gemeldet werden, weil lediglich 12 % aller Führerscheinneulinge
  älter als 25 Jahre sind.
- Es sollten nicht die kompletten Anzeigenvorgänge der Polizei, sondern nur die für die
  Aufgabenerfüllung der Straßenverkehrsbehörde erforderlichen Daten übermittelt werden.

Das Sächsische Staatsministerium des Innern hat in Aussicht gestellt, diese Empfehlungen bei einem einschlägigen Erlaß zu berücksichtigen.

6 Finanzen

6.1 Druck von Lohnsteuerkarten durch private Auftragnehmer

Soweit Gemeinden Lohnsteuerkarten ausstellen, Eintragungen und Änderungen auf ihnen vornehmen oder sie versenden, sind sie örtliche Landesfinanzbehörden (§ 39 Abs. 6 EStG) und haben das Steuergeheimnis (§ 30 AO) zu wahren.

Eine Stadt machte mich auf das *Merkblatt der Oberfinanzdirektion Chemnitz für die Gemeinden über die Ausstellung und Übermittlung von Lohnsteuerkarten* aufmerksam, wonach die Gemeinden Privatunternehmen mit dem Druck der Lohnsteuerkarten beauftragen dürfen.

Gegenüber dem SMF habe ich im Hinblick auf § 30 AO und § 3 SächsMG die Auffassung vertreten, daß die Beauftragung eines Privatunternehmens mit dem Druck der Lohnsteuerkarten wegen der in ihnen enthaltenen sensiblen Daten (Kinderfreibeträge, Steuerklassen, Religionszugehörigkeit, Schwerbehinderung, Geburtsdatum usw.) unzulässig ist. Auch wenn lt. Merkblatt das Privatunternehmen in einem schriftlichen Vertrag auf die "Einhaltung der bestehenden Sicherungsvorschriften" zu verpflichten ist, so habe ich das für nicht sachgerecht gehalten. Denn die meisten Gemeinden dürften kaum in der Lage sein, die technisch-organisatorischen Erfordernisse oder die eingesetzte Software bei einer Privatfirma zu kontrollieren, so daß eine unbemerkte Duplizierung des von der Gemeinde übermittelten Meldedatenbestands nicht ausgeschlossen werden kann.

Auch das SMF hielt es für problematisch, Privatunternehmen Steuerdaten zur Verfügung zu stellen, ohne daß die betreffenden Bediensteten förmlich nach dem Verpflichtungsgesetz verpflichtet wurden, damit sie Amtsträgern gemäß § 30 Abs. 3 Nr. 1 AO gleichstehen. Als Sofortmaßnahme wurde deshalb die nachweisliche Verpflichtung dieser Personen angeordnet. Ab 1994 (Druck der Lohnsteuerkarten 1995) - so hat das SMF im Einvernehmen mit dem SMI festgelegt - soll nach und nach von der Beauftragung privater Auftragnehmer abgegangen werden. Ab 1995 (Druck der Lohnsteuerkarten 1996) sollen ausschließlich juristische Personen des öffentlichen Rechts, die der Aufsicht des Freistaats Sachsen unterstehen, beauftragt werden. Auf den ersten Blick mag das übertrieben scheinen. Aber es gibt Bereiche, in denen wegen meist bundesrechtlicher Vorgaben die Aufgaben nicht ohne weiteres privatisiert werden können.

6.2 Bearbeitung der Steuerangelegenheiten von Amtsangehörigen der Finanz-ämter durch ein Nachbarfinanzamt

Die Geschäftsordnung für die Finanzämter (FAGO) sieht in § 23 Abs. 1 Nr. 4 einen Zeichnungsvorbehalt des Finanzamtsvorstehers für die Steuerangelegenheiten von Amtsangehörigen vor. Damit soll gegenseitigen Begünstigungen und Steuerhinterziehungen durch Amtsangehörige begegnet werden. Diese an sich begrüßenswerte Regelung ist aus datenschutzrechtlicher Sicht insofern problematisch,

als ein Vorgesetzter auf diese Weise Einblick in die Einkommens- und Vermögensverhältnisse seiner Mitarbeiter erhält.

Gemäß § 27 AO kann im Einvernehmen mit der örtlich zuständigen Finanzbehörde eine andere Finanzbehörde die Besteuerung übernehmen, wenn der Betroffene zustimmt. In den Ländern Nordrhein-Westfalen und Rheinland-Pfalz werden auf Antrag eines Finanzamtsbediensteten Steuerangelegenheiten durch ein Nachbarfinanzamt erledigt. Der Antrag braucht nicht begründet zu werden.

Ich habe dem SMF vorgeschlagen, gemäß § 29 FAGO für Sachsen eine entsprechende Anordnung zu treffen.

6.3 Verwendung von (Grund-)Steuerlisten der ehemaligen DDR zu Auskunfts-zwecken

In den neuen Bundesländern sind vielfach Grundbücher nicht (mehr) vorhanden oder in so desolatem Zustand, so daß Auskünfte nach § 12 GBO oftmals nicht möglich sind, obwohl gerade in den neuen Bundesländern diese Auskünfte innerhalb und außerhalb des öffentlichen Bereichs dringend benötigt werden (z. B. offene Vermögensfragen, baurechtliche Nachbarbeteiligung, Grenzfeststellung im Vermessungswesen, Zustellung von grundstücksbezogenen Kommunalabgabebescheiden). Auskunftsuchende Behörden und Bürger haben sich deshalb immer wieder an die kommunalen Steuerämter gewandt, da hier (Grund-) Steuerlisten der DDR und des Deutschen Reichs vorhanden sind, die Hinweise auf die Grundstückseigentümer enthalten. Diese Listen konnten jedoch bisher nicht als Auskunftsquellen genutzt werden, da die Daten dem Steuergeheimnis (§ 30 AO) unterliegen.

Durch meine Initiative bei den zuständigen Bundes- und Landesministerien sowie beim Bundesbeauftragten für den Datenschutz konnte erreicht werden, daß die für die Verwaltung der Grundsteuer zuständigen Behörden nunmehr berechtigt sind, gemäß § 31 Abs. 3 AO (eingefügt durch Art. 26 Nr. 2 des Mißbrauchsbekämpfungs- und Steuerbereinigungsgesetz vom 21. Dezember 1993) die vom Steuergeheimnis geschützten Namen und Anschriften von Grundstückseigentümern auch den Gerichten - und damit den Grundbuchämtern - auf Ersuchen mitzuteilen. Ich habe dem SMJ im Einvernehmen mit dem SMF vorgeschlagen, die Grundbücher bzw. Grundakten anhand der bei den kommunalen Steuerämtern vorhandenen Steuerlisten zu aktualisieren. Dann sind die Grundbuchämter künftig in der Lage, die erbetenen Auskünfte zu erteilen. Gegen eine Datenübermittlung, die der "Rekonstruktion" der Grundbücher dient, habe ich keine datenschutzrechtlichen Bedenken, vielmehr halte ich sie für sinnvoll und notwendig.

7 Kultus

7.1 Schule

7.1.1 Verwaltungsvorschrift zum Datenschutz an Schulen

Gemäß Nr. 6.1 der "Schuldatenschutzverwaltungsvorschrift" sind alle öffentlichen Schulen verpflichtet, ein Dateien- und Geräteverzeichnis zu führen, "... sofern eine automatisierte Verarbeitung von personenbezogenen Daten erfolgt".
Diese Formulierung erweckt den Eindruck, ein Dateien- und Geräteverzeichnisses sei nur bei einer *automatisierten* Datenverarbeitung erforderlich. Gemäß § 10 SächsDSG ist jedoch auch bei nicht-automatisierter Datenverarbeitung ein Dateienverzeichnis (aber selbstverständlich kein Geräteverzeichnis) zu führen. Daher wird das Sächsische Staatsministerium für Kultus in einer überarbeiteten Fassung der Verwaltungsvorschrift die Rechtslage klarstellen, wie ich es vorgeschlagen habe.

Auch Nr. 3.1.5 soll überarbeitet werden. Ursprünglich lautete sie: "Nach § 31 Abs. 7 SächsDSG darf eine automatisierte Verarbeitung von Daten der Beschäftigten und Schüler nur im Benehmen mit dem Sächsischen Datenschutzbeauftragten eingeführt, geändert oder erweitert werden. Eine Speicherung von Schülerdaten in automatisierten Dateien ist nicht gestattet". Der zweite Satz ("Eine Speicherung ... ") ist dann durch Nr. 3.2 der "Verwaltungsvorschrift des Sächsischen Staatsministeriums für Kultus zur automatisierten Verarbeitung von Schülerdaten in Schulen und Schulaufsichtsbehörden des Freistaates Sachsen" aufgehoben worden, nicht jedoch Satz 1. Nach Auskunft des SMK hat man die Pflicht, sich mit dem Sächsischen Datenschutzbeauftragten ins Benehmen zu setzen, bewußt aufrechterhalten.

Nach meiner Auffassung ist diese Anordnung nicht sinnvoll, und sie findet auch keine Stütze im Sächsischen Datenschutzgesetz, das eine Pflicht zur Herstellung des Benehmens nur für die Verarbeitung von *Beschäftigten*daten festlegt. Als Lösung bietet sich an, daß bei einer automatisierten Verarbeitung der in Nr. 2.2.1 und Nr. 2.2.2 der Verwaltungsvorschrift zur automatisierten Verarbeitung von Schülerdaten genannten Angaben das Benehmen nicht erforderlich ist. Dabei handelt es sich um die in den Schülerübergabeverzeichnissen und in Schülerdateien genannten Daten. Bei Berufschulen kommen noch einige weitere Angaben, wie Anschrift und Telefonnummer der Ausbildungsstätte, hinzu. Allenfalls dann, wenn sich herausstellt, daß darüber hinaus Daten automatisiert verarbeitet werden müssen, ist die Herstellung des Benehmens erforderlich.
Keinesfalls dürfen nach meiner Auffassung Leistungs- und Verhaltensdaten von Schülern automatisiert verarbeitet werden.

Das SMK hat zugesagt, mich bei der Überarbeitung frühzeitig zu beteiligen.

7.1.2 Verwaltungsvorschrift des SMK über Formblätter für Förderschulen

Förderschulen nehmen im gegliederten Schulwesen Sachsens neben Allgemeinbildenden

Schulen, Berufsbildenden Schulen und Schulen des zweiten Bildungsweges besondere Aufgaben wahr (§ 13 SchulG). Sie werden von Schülern besucht, die wegen der Beeinträchtigung einer oder mehrerer Funktionen auch durch besondere Hilfen in den allgemeinen Schulen nicht oder nicht hinreichend integriert werden können und deshalb für längere Zeit einer besonderen pädagogischen Förderung bedürfen. So werden z. B. Förderschulen für Blinde, Gehörlose, geistig Behinderte und Körperbehinderte eingerichtet. Gemäß § 13 Abs. 5 SchulG stehen den Förderschulen Beratungsstellen zur Verfügung, die für die Früherfassung, Früherkennung und Frühförderung Behinderter oder von Behinderung bedrohter Kinder zuständig sind. Ihnen obliegt außerdem die behindertenspezifische Beratung von Eltern und Lehrern.

Die Entscheidung (Verwaltungsakt) über eine Einschulung in oder den Wechsel an eine Förderschule bereitet die Schulaufsichtsbehörde gemäß § 30 Abs. 2 SchulG, in der Regel das örtlich zuständige Schulamt ("Es *wird beabsichtigt*, Ihr Kind in die Förderschule einzuweisen."), durch Stellungnahmen und Gutachten einer meldenden Stelle (die Einrichtung - in der Regel die Grundschule oder der Kindergarten -, die das Kind derzeit besucht), eines Arztes, eines Psychologen und der Beratungsstelle gemäß § 13 Abs. 5 SchulG vor.

Zur Erfassung und Auswertung der von den genannten Einrichtungen abgegebenen Gutachten und Stellungnahmen hat das SMK eine Verwaltungsvorschrift über die im Rahmen des Aufnahmeverfahrens an Förderschulen zu verwendenden Formblätter erlassen. Ich wurde frühzeitig an der Prüfung der datenschutzrechtlichen Zulässigkeit der dort gestellten Fragen beteiligt. Gerade weil das Förderschulsystem auf die jeweilige Behinderung zugeschnittene Förderschultypen vorsieht, ist die Verwendung eines einheitlichen Formulars aus datenschutzrechtlicher Sicht stets mit der Gefahr verbunden, daß im Einzelfall auch solche Daten erhoben werden, die zur Entscheidung über die Aufnahme wegen einer bestimmten Behinderung nicht erforderlich sind.

Ich habe das SMK deshalb gebeten, die begutachtenden Pädagogen, Ärzte und Psychologen darauf hinzuweisen, daß die als "pädagogisch-psychologisch-medizinische Dokumentation" bezeichneten Formblätter nicht schematisch, sondern je nach den Umständen des Einzelfalles auszufüllen sind. Das SMK hat meine Anregungen zustimmend zur Kenntnis genommen.

7.1.3 Gebührensatzung einer Kreismusikschule

Ein Landratsamt bat mich um Überprüfung der Gebührensatzung einer Kreismusikschule.

Auf Antrag wird die Höchstgebühr ermäßigt. Die Gebühren sind gestaffelt nach dem Nettoeinkommen des Schülers oder bei Minderjährigkeit nach dem Nettoeinkommen der Eltern, das nachgewiesen werden muß. Zur Form des Nachweises äußert sich die Satzung nicht. Hier sollen also Einkommensverhältnisse offenbart werden.

Es ist fraglich, ob die Satzung mit § 14 SächsKAG zu vereinbaren ist. Demgemäß können die Gebühren nach dem Ausmaß der Benutzung (Leistung) oder den durch die

Benutzung durchschnittlich verursachten Kosten bemessen werden. Beide Kriterien können auch verbunden werden. Eine Staffelung der Gebühren nach Einkommen oder nach sozialen Gesichtspunkten ist nicht ausdrücklich vorgesehen. (Anders z. B. § 5 Abs. 3 Satz 2 Niedersächsisches Kommunalabgabengesetz: "Bei der Gebührenbemessung und bei der Festsetzung der Gebührensätze können soziale Gesichtspunkte, auch zugunsten bestimmter Gruppen von Gebührenpflichtigen, berücksichtigt werden".)

Eine Gebührenermäßigung aus sozialen Gesichtspunkten wird unmittelbar nur in § 14 Abs. 2 Satz 2 SächsKAG angesprochen: "Sozial bedingte Gebührenermäßigungen dürfen nicht zu Lasten der übrigen Benutzer eingeräumt werden". Fraglich ist, ob diese Formulierung den Umkehrschluß zuläßt, daß eine sozial bedingte Ermäßigung immer dann zulässig ist, wenn sie nicht zu Lasten der übrigen Benutzer eingeräumt wird.

Das Sächsische Kommunalabgabengesetz ermöglicht *im Einzelfall* eine Gebührenminderung oder einen Gebührenerlaß. § 3 Abs. 1 Nr. 4 b SächsKAG verweist auf § 163 Abs. 1 AO, der erlaubt, Steuern aus Billigkeitsgründen niedriger festzusetzen, und § 3 Abs. 1 Nr. 5 a SächsKAG auf § 227 AO, der einen Erlaß aus Billigkeitsgründen regelt.

Da es sich nicht ausschließlich um ein datenschutzrechtliches Problem handelt, habe ich den Sächsischen Landkreistag um Stellungnahme gebeten, die bisher jedoch nicht vorliegt.

7.2 Datenschutz im kirchlichen Bereich

Ein römisch-katholischer Jurisdiktionsbezirk wandte sich mit der Bitte um Unterstützung an mich. Diese Kirchenbehörde hatte bereits im Februar 1993 bei dem zuständigen SMK die Feststellung ausreichender Datenschutzregelungen gemäß § 14 SächsDSG beantragt, war jedoch längere Zeit nicht beschieden worden. Dies hatte zur Folge, daß staatliche Meldebehörden die gemäß § 30 SächsMG vorgesehene Übermittlung von Meldedaten an die entsprechenden kirchlichen Behörden verweigerten.

Unter "ausreichenden Datenschutzregelungen" sind rechtliche und tatsächliche Regelungen zu verstehen, die den staatlichen Datenschutzstandards nicht im einzelnen, wohl aber in ihrer Summe entsprechen müssen. Die kirchlichen Datenschutzstandards müssen den staatlichen Standards lediglich gleichwertig, brauchen jedoch nicht gleichartig zu sein. Die Forderung nach gleichartigen Regelungen würde gegen die Kompetenzkompetenz der Kirchen (vgl. BVerfGE 7, 198 [207] und ständige Rechtsprechung) und damit gegen das kirchliche Selbstbestimmungsrecht (Art. 140 GG i. V. m. Art. 137 Abs. 3 WRV) verstoßen: Hiernach ist die staatliche Definition und Bestimmung kirchlicher Tätigkeit verfassungswidrig.

Im Bereich des Bistums Dresden-Meißen und der Apostolischen Administratur Görlitz galt zum damaligen Zeitpunkt die "Anordnung über den kirchlichen Datenschutz" (KDO), die durch den jeweiligen Bischof mit Wirkung zum 1.1.1991 bzw. zum 1.3.1991 in Kraft gesetzt worden war. Die KDO wurde in beiden Jurisdiktionsbezirken durch die "Ausführungsbestimmungen zur Anordnung über den kirchlichen Datenschutz" ergänzt.

Im Bereich der Gliedkirchen der Evangelischen Kirche in Deutschland (EKD) galt bereits seit 1991 das (EKD-)Kirchengesetz über die Mitgliedschaft, das kirchliche Meldewesen und den Schutz der Daten der Kirchenmitglieder vom 10.11.1977. Hierauf und auf die für den evangelischen Bereich getroffenen Feststellungen gemäß § 14 SächsDSG habe ich in meinem 1. Tätigkeitsbericht bereits hingewiesen.

Sowohl die datenschutzrechtlichen Regelungen der Katholischen Kirche als auch der evangelischen Gliedkirchen in Sachsen orientierten sich zum Zeitpunkt der an mich herangetragenen Bitte um Unterstützung noch stark an der Fassung des Bundesdatenschutzgesetzes 1977. Die Gesetze bzw. die Anordnungen waren noch nicht an die Neuerungen des Bundesdatenschutzgesetzes 1990 angepaßt. Insbesondere fehlte der nach dem Bundesdatenschutzgesetz 1990 vorgesehene Schadensersatzanspruch nach § 7 BDSG und die Widerspruchs- und Auskunftsrechte gemäß §§ 19 f., 34 f. BDSG. Auch bezogen sich die kirchlichen Regelungen noch nicht auf in Akten gespeicherte Daten. Zudem zeigte sich bei einem Vergleich z. B. der evangelischen Datenschutzverordnung für die Krankenhäuser mit den Regelungen des Sächsischen Krankenhausgesetzes, daß einige kirchliche Regelungen enger gefaßt waren als die entsprechenden staatlichen Normen. Gleichwohl wurden jedoch in beiden Kirchen die sich aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG, Art. 15 und 14 Abs. 1, Art. 33 SächsVerf ergebenden Mindestanforderungen an einen effektiven und verfahrensmäßig gesicherten Schutz des Rechts auf informationelle Selbstbestimmung nicht unterschritten. Der genannte verfassungsrechtliche Maßstab ist auch im Bereich der Kirchen anzulegen, weil es sich um einen "unentbehrlichen, elementaren Grundsatz rechtsstaatlichen Gemeinschaftslebens" (BGHZ 22, 387 f.) und damit um ein "allgemeines Gesetz" im Sinne von Art. 137 Abs. 3 Satz 1 WRV handelt.

Zur Vorbereitung einer Entscheidung habe ich im September 1993 in meinen Diensträumen ein Gespräch mit Vertretern des Bistums Dresden-Meißen, der Apostolischen Administratur Görlitz, der Evangelisch-Lutherischen Landeskirche Sachsens, der Evangelischen Kirche der schlesischen Oberlausitz sowie des SMK geführt. Ich habe mich dabei über den Stand der Novellierung der KDO bzw. des Evangelischen Kirchengesetzes über den Datenschutz unterrichten lassen. Ich bin damals zu der Überzeugung gelangt, daß das - mittlerweile am 12.11.1993 in Kraft getretene - neugefaßte (EKD-)Kirchengesetz über den Datenschutz den datenschutzrechtlichen Standards des Bundesdatenschutzgesetzes 90 entsprechen werde; gleiches gilt für die von der Vollversammlung der deutschen Bischöfe in Fulda im November 1993 beschlossene und in den beiden im Freistaat gelegenen Jurisdiktionsbezirken der Katholischen Kirche zum 1.1.94 in Kraft getretene Neufassung der KDO.

Im Vorgriff auf die genannten Neufassungen sowie unter Berücksichtigung des oben angeführten Umstandes, daß schon die bis dato bestehenden kirchlichen Datenschutzregelungen den verfassungsrechtlich geforderten Datenschutzstandard nicht unterschritten hatten, habe ich dem SMK im Oktober 1993 mein Einvernehmen mit der Feststellung ausreichender Datenschutzmaßnahmen im Bereich der beiden Jurisdiktionsbezirke der Katholischen Kirche in Sachsen mitgeteilt. Das SMK hat daraufhin mit Schreiben vom 27.10.93 die beantragte Feststellung gemäß § 14

SächsDSG getroffen. Die entsprechende Bekanntmachung wurde im Amtsblatt des SMK veröffentlicht (AblSMK Nr. 6 vom 14. März 1994).

Ich habe die Aufgabe, auch in Zukunft regelmäßig - jedoch nur generell - zu prüfen, ob der Datenschutzstandard der Kirchen "ausreichend" im Sinne von § 14 SächsDSG ist. Eine Einzelfallkontrolle innerkirchlicher Vorgänge steht staatlichen Behörden, also auch mir, aber nicht zu. Ich freue mich auf eine weitere gute Zusammenarbeit.

8 Justiz

8.1 Protokollierung von Einsichtnahmen in das Grundbuch

Zahlreiche Eingaben von Bürgern an die Landes- und den Bundesbeauftragten für den Datenschutz belegen die Notwendigkeit, Einsichtnahmen in das Grundbuch zu dokumentieren. So wurden beispielsweise in einem Fall im Rahmen einer ortspolitischen Auseinandersetzung Grundbuchinformationen über Eigentumsverhältnisse durch einen Rechtsanwalt in einem Leserbrief an die Lokalpresse verwendet. In einem anderen Fall erfuhren Dritte ohne berechtigtes Interesse von dem Grundbesitz der Ehefrau eines Beschwerdeführers. In einer Ehescheidungssache erhielten Anwälte Einsicht in das Grundbuch, ohne daß der Anlaß im nachhinein erkennbar war.

Wenn die Grundbucheinsichten vom Grundbuchamt protokolliert würden, ist zu erwarten, daß in vielen Fällen schon das Bewußtsein, das eigene Verhalten könne bei einer späteren Kontrolle nachgeprüft werden, von unberechtigten Einsichtnahmen abhält. Diesem Vorschlag der Datenschutzbeauftragten stehen die Justizverwaltungen der Länder (auch Sachsens) bislang ablehnend gegenüber und führen als Begründung die Arbeitsbelastung der Grundbuchämter an. Da das Grundbuch künftig automatisiert geführt werden wird, kann automatisiert protokolliert und gelöscht werden, wenn dies von Anfang an programmgemäß vorgesehen ist. Protokolliert und nach angemessener Frist gelöscht werden sollten Name, Vorname und Anschrift des Einsichtnehmenden mit Datum und Grund der Einsichtnahme. Dies wäre ein geeignetes Mittel, unberechtigte Einsichtnahmen in das Grundbuch zu verhindern.

Die Protokollierung allein schützt die Daten des Eingetragenen nicht ausreichend. Eine Lösung könnte mit folgender "Anhörungsregelung" erreicht werden: In den weit überwiegenden "Normalfällen" von Einsichtnahmen (z. B. durch Notare, Gerichte, Behörden, Gläubiger) wird der Betroffene nicht angehört, da das Interesse des Rechtsverkehrs an einer unbürokratischen Einsichtnahme hier höher als das Persönlichkeitsrecht des Betroffenen zu werten ist. In allen anderen Fällen von Einsichtnahmeersuchen gebietet das Recht auf informationelle Selbstbestimmung, daß der Eingetragene vorher angehört wird. Als formell Beteiligter hätte der Eingetragene dann auch die Möglichkeit, eine Bewilligung der Einsichtnahme mit dem Rechtsmittel der Beschwerde nach § 71 GBO anzufechten und die Einsichtnahme damit zu verhindern. Auch neuere Literatur und Rechtsprechung tendieren zu dieser Auffassung.
Die Bedenken der Justizverwaltungen, daß die Grundbuchämter nicht über die für eine Anhörung erforderlichen aktuellen Anschriften der Grundstückseigentümer verfügten und deren Ermittlung einen erheblichen Aufwand erfordere, sind weitgehend unbegründet. Eine Anhörung der Eingetragenen erfolgt nur in wenigen Ausnahmefällen. Auch wird die Anschrift der Grundstückseigentümer vielfach noch auf dem aktuellen Stand sein. Schließlich ist die Ermittlung der aktuellen Anschriften in den verbleibenden Fällen durch das Grundbuchamt nach § 29 SächsMG (auch telefonisch) ohne großen Aufwand möglich.

Vergleiche zu Grundbuchfragen auch Abschnitt 9.2.1.

8.2 Geschäftsstellenautomation bei der Staatsanwaltschaft

Über den Einsatz des automatisierten Aktenverwaltungssystems SIJUS-Straf bei der Staatsanwaltschaft Dresden habe ich in meinem 1. Tätigkeitsbericht (unter 8.5) berichtet. Bei einem Informations- und Kontrollbesuch dieser Behörde im Februar 1994 mußte ich feststellen, daß die Anwendung des Systems datenschutzrechtlichen Anforderungen nicht in ausreichendem Maße genügen kann.

SIJUS-Straf ist ein Datenverarbeitungssystem, das alle für die Staatsanwaltschaft anfallenden Verfahrensdaten bereithält und zur weiteren Verarbeitung zur Verfügung stellt. Die in SIJUS-Straf enthaltene Namenskartei enthält folgende Daten: Namen, Vornamen, Geburtsort und -datum, Anschrift, Geburtsnamen, Namen der Mutter, Beruf, Familienstand, Staatsangehörigkeit. Dieser Datensatz verstößt nicht gegen datenschutzrechtliche Vorschriften, da er in diesem Umfang als Suchkriterium für die Textverarbeitung der Staatsanwaltschaft (Strafbefehle, Anklageschriften etc.) und für Anfragen beim BZR erforderlich ist.

Datenschutzrechtlich bedenklich ist jedoch, daß keine Löschungskomponente vorgesehen ist. Da die Datenspeicherung in der zentralen Namenskartei von SIJUS-Straf allein dem Auffinden der registrierten Ermittlungsakte dient, sind die Daten auch nur so lange zu speichern, wie die dazugehörenden Akten nach den Aufbewahrungsbestimmungen aufzubewahren sind. Sobald diese ausgesondert werden, müssen auch die entsprechenden Daten in der Namenskartei gelöscht werden. Aus meiner Sicht kann dies sinnvoll nur durch eine automatische Löschfunktion in SIJUS-Straf gewährleistet werden, die aber bisher fehlt.

Auch die jetzt im Programm vorgesehene Protokollierungsregelung ist aus datenschutzrechtlicher Sicht zumindest dann unzureichend, wenn der Kreis der Anwender in Zukunft erweitert werden sollte. Bisher wird nur so protokolliert, daß dem jeweiligen Benutzer angezeigt wird, wer der vorherige Anwender war. Dies ist zwar im jetzigen Ausbaustadium noch ausreichend, da nur wenige Personen das System zu bestimmten Zwecken nutzen dürfen. Spätestens dann, wenn der Kreis der Anwender erweitert würde, müßte jedoch nachvollziehbar sein, wer *zu welchem Zweck* auf welche Daten zugegriffen hat.

Auf diese Mängel habe ich das SMJus aufmerksam gemacht und um Stellungnahme gebeten.

8.3 Aussonderung von Karteikarten der zentralen manuellen Namenskartei bei Staatsanwaltschaften

Schon in meinem 1. Tätigkeitsbericht (unter 8.4) habe ich kritisiert, daß aufgrund der in den alten Bundesländern bestehenden Aufbewahrungsbestimmungen für das Schriftgut der ordentlichen Gerichtsbarkeit, der Staatsanwaltschaften und der Justizvollzugsbehörden (Aufbewahrungsbestimmungen) die für die Verfahrensakten angelegten Bestände der zentralen manuellen Namenskartei länger aufbewahrt werden als

der dazugehörige Aktenvorgang. Auch das SMJus ging aufgrund einer anschließend durchgeführten Praxisbefragung davon aus, daß die Aufbewahrung der seit dem 3. Oktober 1990 angelegten Namenskarteikarten bei den Staatsanwaltschaften nach der Vernichtung der Verfahrensakten zur Erfüllung staatsanwaltschaftlicher Aufgaben nicht erforderlich ist. Etwas anderes gelte nur für die vorher angelegten Karteikarten, die zu Rehabilitierungszwecken benötigt würden. Ich habe daraufhin vorgeschlagen, die bisher in Sachsen noch nicht geltenden Aufbewahrungsvorschriften in diesem Punkt nicht zu übernehmen. Auch wenn es sich bei den Aufbewahrungsbestimmungen um eine bundeseinheitlich praktizierte Vorschrift handelt, sind die einzelnen Länder nicht verpflichtet, diese vollständig zu übernehmen. Insbesondere ist dies nicht geboten, wenn in einem Land eine von den anderen Ländern abweichende Situation vorliegt. So existieren im Freistaat Sachsen - im Gegensatz zu den alten Bundesländern - noch keine Karteikarten, deren zugrundeliegende Akten bereits vernichtet sind. Es sollte nicht abgewartet werden, ob die anderen Bundesländer irgendwann die Aufbewahrungsbestimmungen in diesem Punkt ändern werden. Dies insbesondere dann nicht, wenn fraglich ist, ob in den alten Bundesländern eine Änderung gewünscht wird, da es dort einen großen Verwaltungsaufwand erfordern würde herauszufinden, bei welchen Karteikarten die zugehörigen Verfahrensakten bereits ausgesondert sind.

Das SMJus hat mir mitgeteilt, daß meine Anregungen bei der -noch nicht beschlossenen - Übernahme der Aufbewahrungsbestimmungen für den Freistaat Sachsen geprüft und gegebenenfalls berücksichtigt würden.

8.4 Zweckgebundene Verwendung von Gauck-Unterlagen

Ein Oberschulamt in Sachsen hat Informationen aus einer von der Gauck-Behörde übersandten IM-Vorlaufakte als Kündigungsgrund verwertet, obwohl der Petent weder hauptamtlich noch inoffiziell für das Ministerium für Staatssicherheit tätig gewesen war. Darin lag meiner Auffassung nach ein Verstoß gegen den in § 29 StUG normierten Zweckbindungsgrundsatz.

Dem Oberschulamt wurden die personenbezogenen Daten des Petenten nach § 21 Abs. 1 Nr. 6 StUG ausschließlich übermittelt um festzustellen, ob dieser hauptamtlich oder inoffiziell für den Staatssicherheitsdienst tätig war.

§ 6 StUG enthält die Legaldefinition der hauptamtlichen und inoffiziellen Mitarbeiter des Staatssicherheitsdienstes (§ 6 Abs.4 StUG) sowie die Definition der Betroffenen (§ 6 Abs. 3 StUG). Betroffene (=Opfer) sind danach auch solche Personen, zu denen der Staatssicherheitsdienst Informationen gesammelt hat, die der Anbahnung und Werbung von diesen Personen für den Staatssicherheitsdienst gedient haben. Etwas anderes gilt nur, wenn die betreffende Person später Mitarbeiter des MfS wurde (§ 6 Abs. 3 Nr. 1), also seine Anwerbung erfolgreich war. Scheiterte die Werbung jedoch, genießt der Kandidat auch in der Anwerbungsphase den Schutz des Gesetzes als Betroffener. Dies ergibt sich ebenfalls aus den Materialien zum StUG (Beschlußempfehlung des Innenausschusses 4. Ausschuß zum StUG, BT-Drucksache 12/1540, Begründung zu § 4).

Zu dem Petenten wurde nur eine IM-Vorlaufakte über einen Anwerbungsversuch angelegt. Der Petent wurde später nicht Mitarbeiter des Ministeriums für Staatssicherheit. Seine personenbezogenen Daten durften deshalb nach § 29 StUG nicht zu anderen Zwecken verwendet werden.

Darüber hinaus stand auch § 5 StUG einer Weiterverwendung der Gauck-Unterlagen des Petenten entgegen. Nach § 5 StUG dürfen personenbezogene Informationen über Betroffene nämlich nicht zum Nachteil dieser Personen verwendet werden. Auch gegen dieses Verbot verstieß das Oberschulamt, indem es Daten aus der IM-Vorlaufakte des Petenten als Kündigungsgrund verwendete.
Eine Stellungnahme des SMK steht noch aus.

8.5 Anonymisierung von Prüfungsakten

In der Zweiten Juristischen Staatsprüfung werden Originalakten mit personenbezogenen Daten bearbeitet. Zum Schutz des Rechts auf informationelle Selbstbestimmung der Betroffenen sollten deshalb die Akten anonymisiert werden.

Ich begrüße deshalb die Regelung des SMJus, wonach Originalfälle oder Urteile, bevor sie Gegenstand einer Prüfungsarbeit werden, so zu verändern sind, daß kein Personenbezug mehr besteht. Klausuren sollen nicht auf einen einzigen Fall oder ein veröffentlichtes Urteil beschränkt werden, weil dies auch aus prüfungsrechtlichen Gründen bedenklich wäre.

8.6 Feststellung der "Ersttäterschaft" von Ladendieben

Wie in einigen anderen Bundesländern sind auch die Staatsanwaltschaften im Freistaat Sachsen durch ihre Landesjustizverwaltung grundsätzlich gehalten, Ermittlungsverfahren wegen Ladendiebstahls von geringer Schadenshöhe nach §§ 153, 153 a StPO einzustellen, wenn die Tat erstmals begangen wurde ("Erstbegehung"). Hierbei stellt sich das - auch datenschutzrechtlich bedeutsame - Problem, anhand welcher Informationen die Staatsanwaltschaft beurteilen kann, ob eine "Ersttäterschaft" vorliegt, werden doch Einstellungen nach §§ 153, 153 a StPO nicht in das Bundeszentralregister aufgenommen. Die Staatsanwaltschaft ist also auf entsprechende eigene Aufzeichnungen (z. B. zentrale Namenskartei) über Verfahrenseinstellungen angewiesen, was ich auch aus datenschutzrechtlicher Sicht für zulässig halte:
Nach § 161 i. V. m. § 160 Abs. 3 StPO soll die Staatsanwaltschaft im Rahmen ihrer Ermittlungstätigkeit auch die Umstände ermitteln, die für die Bestimmung der Rechtsfolgen der Tat von Bedeutung sind. Der Umfang der Schuld des Täters richtet sich dabei unter anderem auch nach dem Vorleben des Täters (§ 46 Abs. 2 StGB). Auch Einstellungen nach §§ 153, 153 a StPO sind bei der Schuldfrage zu berücksichtigen, da bei diesen Einstellungen nicht die Schuld des Täters ausgeschlossen, sondern nur als gering angesehen wird. Häufig sind derartige Fälle aber nicht zu Ende ermittelt worden, und der Beschuldigte hat sich nur aus Gründen der

Prozeßökonomie mit einer Einstellung nach § 153 a StPO einverstanden erklärt. Deshalb darf nur die Tatsache der Einwilligung, nicht aber der weitere - bruchstückhafte - Akteninhalt verwertet werden.

8.7 Nutzung der DDR-Personenkennzahl durch die Strafverfol-gungs-behörden

Im September 1993 lag dem Bundestag ein Änderungsantrag für das Stasi-Unterlagen-Gesetz vor, der es der Gauck-Behörde und der Zentralen Ermittlungskommission für Regierungs- und Vereinigungskriminalität (ZERV) ermöglichen sollte, den reduzierten Meldedatenbestand aus dem Zentralen Einwohnerregister (ZER) der ehemaligen DDR samt Personenkennzahl (PKZ) zur Erfüllung ihrer Aufgaben zu nutzen, insbesondere als Such- und Identifizierungsmittel. Dieser Änderungsantrag fand wegen der engen Zweckbindung der Datennutzung die Zustimmung der Datenschutzbeauftragten.

Mitte Dezember erweiterte jedoch der Rechtsausschuß des Deutschen Bundestages bei der Beratung des Änderungsgesetzes die Nutzungsmöglichkeit zugunsten der Gerichte und Strafverfolgungsbehörden, ohne eine spezielle Zweckbindung vorzusehen. Hiervon wurden die Datenschutzbeauftragten der neuen Länder durch ihre Innen- und Justizministerien nicht informiert.

Am 4. Februar 1994 hat der Deutsche Bundestag die Änderung des Stasi-Unterlagen-Gesetzes in der Fassung des Vorschlages des Rechtsausschusses beschlossen. Die Ausweitung der Verwendung des reduzierten Meldedatenbestands des ZER auf Strafverfolgungsbehörden ist deshalb bedenklich, weil dadurch künftig die PKZ durch Polizeibehörden für die Strafverfolgung nutzbar gemacht werden darf. Gerade das war nach dem Einigungsvertrag aber verboten. Nun besteht die Gefahr, daß mit der PKZ als Hauptsuchkriterium für staatliche Datenbestände der DDR ein zentraler Meldedatenbestand wieder als Mittel der Ermittlungtätigkeit von Polizei, Staatsanwaltschaft und Gerichten aufleben kann. Dies ist nicht mehr mit der besonderen geschichtlichen Situation des Einigungsprozesses zu begründen, da die Regelung erst künftig wirksam wird. Für die Zukunft soll nach dem Einigungsvertrag aber ein Deutschland mit einheitlichen rechtlichen Bedingungen für alle geschaffen werden. Diesem Ziel läuft die neue Regelung zuwider.

9 Wirtschaft und Arbeit

9.1 Verkehrswesen

9.1.1 Erforderlichkeit der Kenntnis von eingestellten Strafverfahren für die Beurteilung der verkehrsrechtlichen Zuverlässigkeit oder Eignung

Im Berichtszeitraum lagen mir unter anderem der Entwurf eines Gesetzes zur Änderung des Straßenverkehrsgesetzes und der Entwurf einer Rechtsverordnung zu § 29 d LuftVG (Überprüfung des Luftfahrtpersonals) vor. Neben anderen datenschutzrechtlich erheblichen Regelungen enthielten beide Entwürfe Vorschriften zu Mitteilungen über eingestellte strafrechtliche Ermittlungsverfahren:

- Nach dem Entwurf einer Verordnung zu § 29 d LuftVG sollten die Flugplatz- oder Luftfahrtunternehmen der zuständigen Luftfahrtbehörde zur Überprüfung der Zuverlässigkeit des Luftfahrtpersonals auch Kenntnisse über eingestellte Strafverfahren weitergeben.
- Der Entwurf einer Änderung des Straßenverkehrsgesetzes sah die Aufnahme von Einstellungen nach § 153 a und 153 b StPO in das Verkehrszentralregister (VZR) vor. (Das VZR dient u. a. den Fahrerlaubnisbehörden zur Ermittlung der Eignungsfeststellung von Führerscheinbewerbern.)

Gegen beide Vorschriften bestehen datenschutzrechtliche Bedenken im Hinblick auf den Grundsatz der Erforderlichkeit:

Einstellungen von Ermittlungsverfahren sieht die Strafprozeßordnung in § 170 Abs. 2 und in den §§ 153 ff. vor.
Nach § 170 Abs. 2 StPO stellt die Staatsanwaltschaft ein Ermittlungsverfahren ein, wenn die Ermittlungen keinen für eine Anklageerhebung hinreichenden Tatverdacht ergeben haben. Demgemäß kann diese Tatsache auch nicht für die Beurteilung der Zuverlässigkeit oder Eignung eines Betroffenen von Bedeutung sein.

Im Ergebnis gilt das gleiche auch bei Einstellungen gemäß §§ 153, 153 a, 153 b StPO:

§ 153 StPO sieht die Einstellungen bei Vergehen vor, wenn die Schuld "des Täters" als gering anzusehen *"wäre"*. Aus dieser Formulierung wird deutlich, daß die Schuldfrage nicht abschließend geklärt ist. Daher kann die Einstellung nach § 153 StPO nicht den Schluß auf eine "Unzuverlässigkeit" oder "Nichteignung zum Führen von Kraftfahrzeugen" rechtfertigen.

Gemäß § 153 a StPO kann ein Ermittlungsverfahren mit Zustimmung des Gerichts *und* des Beschuldigten unter Festsetzung von "Auflagen und Weisungen" eingestellt werden, wenn die Schwere der Schuld einer Einstellung nicht entgegensteht. Auch bei Einstellungen gemäß § 153 a StPO steht eine Schuld *nicht mit Sicherheit fest*. Die Staatsanwaltschaft hat lediglich einen *hinreichenden Verdacht* ermittelt. Eine andere Beurteilung ergibt sich auch nicht aus dem Umstand, daß der Beschuldigte der Einstellung "zustimmen" muß. Die Zustimmung und damit die erklärte Bereitschaft, die

verhängten "Auflagen und Weisungen" zu erfüllen, darf nämlich nicht als "Schuldeingeständnis" gewertet werden. In der Praxis gibt es nicht selten Fälle, in denen ein Beschuldigter allein deshalb einer Einstellung gemäß § 153 a StPO zustimmt, weil er das ihm lästige Strafverfahren schnellstmöglich beendet wissen will, etwa um seine Familie zu schonen oder politische Weiterungen zu vermeiden.

Nach § 153 b StPO kann die Staatsanwaltschaft mit Zustimmung des Gerichts von der Anklageerhebung absehen, wenn die Voraussetzungen vorliegen, unter denen das Gericht von Strafe absehen könnte. Einstellungen nach § 153 b StPO sind aus einer Vielzahl gesetzlich festgelegter Gründe möglich. Die Schuldfrage ist auch in diesen Fällen nicht stets ausermittelt. So stellt die Staatsanwaltschaft beispielsweise ein Ermittlungsverfahren im Zusammenhang mit einem Verkehrsunfall wegen Straßenverkehrsgefährdung (§ 315 c StGB) gemäß § 153 b StPO i. V. m. § 60 StGB in der Regel schon lediglich deswegen ein, weil der Beschuldigte bei dem Unfall selbst schwere Verletzungen erlitten hat.

Zusammengefaßt: In allen Fällen einer Einstellung des Ermittlungsverfahrens bleibt offen, ob der Beschuldigte tatsächlich Täter war, sowie, ob ihn gegebenenfalls eine Schuld trifft. Deshalb halte ich die Übermittlung oder die Speicherung der Tatsache, daß ein Ermittlungsverfahren gegen einen Betroffenen eingestellt worden ist, für zum Zwecke der Zuverlässigkeitsüberprüfung oder Eignungsfeststellung *ungeeignet*, also nicht erforderlich. Ich habe den Bundesbeauftragten für den Datenschutz und das SMWA entsprechend unterrichtet und gebeten, meine datenschutzrechtlichen Bedenken in die Beratungen auf Bundesebene einzubringen. Das Ergebnis steht noch aus.

9.1.2 Übermittlung von Halterdaten an Private zur Geltendmachung von Rechts-ansprüchen

Das Straßenverkehrsgesetz regelt in § 39 die Voraussetzungen für die Übermittlung von Halterdaten durch die Zulassungsstellen an Private zur Durchsetzung von Rechtsansprüchen.

Ich hatte mich in diesem Zusammenhang mit folgenden Sachverhalten zu befassen:
- Ein Petent teilte mit, ein Kraftfahrzeugführer sei rücksichtslos und mit überhöhter Geschwindigkeit auf einer öffentlichen Straße durch eine Regenpfütze nahe dem Gehweg gefahren. Das "heraufspritzende Regenwasser" habe seine Kleidung erheblich verschmutzt. Da der Fahrer nicht angehalten habe, erwäge er zivilrechtliche Schritte.
- Ein anderer schilderte, er habe eines Morgens in seinem zur Straße gelegenen Garten ein stark beschädigtes Kraftfahrzeug vorgefunden. Dieses habe er durch ein Abschleppunternehmen entfernen lassen. Die hierfür aufgewendeten Kosten wolle er ersetzt haben.

Die Petenten fragten, ob sie über die Angabe des Kennzeichens bei der Zulassungsstelle Name und Anschrift des jeweiligen Fahrzeughalters erfahren könnten.

Nach § 39 Abs. 1 StVG sind unter anderem Name und Anschrift des Halters

mitzuteilen, sofern dargelegt wird, daß diese Daten zur Geltendmachung von Rechtsansprüchen im Zusammenhang mit der Teilnahme am Straßenverkehr benötigt werden (einfache Registerauskunft). Gemäß § 7 Abs. 1 StVG ist grundsätzlich auch der Halter für Sachbeschädigungen, die beim Betrieb eines Kraftfahrzeugs entstehen, schadensersatzpflichtig (Gefährdungshaftung, im Unterschied zur ebenfalls zu prüfenden Verschuldenshaftung des Fahrers; beide haften unter Umständen als Gesamtschuldner). Ich hatte daher im eingangs geschilderten Fall keine Bedenken gegen die Übermittlung der Halterdaten, wenn gegenüber der Zulassungsstelle Darlegungen im oben genannten Sinn gemacht werden.

Schwieriger war die Frage der Zulässigkeit der Datenübermittlung bei der zweiten Fallgestaltung zu beantworten. Hier ist das Straßenverkehrsrecht mit seiner typischen Gefährdungshaftung nicht anwendbar. Nach dem Bürgerlichen Gesetzbuch ist nur der *Verursacher* Anspruchsgegner, also derjenige, der das Kfz in den Garten verbracht und dort liegengelassen hat. Er ist nicht unbedingt mit dem Halter identisch. Diese Rechtslage steht einer Registerauskunft nach § 39 Abs. 1 StVG aber nicht entgegen, da die Auskunft gerade den Sinn hat, den Anspruchsgegner *zu ermitteln*. Einziger Anhaltspunkt ist für den Gläubiger zunächst der über das Fahrzeugkennzeichen ermittelbare Halter. Der Geschädigte benötigt daher zumindest Namen und Anschrift des Halters *zur Ermittlung des Schuldners* und damit zur Geltendmachung seiner Ansprüche.
Es lag auch ein "Zusammenhang mit der Teilnahme am Straßenverkehr" vor. Dieses Merkmal wird sehr weit ausgelegt: Es genügt bereits ein mittelbarer Bezug zum Straßenverkehr, insbesondere muß das möglicherweise zum Ersatz berechtigende Ereignis nicht im öffentlichen Straßenraum eingetreten sein. Ein Zusammenhang mit der Teilnahme am Straßenverkehr lag vor, weil davon auszugehen war, daß das Kfz über den öffentlichen Verkehrsraum (Straße) in den Garten gefahren worden war. Also bestanden auch hier keine datenschutzrechtlichen Bedenken gegen eine Registerauskunft.

9.1.3 Übermittlung von Kraftfahrzeughalterdaten an ausländische Behörden zur Verfolgung von Verkehrsordnungswidrigkeiten

Mehrere Kraftfahrzeugzulassungsstellen im Freistaat teilten mir mit, daß sie Namen und Anschriften von Kraftfahrzeughaltern an ausländische Behörden zur Verfolgung von Ordnungswidrigkeiten im Straßenverkehr auf Verlangen von Botschaften weitergeben würden.

Ich habe hierzu folgendes mitgeteilt:

Rechtsgrundlage für die Übermittlung von Halterdaten an Empfänger außerhalb Deutschlands ist § 37 StVG. Hiernach dürfen Halterdaten von den Registerbehörden nur zur Erfüllung von Verpflichtungen aus (multi- oder bilateralen) Vereinbarungen mit anderen Staaten oder zur Durchführung von Rechtsakten der Europäischen Gemeinschaft übermittelt werden. Da diese Vorschrift die Übermittlung von Halterdaten an ausländische Stellen *abschließend regelt*, kann die Weitergabe von Halterdaten an Behörden außerhalb des Bundesgebietes nicht auf die allgemeine Vorschrift des § 35

StVG (Grundsatz der Erforderlichkeit) gestützt werden.

Zweiseitige Vereinbarungen bestehen nach meiner Kenntnis mit Österreich, der Schweiz, Belgien, Luxemburg und Frankreich.

Das SMWA hat die sächsischen Zulassungsstellen entsprechend unterrichtet.

9.1.4 Ermittlung von Tatsachen im Rahmen der Eignungsprüfung bei Anträgen auf Ersterteilung einer Fahrerlaubnis

Gemäß § 9 StVZO haben die Fahrerlaubnisbehörden von Amts wegen zu ermitteln, ob bei Führerscheinbewerbern Bedenken gegen die Eignung zum Führen von Kraftfahrzeugen vorliegen. Der Landesbeauftragte für den Datenschutz in Schleswig-Holstein informierte mich darüber, daß in seinem Zuständigkeitsbereich die Fahrerlaubnisbehörden bei Anträgen auf Ersterteilung einer Fahrerlaubnis auf § 9 StVZO gestützte "Regelanfragen" bei den Ordnungsämtern und Polizeistationen über die Betroffenen stellen. Diese Verfahrensweise unterliegt erheblichen datenschutzrechtlichen Bedenken, die ich den anderen Landesbeauftragten für den Datenschutz und dem SMWA mitgeteilt habe:

Das Verfahren zur Ermittlung der Eignung eines Antragstellers ist in zahlreichen Vorschriften der Straßenverkehrszulassungsordnung und des Straßenverkehrsgesetzes geregelt. Beispielsweise ist gemäß § 9 a StVZO ein Sehtest vorgeschrieben; gemäß § 2 StVG muß der Antragsteller im Rahmen der Prüfung Kenntnisse über die Gefahrenlehre und über eine umweltbewußte Fahrweise nachweisen; außerdem muß der Prüfling den Nachweis erbringen, daß er in der Lage ist, Unfallverletzte sachgemäß zu versorgen (Erste-Hilfe-Kurs). Zur Ermittlung, ob der Antragsteller bereits gegen das Strafgesetzbuch oder das Ordnungswidrigkeitengesetz im Zusammenhang mit der Teilnahme am Straßenverkehr verstoßen hat, können die Fahrerlaubnisbehörden auf das Verkehrszentralregister zugreifen (vgl. § 30 Abs. 2 StVG). Über das gesetzlich geregelte Verfahren hinausgehende Anfragen zur Eignungsfeststellung bei anderen Behörden ohne konkreten Anlaß halte ich für unverhältnismäßig und mit dem Gebot, personenbezogene Daten grundsätzlich beim Betroffenen selbst zu erheben, für nicht vereinbar. Nur wenn konkrete Anhaltspunkte vorliegen, die auf eine fehlende Eignung hinweisen, können weitere Ermittlungsmaßnahmen gerechtfertigt sein (z. B. der Antragsteller erscheint betrunken zur Prüfung).

Das SMWA teilt meine Auffassung. Allerdings besteht in Sachsen derzeit kein Handlungsbedarf, da die Fahrerlaubnisbehörden keine "Regelanfragen" an andere Behörden bei Anträgen auf Ersterteilung einer Fahrerlaubnis stellen.

9.1.5 Weitergabe personenbezogener Daten eines Führerscheinbewerbers an Gutachterstellen

Gemäß § 12 Abs. 1 StVZO kann die Verwaltungsbehörde bei Zweifeln, ob ein

Führerscheinbewerber für die Erteilung einer Fahrerlaubnis geeignet ist, *die Vorlage* eines Gutachtens *fordern*.

Bereits im 1. Tätigkeitsbericht (5.12.2) habe ich dargestellt, daß die Vorlage des Gutachtens alleinige Sache des Bewerbers ist und daher die Übermittlung des Verwaltungsvorgangs oder Teile hiervon an die Gutachterstellen durch die Fahrerlaubnisbehörden ohne Einwilligung des Antragstellers unzulässig wäre.

Datenschutzbeauftragte anderer Bundesländer haben sich meiner Auffassung angeschlossen. Erfreulicherweise hat auch das SMWA in meinem Sinne reagiert und die Fahrerlaubnisbehörden im Freistaat angewiesen, beim Verfahren nach § 12 StVZO folgendes (auszugsweise) zu beachten:

1. Haben die Fahrerlaubnisbehörden begründete Zweifel an der Fahreignung eines Führerscheinbewerbers und fordern sie daher die Vorlage eines Gutachtens, hat der Antragsteller *Wahlfreiheit*, welche Gutachterstelle er beauftragt.

2. Die zur Begutachtung erforderlichen Unterlagen aus dem Verwaltungsvorgang wählt die Fahrerlaubnisbehörde gemeinsam mit dem Führerscheinbewerber aus und übergibt sie (in Kopie) dem Bewerber. Dieser legt die Unterlagen der Gutachterstelle vor. Eine Mitwirkung der Behörde findet nur auf ausdrücklichen Wunsch des Führerscheinbewerbers statt.

Gegen diese Verfahrensweise bestehen keine datenschutzrechtlichen Bedenken mehr.

Dem Führerscheinbewerber bleibt es selbstverständlich unbenommen, in die unmittelbare Übersendung der zur Begutachtung *erforderlichen Unterlagen* durch die Fahrerlaubnisbehörden an die von ihm gewählte Gutachterstelle einzuwilligen. Aus dem gegebenenfalls verwendeten Einwilligungsformular müßte der genaue Umfang der Unterlagen ersichtlich sein. Außerdem müßte ein Hinweis auf den Zweck der Übermittlung gegeben werden und der Empfänger der vorgesehenen Datenübermittlung (Gutachterstelle) genau bezeichnet werden. Der Betroffene müßte weiterhin auf das Recht zur Verweigerung der Einwilligung und darauf hingewiesen werden, daß er in diesem Fall selbst die Unterlagen der Gutachterstelle vorlegen muß (vgl. § 4 Abs. 2 SächsDSG). Ich hätte es begrüßt, wenn die Anforderungen, die an eine datenschutzgerechte Einwilligung zu stellen sind, in die Weisung des SMWA aufgenommen worden wären.

9.2 Offene Vermögensfragen

9.2.1 Anforderung von Grundbuchauszügen durch die Grundstücksverkehrsgenehmigungs-Behörde

Im 1. Tätigkeitsbericht (9.2.4) habe ich berichtet, daß ich ein Landratsamt in dessen Eigenschaft als GVO-Behörde darauf hingewiesen habe, daß und aus welchen Gründen es nicht erforderlich und daher unzulässig ist, im Genehmigungsverfahren nach der

Grundstücksverkehrsordnung von den Antragstellern die Vorlage von Grundbuchauszügen zu verlangen.
Die vom Landratsamt dagegen vorgebrachten Einwendungen habe ich in einer ausführlichen Stellungnahme zurückgewiesen, die auf die konkreten schwierigen Gegebenheiten der Grundstücks-Bezeichnungen, mit denen die Vermögensämter zu kämpfen haben, einging.
Wegen des die Grundbuchämter entlastenden und die Erteilung von Grundstücksverkehrsgenehmigungen beschleunigenden Effektes habe ich dies Schreiben den beiden zuständigen Ministerien, dem SMJus und SMI, zur Verfügung gestellt. Das SMJus jedenfalls scheint von meinem Schreiben Gebrauch gemacht zu haben. Denn in der Folgezeit machte eine Stadtverwaltung, ihre Funktionen als Amt zur Regelung offener Vermögensfragen und als GVO-Behörde nicht auseinanderhaltend, Einwände gegen mein ihm vom örtlichen Grundbuchamt übersandtes Schreiben geltend. Nachdem ich auch diese Einwände widerlegt habe, scheint in dieser Hinsicht Ruhe eingekehrt zu sein. Die ohnehin stark belasteten Grundbuchämter, die bekanntlich vielfach einen der Engpässe im Bereich der Regelung offener Vermögensfragen bzw. des Grundstücksverkehres darstellen, sind von diesen unnötigen Anforderungen entlastet.

9.2.2 Investitionsvorranggesetz: Recht des Anmelders auf Einsicht in den Vorhabenplan

Damit die langwierige Bearbeitung der vielen Anträge auf Rückübertragung von Vermögenswerten nach Möglichkeit die dringend nötige Investitionstätigkeit (einschließlich des Baus von Wohnungen) nicht behinderte, hat man bekanntlich (zunächst nur für den Bereich der in Volkseigentum überführten Grundstücke und Gebäude) von Anfang an neben dem Vermögensgesetz auch das "Gesetz über besondere Investitionen in der Deutschen Demokratischen Republik", üblicherweise kurz als "Investitionsgesetz" oder "InvG" bezeichnet, geschaffen. Beide Gesetze sind, als Bestandteil des Einigungsvertrages (Anl. II Kap. III Sachgeb. B Abschn. I Nr. 4 und 5) beschlossen worden und noch am 29. September 1990 als DDR-Gesetze in Kraft getreten (vgl. Art. 45 Abs. 1 EVertr, Bekanntmachung über das Inkrafttreten des Einigungsvertrages vom 29. September 1990, DDR-GBl. 1988).

Das Investitionsgesetz enthielt die sogenannte *Vorfahrt für Investitionen*, zu der später (durch das sogenannte Hemmnisbeseitigungsgesetz) die im Jargon so genannte *Supervorfahrt* hinzukam, die als § 3a in das Vermögensgesetz eingeführt wurde. Im Jahre 1992 wurden beide Regelungen durch eine neue, wesentlich verbesserte ersetzt, das *Gesetz über den Vorrang für Investitionen bei Rückübertragungsansprüchen nach dem Vermögensgesetz (Investitionsvorranggesetz)*. Es regelt das Investitionsvorrangverfahren, in dem, vereinfacht ausgedrückt, einem Grundstückseigentümer (*Verfügungsberechtigter*) erlaubt wird, einem Investor Rechte an einem Grundstück (einschließlich Gebäude) oder Unternehmen zu verschaffen *zu Lasten desjenigen*, dessen Antrag auf Rückübertragung noch nicht bestandskräftig abgelehnt ist (*Anmelder*).
Stellt sich später heraus, daß der Anmelder seinen Anspruch auf Rückübertragung *zu*

Recht erhoben hatte, erhält er den Erlös bzw. den Verkehrswert, aber eben nicht das Grundstück selbst.

Von einem Vorgang aus diesem Bereich erfuhr ich durch einen in den Landtagsdrucksachen veröffentlichten Beschluß des Petitionsausschusses, an den sich ein Alteigentümer gewandt hatte. Er hatte sich darüber beklagt, daß ihm von der Gemeinde als Investitionsvorrangverfahrens-Behörde, die zugleich auch Verfügungsberechtigte war (vgl. § 4 Abs. 2 InVorG), die Einsicht in den 'Investitionsplan' versagt wurde, der für den von der Verfügungsberechtigten beigebrachten Investitions-Interessenten - das Gesetz nennt ihn *Vorhabenträger* - zum Zweck der Erlangung des Investitionsvorrangbescheides eingereicht worden war.

Der Petitionsausschuß hat die Eingabe dahingehend beschieden, daß die Gemeinde mit der Verweigerung der Möglichkeit der Einsichtnahme in den eingereichten Vorhabenplan nicht gegen Verfahrensvorschriften verstoßen habe. Denn das Gesetz verlange nur, daß der Anmelder in die Lage versetzt werde, "annähernd gleiche investive Maßnahmen" (vgl. § 7 Abs. 1 S. InVorG) zuzusagen wie der Vorhabenträger. Dafür sei es ausreichend, wenn die Behörde dem Anmelder "die Grundzüge der geplanten Investition" mitteile.

Diese Rechtsauffassung, an deren Zustandekommen möglicherweise die für den Fall aufsichtlich zuständigen Staatsministerien nicht ganz unbeteiligt sind, ist in einem vordergründigen Sinne durchaus *datenschutzfreundlich*: Sie besagt, daß die *Unterlassung* der Übermittlung von Daten, nämlich des vollen Inhalts des der Behörde vorgelegten Vorhabenplanes (§ 4 Abs. 3 S. 1 InVorG), zugunsten der Beschränkung auf "die Grundzüge der geplanten Investition" des Vorhabenträgers erlaubt sei. Nichtsdestoweniger habe ich mich - und zwar um meiner *beiden* in § 57 SächsVerf festgelegten Aufgaben willen - für verpflichtet gehalten, darauf hinzuweisen, daß diese Rechtsauffassung meines Erachtens unrichtig ist.

Dies ergibt schon der Gesetzeswortlaut: Gemäß § 5 Abs. 1 S. 1 i. V. m. S. 2 InVorG hat die für das Verfahren zuständige Behörde dem sogenannten Anmelder *'den Vorhabenplan'* zu übermitteln. Darunter ist gemäß § 4 Abs. 3 InVorG die vor der Erteilung des Investitionsvorrangbescheides vom Vorhabenträger der zuständigen Behörde vorgelegte "Beschreibung der wesentlichen Merkmale des Vorhabens" zu verstehen, deren *Mindest*inhalt § 4 Abs. 3 S. 2 InVorG umschreibt. § 5 Abs. 1 S. 2 InVorG ist *nicht* zu entnehmen, daß dem Anmelder nur eine den *Mindest*inhalt des Vorhabenplanes enthaltende Fassung des der Behörde eingereichten Vorhabenplanes zu übersenden ist. Zu übermitteln ist vielmehr nach dem Wortlaut des § 5 Abs. 1 S. 2 "*der* Vorhabenplan", also die eine, vollständige Gesamtheit der als *Beschreibung der wesentlichen Merkmale des Vorhabens* der Behörde tatsächlich eingereichten Unterlagen.

Der *rechtsstaatliche Grund* dieser Regelung ist klar: Dem einen der beiden Bewerber um das Grundstück darf es nicht erlaubt sein, die Behörde mit Schilderungen seines Vorhabens zu beeindrucken, welche sein Mitbewerber, nämlich der gemäß § 7 Abs. 1 S. 2 und 3 InVorG *bei gleichwertigem Vorhaben zu bevorzugende* Anmelder, nicht kennt.

Dem entsprechend enthält die Übermittlungsregelung des § 5 Abs. 1 S. 2 InVorG lediglich eine Konkretisierung des dem Anmelder ohnehin nach § 28 Abs. 1 VwVfG in Verbindung mit § 1 SächsVwVfG zustehenden *Rechtes* darauf, Gelegenheit zu erhalten, sich zu den für die Entscheidung erheblichen Tatsachen zu äußern (*rechtliches Gehör)*, welches durch das gemäß § 29 Abs. 1 S. 1 VwVfG (in Verbindung mit § 1 SächsVwVfG) bestehende *Recht auf Gewährung von Akteneinsicht*, erforderlichenfalls Aktenüberlassung oder Zusendung von Aktenauszügen, ausgefüllt wird (vgl. Obermayer Rdnr. 31 zu § 28 VwVfG); wobei zu berücksichtigen ist, daß dem der vergleichsweise weite Erheblichkeits-Begriff des Prozeßrechtes zugrunde zu legen ist, also daß es genügt, wenn die *Möglichkeit*, daß die Entscheidung bei Berücksichtigung des in Frage stehenden Vorbringens *anders* ausfällt, *nicht* unter jedem denkbaren Gesichtspunkt *auszuschließen* ist (vgl. Kopp Rdnr. 17 zu § 28 VwVfG).

Deshalb kann es nicht überraschen, daß die Rechtsprechung bereits zum alten § 3a VermG im oben dargelegten Umfang eine Unterrichtungspflicht der Investitionsvorrangbehörde gegenüber dem Anmelder festgestellt hat: KreisG Dresden, Zweite Kammer für Verwaltungssachen, Beschl. vom 10.3.1992 - II K 858/91 (VG), VIZ 1992 330, 331; ähnlich BezG Potsdam, Erster Senat für Verwaltungssachen, Beschl. vom 31.3.1992 - I B 15/91 V, ZOV 1992, 171, 172 lSp.

Dem wird man hinzufügen können: Echte *Betriebsgeheimnisse* gehören nicht in den Vorhabenplan; die Behörde ist gehalten, dem Vorhabenträger Gelegenheit zu geben, diesbezügliche Unterlagen zurückzunehmen. Der in der Literatur erörterten Gefahr, daß der Anmelder den Vorhabenplan lediglich *abschreibt*, kann dadurch begegnet werden, daß die Behörde von der in § 7 Abs. 1 S. 3 InVorG vorgesehenen Ausnahmemöglichkeit Gebrauch macht (weil ein solcher Anmelder gerade *nicht* die notwendige hinreichende Gewähr für die Verwirklichung des Vorhabens bietet, vgl. § 4 Abs. 1 S. 1 InVorG).

10 Soziales und Gesundheit

10.1 Gesundheitswesen

10.1.1 Sächsisches Krankenhausgesetz

Am 1. September 1993 ist das Sächsische Krankenhausgesetz in Kraft getreten. Es enthält in § 33 ausführliche Datenschutzbestimmungen, zu denen ich frühzeitig Stellung genommen habe (1. Tätigkeitsbericht unter 10.1.1 zu § 35 des Entwurfs).

Der Begriff Patientendaten ist sehr weit. Er umfaßt auch die personenbezogenen Daten von Angehörigen, anderer Bezugspersonen und sonstiger Dritter, die dem Krankenhaus im Zusammenhang mit der Behandlung bekanntwerden.

Absatz 1 der Vorschrift regelt die Voraussetzungen einer Datenverarbeitung im Krankenhaus. Die wichtigsten Fälle sind die Einwilligung des Patienten und die Verarbeitung der Daten, soweit dies im Rahmen des Behandlungsverhältnisses auf vertraglicher Grundlage erforderlich ist.

Absatz 2 nennt die Befugnisse für eine Übermittlung an Personen oder Stellen außerhalb des Krankenhauses, z. B. neben der Einwilligung die Übermittlung an Sozialleistungsträger zur Feststellung der Leistungspflicht.

§ 33 regelt weiterhin das Auskunftsrecht des Patienten, die Löschung der Patientendaten, den Zugriff der einzelnen Fachabteilungen nach Abschluß der Behandlung, die technischen und organisatorischen Maßnahmen und die Bedingungen, unter denen sich das Krankenhaus zur Verarbeitung von Patientendaten anderer Personen oder Stellen bedienen kann. Abweichend vom Sächsischen Datenschutzgesetz besteht hier eine gesetzliche Verpflichtung zur Bestellung eines internen Datenschutzbeauftragten. Dies entspricht der Regelung im Sozialdatenschutz, also einem Bereich, in dem ähnlich 'sensible' Daten verarbeitet werden.

Auf meine Anregung wurde eine Vorschrift zum Datenschutz bei Forschungsvorhaben eingefügt (§ 34): Ärzte dürfen Patientendaten, die innerhalb ihrer Fachabteilung gespeichert sind, für eigene wissenschaftliche Forschungsvorhaben verarbeiten oder sonst nutzen. Eine Übermittlung an andere Ärzte oder sonstige Dritte zu Zwecken der wissenschaftlichen Forschung ist nur mit Einwilligung des Patienten zulässig, deren Wirksamkeit übrigens immer daran gebunden ist, daß der Patient über seinen Gesundheitszustand, über Art und Umfang der Daten und die Tragweite der Verwendung der Daten durch den Forscher umfassend aufgeklärt ist. Unter bestimmten Voraussetzungen ist eine Einwilligung nicht erforderlich, nämlich dann, wenn das berechtigte Interesse der Allgemeinheit an der Durchführung des Forschungsvorhabens das Geheimhaltungsinteresse des Patienten erheblich überwiegt oder es nicht zumutbar ist, die Einwilligung einzuholen und zusätzlich schutzwürdige Belange des Patienten nicht beeinträchtigt werden.

In diesem wichtigen Teil des Gesundheitswesens ist eine insgesamt zufriedenstellende

bereichsspezifische Norm geschaffen worden.

10.1.2 Einsatz optischer Speicher im Krankenhaus

In Krankenhäusern entstehen viele Patientenunterlagen, die aufzubewahren sind.
Zunehmend bieten Unternehmen Archivierungssysteme mit optischen Speichermedien für eine raum- und zeitsparende und kostengünstige Archivierung von Patientendaten an. Die Patientenunterlagen werden dabei mit Scannern optisch gelesen und dann in digitalisierter Form auf optischen Speichern (ähnlich den Musik-CD) gespeichert. *Meistens werden sogenannte WORM-Platten (von: write-once-read-many) eingesetzt, die sich in der Regel nur einmal beschreiben lassen.*
Mit entsprechender Software und hochauflösenden Ausgabegeräten können die digitalen Kopien der Originale wieder angezeigt und ausgedruckt werden. Wegen der hohen Speicherungsdichte der optischen Platten lassen sich auf einer Speicherplatte in der Größe einer Musik-CD große Archive mit ca. 200 000 DIN A 4 - Druckseiten speichern und damit sehr viele Patientendaten auf engsten Raum ablegen und wiederfinden. Nach dem Digitalisieren und Speichern der Patientenunterlagen sollen die Originale entweder vernichtet oder in einem gesonderten Archiv ausgelagert werden.
Es sind bereits Gespräche zwischen dem SMS und mir sowie einem Anbieter geführt worden, der diese Technik als Modellprojekt in einem Landeskrankenhaus einführen will.
Die §§ 33 und 34 SächsKHG, die den Datenschutz im Krankenhaus regeln (vgl. vorstehend unter 10.1.1), stehen solchen modernen Archivierungssystemen nicht entgegen.
Diese Verfahren sind allerdings mit großen Risiken verbunden. Höhere Anforderungen an technisch-organisatorische Maßnahmen für die Datensicherheit ergeben sich schon aus der mechanischen Empfindlichkeit optischer Speicherplatten. So vermag z. B. ein versehentlich angebrachter, kaum sichtbarer Kratzer das gesamte auf der optischen Platte gespeicherte Archiv unbrauchbar zu machen.
Gemäß § 33 Abs. 5 SächsKHG ist dem Patienten auf Antrag Einsicht in seine Krankenakte zu gewähren. Er muß die Möglichkeit haben, in Ruhe die Unterlagen zu studieren und in ihnen vor- und zurückzublättern. Es wird daher häufig nicht ausreichen, die Dokumente nur auf dem Bildschirm anzuzeigen. Vielmehr muß dafür gesorgt werden, daß sie jederzeit vollständig ausgedruckt werden können.
Der Beweiswert elektronischer Dokumente ist gegenwärtig in der Bundesrepublik nicht gesetzlich geregelt. Das Risiko, daß in einem Arzthaftungsprozeß die digitalisierte Kopie einer Patientenunterlage nicht als dem Originaldokument gleichwertig anerkannt wird, muß der Anwender des optischen Archivsystems tragen.
Der Patient hat einen Berichtigungsanspruch gemäß § 33 Abs. 1 SächsKHG, § 18 Abs. 1 SächsDSG. Unter der Voraussetzung von § 33 Abs. 6 SächsKHG sind die Daten zu löschen. Bei nur einmal beschreibbaren Datenträgern wie der WORM-Platte können daraus grundlegende Probleme entstehen, die vor ihrem Einsatz zu klären sind. Notfalls wären die optische Platte, auf der z. B. ein Änderungsvermerk anzubringen ist, auf eine neue Platte zu kopieren und bei diesem Vorgang gleich die gewünschten Änderungen auf die neue Platte mit zu speichern. Danach wäre die Originalplatte physisch zu zerstören.
Der Einsatz optischer Archivierungssysteme für Patientendaten und die einzuleitenden Maßnahmen für Datenschutz und Datensicherheit setzen also in jedem Einzelfall eine sorgfältige Analyse und Bewertung, auch der neuen rechtlichen und technischen Risi-

ken, voraus.

10.1.3 Aufbewahrung der Patientenunterlagen aufgelöster Polikliniken

Wie bereits im 1. Tätigkeitsberichts (am Ende des Abschnitts 10.1.4) vermerkt, hatte ich das SMS um eine Liste der aufgelösten Polikliniken und um weitere Auskünfte gebeten, die Aufschluß über den Verbleib der Patientenunterlagen geben können. Diese Liste liegt erst seit kurzem vor. Gemeinsam mit dem für das Archivwesen zuständigen SMI soll nun auf der Grundlage dieser Liste eine Regelung über Aufbewahrung und Herausgabe der Patientenunterlagen erarbeitet werden. Für wichtig halte ich eine Informationsschrift für den Bürger, der Hinweise auf den Aufbewahrungsort der Unterlagen zu entnehmen sind. Dies sind sehr häufig die Gesundheitsämter der Landkreise und kreisfreien Städte.

10.1.4 Krebsregistergesetze

Wie in Abschnitt 10.1.2 meines 1. Tätigkeitsberichtes ausführlich dargelegt, habe ich seit August 1991 in Sachsen die intensiven Bemühungen, das "Nationale Krebsregister" der DDR auf veränderter Grundlage fortzuführen, begleitet.
Sachsen hat schon deswegen ein gesteigertes Interesse an epidemiologischer Krebsforschung, weil hier - wie auch in angrenzenden Gebieten Ostthüringens - zu den allenthalben vorhandenen Krebsursachen eine besonders hohe natürliche geogene Radioaktivität und deren besondere Konzentration durch die Hinterlassenschaften des Bergbaus (unter anderem Wismut AG), hinzukommt.

Im Dezember 1992 hat der Bund ein in seiner Geltung bis Ende 1994 befristetes "Gesetz zur Sicherung und vorläufigen Fortführung der Datensammlungen des 'Nationalen Krebsregisters' der ehemaligen Deutschen Demokratischen Republik" (Krebsregistersicherungsgesetz; BGBl. 1992 I S. 2335) erlassen. Es schafft die nötige Rechtsgrundlage für die Aufbewahrung der aus DDR-Zeiten überkommenen Daten, und es *berechtigt* die Ärzte, epidemiologische Angaben über den Verlauf von Krebserkrankungen zu melden, allerdings nur mit *Einwilligung* des Patienten. Außerdem bestimmt es, unter welchen Voraussetzungen die Daten für die Forschung verwendet werden dürfen.

Mit seinem am 20. Juli 1993 in Kraft getretenen Ausführungsgesetz zum Krebsregister-sicherungsgesetz, dem Sächsischen Krebsregistergesetz (SächsKRG - GVBl. S. 589), hat Sachsen von der Möglichkeit Gebrauch gemacht, den sogenannten Meldemodus abweichend zu regeln: In Sachsen besteht - und dafür habe ich mich eingesetzt - eine ärztliche Melde*pflicht*, die von einer Einwilligung des Patienten unabhängig ist (§ 3 Abs. 1, Abs. 4 S. 2 SächsKRG). Dadurch soll, wie es im Gesetz ausdrücklich heißt, 'ein besonderer Beitrag zu einer wirksamen Krebsforschung und Krebsbekämpfung geleistet werden' (§ 1 Abs. 1 SächsKRG). Die Ärzte sind jedoch gehalten, ihre Patienten über die Meldung und deren Inhalt zu unterrichten, sofern nicht nach ihrem fachlichen Urteil dadurch physische, psychische oder soziale Schäden zu befürchten sind (§ 3 Abs. 4 S. 1 SächsKRG).

Ich habe in meinem 1. Tätigkeitsbericht ausführlich dargelegt, warum ich diese

sächsische Lösung einer einwilligungsunabhängigen Meldepflicht unterstützt habe und weiterhin unterstütze. Gegenüber einem bloßen einwilligungsunabhängigen Melde*recht* der Ärzte, wie es z. B. im Saarland besteht, habe ich folgenden zusätzlichen - allgemeinen - Einwand: Es erscheint mir fragwürdig, wenn der Staat unter Berufung auf ein überwiegendes Allgemeininteresse durch Erteilen entsprechender Erlaubnisse Grundrechtseingriffe vorsieht, jedoch nicht den Mut hat, durch Aufstellen einer entsprechenden *Pflicht* diese auch wirklich anzuordnen und sich dadurch mehr als nur halbherzig zur Dringlichkeit dieses Allgemeininteresses zu bekennen. Eine solche Halbherzigkeit mag auf den ersten Blick menschenfreundlich erscheinen, bei genauerer Betrachtung erweist sie sich jedoch als ein Mangel an Widerspruchsfreiheit, der datenschutzrechtlich beziehungsweise - allgemeiner - verfassungsrechtlich gesehen die Berufung auf das angeblich überwiegende Allgemeininteresse zweifelhaft erscheinen läßt.

Als Ergebnis intensiver Vorarbeiten, in denen der Datenschutz in zufriedenstellender Weise Berücksichtigung gefunden hat, wofür vor allem dem Bundesbeauftragten für den Datenschutz zu danken ist, hat die Bundesregierung im Herbst 1993 dem Bundesrat den Entwurf eines "Gesetzes über Krebsregister" (Krebsregistergesetz - KRG) zugeleitet. Mit diesem Gesetz würde für die Zeit nach dem Außerkrafttreten des Krebsregistersicherungsgesetzes eine insbesondere in datenschutzrechtlicher Hinsicht verbesserte Regelung für die Fortführung des gemeinsamen Krebsregisters der östlichen Bundesländer geschaffen. Im Hinblick auf den Datenschutz bemerkenswert ist vor allem die im Entwurf vorgesehene, aus dem an der Mainzer Universitätsklinik entwickelten "Treuhandmodell" hervorgegangene (und von mir seit langem vorgeschlagene) Lösung der Aufteilung des Krebsregisters in eine *Registerstelle* (sie verwaltet die epidemiologischen Daten) und eine davon räumlich, organisatorisch und personell getrennte und vorgeschaltete *Vertrauensstelle*, die für sämtliche Vorgänge mit noch nicht anonymisiertem Personenbezug zuständig sein soll. Außerdem würden durch dieses Gesetz alle Bundesländer verpflichtet, bis 1999 gleichwertige epidemiologische Krebsregister einzuführen (die in den meisten alten Bundesländern noch fehlen).

Der Bundesrat hat den Gesetzentwurf gemäß Art. 76 Abs. 2 GG abgelehnt, wobei rechtlich vor allem von Bedeutung ist, daß die Herleitung der Gesetzgebungszuständigkeit des Bundes aus Art. 74 Nr. 19 GG zweifelhaft ist. Leider hat die Bundesratmehrheit auch gemeint, für Krebsregister fehle das nötige Geld.

Zur Zeit erscheint es fraglich, ob bis zum Ende der Legislaturperiode im Bund oder überhaupt bis zum Außerkrafttreten des Krebsregistersicherungsgesetzes eine neue Grundlage für die Fortführung des gemeinsamen Krebsregisters der östlichen Bundesländer geschaffen werden wird.

Das Register ist allerdings auch *aus anderen Gründen gefährdet*: Die Melderate ist im Jahre 1993 für Sachsen schätzungsweise auf ein Fünftel dessen gesunken, was zu DDR-Zeiten erreicht worden ist. Daß Sachsen dabei noch bei weitem den höchsten Wert erreicht, ist nur ein schwacher Trost. Denn ein Krebsregister ist epidemiologisch nur nützlich - und andernfalls ohne weiteres aus Datenschutzgründen *rechtswidrig*, weil ungeeignet -, wenn die Meldungen einen Vollständigkeitsgrad von ungefähr 90 % erreichen: Ein Wert, der 1990 in den meisten der östlichen Bundesländer auch noch

erreicht worden ist!
Daraus folgt: Sofern es den Verantwortlichen nicht in absehbarer Zeit gelingt, die Melderate auf den gebotenen Stand zu bringen und für die nötigen Nachmeldungen für den Zeitraum 1991-1993 zu sorgen, ist die Weiterführung des gemeinsamen Krebsregisters in Frage gestellt. Ich vermute, daß hierzu zusätzliche konkrete, energisch durchgeführte Maßnahmen nötig sind; insbesondere bedarf es anscheinend einer geeigneten Einflußnahme auf die niedergelassenen Ärzte, aber wohl auch auf die Kliniken. Man streitet sich allen Ernstes um die Portokosten für die Meldungen. Geld kostet es sicherlich, wenn man die bisherigen diesbezüglichen Aufwendungen nicht vergeblich werden lassen und wenn die Deutschen - unter Wahrung des Datenschutzes - auf diesem Gebiet sich nicht aus dem Kreis derjenigen Völker ausschließen wollen, die sich am Beitrag der medizinischen Forschung zur Zukunftssicherung der Menschheit beteiligen.

10.1.5 Örtliche Krebsdatensammlungen

Wie in meinem 1. Tätigkeitsbericht (Abschnitt 10.1.2, 2. Absatz) dargestellt, waren die Meldungen an das "Nationale Krebsregister beim Zentralinstitut für Krebsforschung der Akademie der Wissenschaften der DDR" bei der für den Wohnort des Patienten zuständigen *Betreuungsstelle für Geschwulstkranke der Abteilung Gesundheitswesen des Rates des Kreises* beziehungsweise später der daraus hervorgegangenen *Poliklinischen Abteilung für Onkologie* einzureichen.

Im September 1993 wurde ich darauf aufmerksam, daß diejenigen zusätzlichen Ausfertigungen dieser Meldungen, die seinerzeit nicht nach Berlin weitergeleitet wurden, sondern bei der Betreuungsstelle beziehungsweise Poliklinischen Abteilung für Onkologie verblieben sind, im Zuge der Umgestaltung des Gesundheitswesens von den Gesundheitsämtern übernommen worden sind, dort noch heute aufbewahrt werden und in einzelnen Fällen in unanonymisierter Form für Forschungszwecke weitergegeben wurden.

Die Prüfung der Rechtslage ergab folgendes:

Bevor sich die Frage stellt, inwieweit es erlaubt ist, diese örtlichen Datenbestände zu Forschungszwecken zu *nutzen*, also in der Regel an Forscher zu übermitteln, ist datenschutzrechtlich zu prüfen, ob es rechtmäßig ist, daß diese Daten - die *örtliche Krebsregister* darstellen - überhaupt bei den Gesundheitsämtern *existieren* und *aufbewahrt werden*.

Seit im "Beitrittsgebiet" das Grundgesetz mit seinem Schutz des Grundrechtes auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG) gilt, bedarf diese Aufbewahrung wie jede sonstige Verarbeitung personenbezogener Daten einer gesetzlichen Ermächtigung (vgl. § 4 Abs. 1 Nr. 1 i. V. m. § 3 Abs. 1, Abs. 2 S. 2 Nr. 2 SächsDSG).

Eine bereichsspezifische Regelung, die eine solche gesetzliche Ermächtigung enthielte, ist nicht ersichtlich. Das Krebsregistersicherungsgesetz des Bundes (vgl. dazu den

vorstehenden Abschnitt) enthält diese notwendige gesetzliche Ermächtigung *nicht.* Denn es begrenzt in seinem § 1 Abs. 2 seinen Anwendungsbereich auf diejenigen Daten, die auf Datenträgern des ehemaligen 'Nationalen Krebsregisters der DDR' oder des gemeinsamen Krebsregisters der sechs östlichen Bundesländer gespeichert sind. Gleichlautende Daten auf anderswo lagernden Datenträgern werden davon nicht erfaßt; das ergibt sich nicht nur aus § 1 Abs. 1 und 2, sondern z. B. auch aus § 9.

Auch das Sächsische Krebsregistergesetz, das Sächsische Krankenhausgesetz und das Gesetz über den öffentlichen Gesundheitsdienst im Freistaat Sachsen enthalten eine solche Ermächtigungsgrundlage nicht.

Aber auch das Sächsische Datenschutzgesetz - hier namentlich dessen § 12 - scheidet als Ermächtigungsgrundlage aus. Denn das Krebsregistersicherungsgesetz des Bundes und das ergänzende Sächsische Krebsregistergesetz stellen zusammen eine *abschließende* Regelung für die gesamte Datenverarbeitung dar, die in Fortführung der Krebsdatensammlung des 'Nationalen Krebsregisters der DDR' geschieht. Durch diese bereichsspezifische Regelung als *Spezialgesetz* wird die Anwendung der *allgemeinen datenschutzrechtlichen Ermächtigungen* des Sächsischen Datenschutzgesetzes ausgeschlossen.

Auch das SMS hat keine Ermächtigungsgrundlage für den Verbleib dieser Daten bei den Gesundheitsämtern namhaft machen können.

Aufgrund dieser Rechtslage habe ich zunächst das SMS gebeten, die örtlichen Krebsdatensammlungen durch entsprechende Anweisungen *sperren* zu lassen.

Wäre der Fortbestand des gemeinsamen Krebsregisters der östlichen Bundesländer in Berlin sicherer, als er zur Zeit erscheint, hätte ich in der Zwischenzeit bereits energischer darauf gedrungen, die örtlichen Krebsdatensammlungen dorthin zu übermitteln, damit sie dort zum Abgleich mit den vorhandenen Daten - zwecks deren Verbesserung - verwendet und dann vernichtet werden. Die Rechtslage dürfte insoweit folgende sein: Zwar gilt § 35 SächsDSG auch für *diese* Altdaten; § 5 SächsArchG dürfte jedoch nicht anwendbar sein. Denn als einziger Aufbewahrungsort für Daten dieses Inhaltes kommt das Krebsregister in Betracht, weil die Krebsregistergesetze auch insoweit vorrangige und abschließende Spezialgesetze sind.

Forschungsvorhaben werden dadurch zwar erschwert, aber nicht unmöglich gemacht. Denn es bleibt der Weg über das gemeinsame Krebsregister in Berlin (er wird zur Zeit für ein von der Datensperrung betroffenes Dresdner Dissertationsvorhaben beschritten). Die in den örtlichen Krebsregistern aufbewahrten Daten dürfen nicht unter weniger strengen Voraussetzungen für Forschungszwecke zugänglich (genutzt) werden, als sie nach dem Krebsregistersicherungsgesetz bzw. einem künftigen Krebsregistergesetz des Bundes für das in Berlin fortgeführte Krebsregister gelten.

Meine Kollegen in den östlichen Bundesländern habe ich auf das Problem hingewiesen. Soweit mir bekannt, steht in Mecklenburg-Vorpommern die Vernichtung dieser Daten bevor.

10.1.6 Patientendaten auf offener Postkarte

In der ehemaligen DDR war es durchaus üblich, daß Patienten von Polikliniken, Ärzten und Krankenhäusern auf *offener Postkarte* zur Behandlung oder Untersuchung bestellt wurden.

Eintragungen auf der Postkarte, daß sich der Angeschriebene selbst oder mit seinem Kind aus einem besonderen Anlaß (z. B. einer medizinischen Untersuchung) zu einer gegebenen Zeit an einem bestimmten Ort (z. B. eine bestimmte Station in einem Krankenhaus) einzufinden und spezielle Unterlagen, die angegeben werden, mitzubringen hat, sind überaus sensible personenbezogene Patientendaten aus dem Privatbereich, die Außenstehende nichts angehen. Eine Offenbarung durch den Arzt oder seine Arzthelferin auf der Postkarte kann die ärztliche Schweigepflicht nach § 203 Abs. 1 bzw. Abs. 3 StGB verletzen. Der anordnende Arzt verletzt möglicherweise auch § 2 Abs. 1 der vorläufigen Berufsordnung für die Ärzte Sachsens vom 22.9.1990.

Auch wenn die Bundespost den Transport nach den Bestimmungen der Postordnung und entsprechend dem Brief- und Postgeheimnis (Art. 10 GG) durchführt, können fremde Personen unbefugt Kenntnis von dieser Bestellung zum Arzt erhalten, z. B. wenn Briefkästen gemeinsam von Familienmitgliedern in einer Wohngemeinschaft oder von Hausbewohnern genutzt werden. Wird der Nachbar mit der Leerung des Briefkastens während des Urlaubs oder einer sonstigen Abwesenheit beauftragt, so kann dieser Kenntnis von sensiblen personenbezogenen Daten der Privatsphäre erhalten.

Wenn z. B. ein Arbeitgeber - über Umwege - von gesundheitlichen Problemen eines Bewerbers für einen Arbeitsplatz erfährt und diesen dann nicht einstellt, so zeigt das, welche schwerwiegenden Konsequenzen der leichtfertige und unsensible Umgang mit Patientendaten haben kann und daß möglicherweise dadurch sogar Schadenersatzforderungen des Betroffenen entstehen können.

Die Mitarbeiter des Krankenhauses, das die Bestellkarte versandt hatte, erklärten sich sofort bereit, in Zukunft solche Bestellkarten nur noch im geschlossenen Umschlag zu verschicken.

10.1.7 Erstes Gesetz zur Änderung des Gesetzes über den Öffentlichen Gesundheits-dienst im Freistaat Sachsen

Im Berichtszeitraum wurde ich an der Neufassung des Gesetzes über den Öffentlichen Gesundheitsdienst in Sachsen beteiligt. Der Entwurf sah unter anderem vor, bei der Abnahme neuerrichteter Apotheken durch die Aufsichtsbehörden "ehrenamtliche Pharmazieräte" einzusetzen. Zum ehrenamtlichen Pharmazierat hätten auch Leiter konkurrierender Apotheken bestellt werden können.

Gemäß § 64 Abs. 2 S. 3 AMG kann die zuständige Behörde bei Apotheken, die keine Krankenhausapotheken sind oder die einer Erlaubnis nach § 13 AMG nicht bedürfen, *Sachverständige* mit der *Überwachung* beauftragen. § 64 AMG erlaubt damit nur die Überwachung, nicht auch die Abnahme von Apotheken durch Sachverständige. Die im

Gesetzentwurf vorgesehene Möglichkeit der Abnahme einer neuerrichteten Apotheke durch ehrenamtliche Pharmazieräte als Sachverständige im Sinne des Arzneimittelgesetzes hätte daher gegen die gemäß Art. 72 Abs. 1 GG (i. V. m. Art. 74 Nr. 19 GG) vorgehende bundesrechtliche Regelung verstoßen. .

Darüber hinaus hatte ich grundsätzliche Bedenken gegen die vorbehaltlose Übertragung von Kontrollbefugnissen an potentielle oder tatsächliche Konkurrenzapotheker. Die mit der Überwachung verbundenen Datenerhebungsbefugnisse sind in diesen Fällen einer erhöhten Mißbrauchsgefahr ausgesetzt. Dies gilt in besonderem Maße unter den Bedingungen des grundlegenden Umbruchs im Apothekenwesen in Sachsen. Aus diesem Grunde sind auch langjährige positive Erfahrungen mit ehrenamtlichen Pharmazieräten aus den westlichen Ländern nicht ohne weiteres auf die Situation in Sachsen übertragbar. Aufsicht und Wettbewerb schließen sich im übrigen nicht nur unter den Bedingungen Sachsens prinzipiell gegenseitig aus.

Das SMS hat auf meinen Rat hin die Möglichkeit der Abnahme neuerrichteter Apotheken durch ehrenamtliche Pharmazieräte aus dem Gesetzentwurf gestrichen. Meine prinzipiellen Bedenken wegen der Unvereinbarkeit von Wettbewerb und Aufsicht konnten durch folgende Beschränkung im wesentlichen ausgeräumt werden: Ehrenamtliche Pharmazieräte dürfen weder in dem Stadt- oder Landkreis, in dem sie ihre Apotheke betreiben, noch in den daran angrenzenden Kreisen überwachend tätig werden. Dieses "negative Territorialprinzip" schließt meines Erachtens die Gefahr der Befangenheit eines ehrenamtlichen Pharmazierats im Regelfall hinreichend sicher aus.

Die Regelung gewährleistet zugleich den bestmöglichen Schutz des Grundrechts auf informationelle Selbstbestimmung, weil die konkrete Gefahr des Mißbrauchs der den ehrenamtlichen Pharmazieräten eingeräumten Datenerhebungsbefugnisse erheblich vermindert werden konnte.

Weiterhin wurde auf meine Anregung eine Bestimmung über den Umfang der Datenerhebung durch ehrenamtliche Pharmazieräte in den überarbeiteten Gesetzesentwurf aufgenommen. Danach dürfen die ehrenamtlichen Pharmazieräte personenbezogene Daten nur erheben, soweit dies zur Überwachung der Apotheke erforderlich ist.

10.1.8 Entwicklung eines EDV-Systems für die Gesundheitsämter

Ein Softwarehaus entwickelte für die Gesundheitsämter der Kreise und kreisfreien Städte in Abstimmung mit dem SMS ein komplexes Programmsystem unter Verwendung des Datenbanksystems easy-card für Personalcomputer. Das System soll unter anderem sowohl das Führen der vielfältigen Karteien in den Ämtern als auch die kommunale Berichterstattung an das SMS erleichtern. Eine erste Dokumentation zu diesem EDV-System wurde mir bedauerlicherweise erst kurz vor der ersten Auslieferung vorgelegt.

Nach einer ersten Einsicht habe ich angeregt, die Einführung des Systems unter Datenschutzaspekten in zwei Etappen vorzunehmen. Dieser Vorschlag wurde vom Entwickler aufgegriffen. Die Datenbankbestandteile mit besonders sensiblen personenbezogenen Daten, z. B. zu übertragbaren Seuchen, werden nicht in der ersten, sondern in der zwei-

ten Etappe ausgeliefert.

Unter Berücksichtigung der Bekanntmachung des Sächsischen Datenschutzbeauftragten zur Führung des Dateien- und Geräteverzeichnisses nach § 10 SächsDSG vom 29.9.93 hatte der Entwickler vorgesehen, gleichzeitig mit der Auslieferung den Gesundheitsämtern schon teilweise ausgefüllte Formulare für die Dateibeschreibung nach § 10 SächsDSG zu übergeben. Das wird den entsprechenden öffentlichen Stellen das Anlegen der geforderten Verzeichnisse erleichtern.

Auf eine datenschutzgerechte Gestaltung dieses EDV-Systems für die Gesundheitsämter werde ich weiter Einfluß nehmen.

10.1.9 Entwurf eines Sächsischen Heilberufekammergesetzes

Das Recht der Heilberufe - also der Ärzte, Zahnärzte, Tierärzte und Apotheker - soll in Sachsen möglichst bald gesetzlich geregelt werden. In dem als vorläufige Regelung gedachten Kammergesetz der DDR vom 13.7.1990 (GBl. I S. 7, 11) sind wesentliche Gegenstände des Rechts der Heilberufe - unter anderem die Berufsgerichtsbarkeit - nicht oder unvollständig erfaßt. Das SMS hat daher einen Gesetzesentwurf über die Berufsausübung, Berufsvertretungen und Berufsgerichtsbarkeit der Angehörigen von Heilberufen vorgelegt und mich frühzeitig beteiligt.

Schwerpunkt meiner Anregungen waren die für das berufsgerichtliche Verfahren vorgesehenen Regelungen der Amts- und Rechtshilfe. Verletzt nämlich ein Angehöriger eines Heilberufes seine Berufspflichten, so kann *neben oder anstelle* eines Ordnungswidrigkeiten- oder Strafverfahrens vor einem ordentlichen Gericht ein Verfahren vor dem Landgericht Dresden als Berufsgericht in erster Instanz und dem Oberlandesgericht Dresden als Landesberufsgericht im zweiten Rechtszug durchgeführt werden.

Im Wege der Amts- und Rechtshilfe dürfen z. B. Akten aus dem Studium, dem Examensverfahren, dem Promotions- und Habilitationsverfahren, dem Approbationsverfahren, dem berufsspezifischen Kammerzulassungsverfahren, anderen berufs- oder strafgerichtlichen Verfahren sowie (bei Apothekern) aus dem gewerberechtlichen Zulassungsverfahren des Beschuldigten beigezogen werden. Damit werden zwangsläufig auch Daten erhoben, die zur Verfolgung der konkreten berufsständischen Verfehlung nicht erforderlich sind. So kann etwa der Lebenslauf in der Dissertationsschrift z. B. auch Angaben zum Geburtsnamen der Mutter des Beschuldigten enthalten.

Das Bundesverfassungsgericht hat in seinem Volkszählungsurteil (BVerfGE 65, 1 ff.) ausgeführt, daß bei Datenerhebungen ohne oder gegen den Willen des Betroffenen der Verwendungszweck bereichsspezifisch und präzise zu bestimmen ist und die Grundsätze der Zweckbindung und Erforderlichkeit zu beachten sind (BVerfGE 65, 1 [46]).

Ich habe deshalb angeregt, in die vorgesehenen Amts- und Rechtshilfevorschriften einen ausdrücklichen Hinweis auf den Zweckbindungs- und Erforderlichkeitsgrundsatz aufzunehmen. Das SMS griff diesen Vorschlag auf und fügte folgende Formulierung in den Entwurf ein: "Akten und sonstige Unterlagen, die personenbezogene Daten enthalten, dürfen nur verwertet werden, soweit der Zweck des berufsgerichtlichen Verfahrens dies

erfordert."

In einer Hauptverhandlung über eine Berufsverfehlung werden außerdem oftmals Patientendaten offenbart. Soweit diese Offenbarung durch den Beschuldigten selbst erfolgt, ist anerkannt, daß es sich dabei um eine gerechtfertigte Offenbarung zum Zwecke der Selbstverteidigung handeln kann. Der Patient wird jedoch in seinem Recht auf informationelle Selbstbestimmung verletzt, wenn seine Krankheit oder andere relevante Daten ohne seine Kenntnis vom Gericht oder Zeugen in die Hauptverhandlung eingeführt werden. Die Heilberufekammergesetze anderer Länder sehen deshalb vor, die Hauptverhandlung nichtöffentlich durchzuführen. Der sächsische Entwurf sieht demgegenüber den Grundsatz der Öffentlichkeit der Hauptverhandlung vor. Zum Schutz der Patientendaten habe ich eine Einschränkung dieses Grundsatzes insoweit vorgeschlagen, als Daten, die einem besonderen Berufs- oder Amtsgeheimnis unterliegen, in der Hauptverhandlung nur in anonymisierter Form erörtert werden *sollen*.

Die beiden genannten Einschränkungen bei der Verwertung und Erörterung personenbezogener Daten in der Hauptverhandlung werden aller Voraussicht nach in das Gesetz aufgenommen. Mit der Forderung nach einer anonymisierten Erörterung von Patientendaten wird in Sachsen eine vorbildliche Regelung geschaffen.

10.2 Sozialwesen

10.2.1 Verwendung von Versichertendaten für Werbezwecke

Versicherungspflichtig Beschäftigte eines Handwerksbetriebs sind kraft Gesetzes Mitglied einer Innungskrankenkasse, wenn der Handwerksbetrieb Mitglied einer Handwerksinnung ist und für diese eine Innungskrankenkasse besteht (§ 175 Abs. 1 SGB V). Entsprechendes gilt für Betriebskrankenkassen (§ 174 SGB V).
Falls eine Innungs- oder Betriebskrankenkasse nicht besteht, sind die Beschäftigten Mitglied einer anderen Krankenkasse, häufig einer Allgemeinen Ortskrankenkasse.
Durch Ausdehnung einer Innungs- oder Betriebskrankenkasse auf einen solchen Betrieb werden sie Mitglied der Innungs- oder Betriebskrankenkasse. Dasselbe gilt bei betrieblichen Änderungen, die dazu führen, daß ein Betrieb Mitglied einer Innungs- oder Betriebskrankenkasse wird. Der Gesetzgeber hat jedoch für diese Fälle ein Wahlrecht geschaffen. Gemäß § 183 Abs. 6 SGB V können die Beschäftigten die Mitgliedschaft bei der bisherigen Krankenkasse wählen, indem sie erklären, daß sie bei dieser bleiben wollen.
Die Allgemeinen Ortskrankenkassen wenden sich an ihre Mitglieder, um sie zu einer solchen Erklärung zu bewegen.
Der IKK-Landesverband hat mich um datenschutzrechtliche Prüfung gebeten, ob dies rechtmäßig ist.

Da auch andere Landesdatenschutzbeauftragte von Innungs- oder Betriebskrankenkassen mit dem Problem befaßt wurden, entwickelte sich eine lebhafte Diskussion zwischen den Datenschutzbeauftragten, in der zum Teil unterschiedliche Auffassungen deutlich wurden. Es bildete sich die auch von mir geteilte mehrheitliche Auffassung heraus, daß eine Unterrichtung der (bisherigen) Mitglieder durch die AOK gemäß § 284 Abs. 3 2.

Fall SGB V, § 13 SGB I erlaubt ist.

Nach der erstgenannten Vorschrift düfen die Krankenkassen die rechtmäßig erhobenen und erfaßten versichertenbezogenen Daten nutzen, soweit dies durch Rechtsvorschriften des Sozialgesetzbuches angeordnet oder erlaubt ist. Nach § 13 SGB I sind die Leistungsträger verpflichtet, im Rahmen ihrer Zuständigkeit die Bevölkerung über die Rechte und Pflichten nach dem Sozialgesetzbuch aufzuklären. Die Verwendung des Begriffs "Bevölkerung" könnte darauf hindeuten, daß Adressat von Aufklärungsmaßnahmen die Allgemeinheit ist und nicht ein bestimmter Personenkreis wie die Mitglieder. Die Aufklärung erfolgt jedoch über "die Rechte und Pflichten nach diesem Gesetzbuch". Die Verpflichtung besteht also nur gegenüber bestimmten Personen aus der Gesamtbevölkerung, nämlich denjenigen, die solche Rechte und Pflichten haben können, hier also den Mitgliedern, für die mit der Errichtung oder Ausdehnung der IKK oder BKK oder mit der betrieblichen Veränderung neue Rechte und Pflichten entstehen.
Die *Pflicht* umfaßt auch das *Recht*, die Mitglieder zu informieren.

Von Bedeutung für diese Beurteilung ist der Beschluß des Landessozialgerichts Baden-Württemberg vom 30.8.1989 (L 4 Kr 1430/89 eA). Das Gericht ging - ohne die Frage zu problematisieren - davon aus, die AOK dürfe gemäß §§ 13 bis 15 SGB I ihre Mitglieder über die bei der Abstimmung über die Gründung einer BKK zu bedenkenden Umstände und die Folgen, die eine solche Gründung haben könnte, unterrichten. Auch hier hatte die AOK ihre Mitglieder gezielt angeschrieben. Selbstverständlich muß sich die Aufklärung, auch darauf machte das Gericht aufmerksam, im Rahmen einer sachlichen Argumentation bewegen und darf nicht den Charakter einer gegen wettbewerbsrechtliche Grundsätze verstoßenden Werbung annehmen.

Auch die Innungskrankenkassen nehmen für sich das Recht in Anspruch, gezielt Personen anzuschreiben, um deren Entscheidung über einen Wechsel zu den IKK zu beeinflussen. Hintergrund ist, daß zwischen den Innungskrankenkassen und den Ortskrankenkassen unterschiedliche Auffassungen darüber bestehen, was eine "betriebliche Änderung" ist. Sie liegt nach Auffassung der Allgemeinen Ortskrankenkassen z. B. auch vor, wenn der Betrieb nach dem 1. Januar 1993 (dem Inkrafttreten von § 183 Abs. 6 SGB V) einer Innung beitritt, die bereits zu diesem Zeitpunkt Mitglied einer Innungskrankenkasse war. Diese Auffassung ist vom Sozialgericht Leipzig in einer einstweiligen Anordnung verworfen worden (Beschluß vom 9. Juli 1993 - S 1 Kr 13/93.UR; im Hauptsacheverfahren wurde noch nicht entschieden). In solchen Fällen wendet sich die Innungskrankenkasse an die Mitarbeiter (wenn sie über deren Daten verfügt, weil z. B. ein Arbeitgeber der Innungskrankenkasse beigetreten ist und Daten seiner Mitarbeiter gemeldet hat) und stellt ihre Auffassung dar, daß kein Wahlrecht bestehe. Ob dieses Vorgehen durch § 284 Abs. 3 SGB V, § 13 SGB I gedeckt ist, wird mit diesen Krankenkassen noch zu diskutieren sein.

10.2.2 Angabe der weiteren Arbeitgeber bei mehrfach geringfügig Beschäftigten

Mehrfache geringfügige Beschäftigungen werden zusammengerechnet (§ 8 Abs. 2 SGB IV). Wenn erst nachträglich diese mehrfachen Beschäftigungen bekannt werden, zieht die Krankenkasse, die als Einzugsstelle gemäß § 28 h SGB IV für den Gesamtsozialver-

sicherungsbeitrag zuständig ist, die Arbeitgeber zu den nun erhöhten Beiträgen zur Sozialversicherung heran. Häufig wußten die Arbeitgeber nicht, daß ihr Arbeitnehmer weitere Beschäftigungen ausübt. Die erhöhten Sozialbeiträge wurden daher nicht einkalkuliert. Die Arbeitgeber setzen sich daher gegen die nachträgliche Heranziehung zur Wehr und verlangen von der Leistungsstelle die Bekanntgabe der anderen (angeblichen) Arbeitgeber.

Ein Landesverband einer Krankenkasse bat mich um Auskunft, ob diese Mitteilung zulässig ist.

Nach Auffassung des Sozialgerichts Münster (Urteil vom 3.3.1993 - S 9 Kr 46/91) muß die Krankenkasse die anderen Arbeitgeber, bei denen eine weitere Beschäftigung stattgefunden haben soll, genau benennen und die genauen Zeiträume und die Höhe des Arbeitsentgelts mitteilen. Nur dann sei gewährleistet, daß der Betroffene seine Interessen sachgemäß vertreten könne. Die in § 35 Abs. 1 SGB X normierte Begründungspflicht, die auch der Nachprüfung der Verwaltungsentscheidung durch Aufsichtsbehörden und Gerichte diene, sei gegenüber dem Gebot der Geheimhaltung insoweit vorrangig.

Eine Reihe von Krankenkassen berufen sich auf diese Entscheidung. Sie führte zu einer Diskussion zwischen den Landesdatenschutzbeauftragten.

Ich teile nicht die Auffassung des Sozialgerichts Münster. Name und Anschrift des Arbeitgebers eines sozialversicherungspflichtigen Arbeitnehmers gehören zu den durch das Sozialgeheimnis (§ 35 Abs. 1 Satz 1 SGB I) geschützten Angaben, deren Offenbarung gemäß § 35 Abs. 2 SGB I nur unter den Voraussetzungen der §§ 67 ff. SGB X zulässig ist.

Als Offenbarungsbefugnis kommt hier § 69 Abs. 1 Nr. 1 1. Fall SGB X in Betracht. Die Offenbarung dieser Daten durch die Krankenkasse muß also für die Erfüllung einer gesetzlichen Aufgabe nach dem Sozialgesetzbuch erforderlich sein.

Die gesetzliche Aufgabe ergibt sich aus § 28 h Abs. 2 SGB IV. Nach dieser Norm entscheidet die Einzugsstelle über die Versicherungspflicht und die Beitragshöhe der Kranken- und Rentenversicherung sowie über die Beitragspflicht und Beitragshöhe nach dem Arbeitsförderungsgesetz.

Die Entscheidung ergeht durch Verwaltungsakt. Dieser ist gemäß § 35 SGB X zu begründen. In der Begründung sind die wesentlichen tatsächlichen und rechtlichen Gründe mitzuteilen. Der Betroffene soll in die Lage versetzt werden, die für die Behörde maßgeblichen rechtlichen und tatsächlichen Gesichtspunkte nachzuvollziehen, damit er gegebenenfalls einen Rechtsbehelf (Art. 19 Abs. 4 GG) einlegen und begründen kann. Neben dieser Rechtsschutzfunktion werden in der Literatur die Befriedungsfunktion genannt (dem Betroffenen solle es durch die Begründung leichter gemacht werden, die Verwaltungsentscheidung zu akzeptieren) sowie die Beweisfunktion, nämlich die Möglichkeit für die erlassende Behörde, die Widerspruchsbehörde und das Gericht, im Streitfall die der Entscheidung zugrundeliegenden tatsächlichen und rechtlichen Erwägungen nachzuvollziehen.

Bei Anlegen dieser Maßstäbe ist eine Offenbarung der Daten zur gesetzlichen Aufgabenerfüllung nicht erforderlich, wenn das Bestehen eines weiteren Beschäftigungsverhältnisses zwischen Krankenkasse und Arbeitgeber nicht strittig ist. Ob der Arbeitgeber bestreiten will, weiß die Krankenkasse, da er vor Erlaß des Verwaltungsakts zu hören ist (§ 24 SGB X). Wenn er nicht bestreitet, genügen die Angaben über das Bestehen einer weiteren Beschäftigung und über deren Umfang (Überschneidungszeiträume, Höhe des Entgelts). Allenfalls dann, wenn er bestreitet, stellt sich die Frage, ob man unter dem Gesichtspunkt der Rechtsschutzfunktion und der Beweisfunktion eine Verpflichtung zur Offenlegung bejahen muß, um so den Arbeitgeber beziehungsweise das Gericht in die Lage zu versetzen, den Verwaltungsakt zu überprüfen.

Dies ist vom Sozialgericht Gießen in dessen Urteil vom 1.7.1992 (S 9/Kr-429/91, veröffentlicht in der Zeitschrift "Der Betriebsberater" 1992, Seite 1642), verneint worden. Es hat eine zum Urteil des Sozialgerichts Münster gegenteilige Entscheidung getroffen. Nach Auffassung des Gerichts hatte die beklagte Krankenkasse zu Recht die Mitteilung des Namens des anderen Arbeitgebers verweigert, da sonst berechtigte Geheimhaltungsinteressen verletzt würden. Aus der Anlage zum Bescheid habe sich für die Klägerin eindeutig die Höhe und der Zeitraum, für den die Beiträge nachzuentrichten seien, ergeben. Bei Zweifeln über die Ordnungsmäßigkeit der Berechnung habe sich die Klägerin durch die von der Beklagten angebotene Akteneinsicht Gewißheit verschaffen können.

Der Arbeitgeber kann also durch Akteneinsicht klären, daß die Krankenkasse die Beiträge richtig festgesetzt hat, ohne daß er den Namen des anderen Arbeitgebers erfährt. Die Krankenkasse kann die jeweiligen Angaben bei der Akteneinsicht abdecken.

Auf der Grundlage dieser Entscheidung habe ich den Landesverband gebeten, die anderen Arbeitgeber nicht mehr anzugeben, sondern auf Verlangen Akteneinsicht zu gewähren. Bei dieser Akteneinsicht muß Sorge getragen werden, daß personenbezogene Angaben nicht offenbart werden.

Letztlich müssen die sächsischen Sozialgerichte entscheiden, welcher Auffassung sie folgen. Bis dahin sollte wie von mir vorgeschlagen verfahren werden.

10.2.3 Übermittlung von Adreßdaten des Auszubildenden an Ersatzkassen

Eine Familie aus Dresden wandte sich an mich und bat um eine datenschutzrechtliche Prüfung folgenden Vorgangs: Die Tochter hatte sich um die Ausbildung zur Krankenschwester in einem Städtischen Krankenhaus beworben. Ein Zwischenbescheid des Krankenhauses ließ offen, ob die Tochter für die Ausbildung angenommen werde. Wochen später suchten Vertreter von Ersatzkassen die Familie auf. Diese Vertreter gratulierten zu der Lehrstelle für die Tochter und begannen dann unmittelbar ein Werbegespräch wegen der Mitgliedschaft in der entsprechenden Ersatzkasse.

Meine Nachforschungen ergaben: Das Krankenhaus hatte gleichlautende Listen der auszubildenden Krankenschwestern an Vertreter von drei Ersatzkassen weitergegeben.

Begründet wurde diese Zusammenstellung und Übermittlung von Bewerberdaten insbesondere durch Verweis auf Erklärungen eines Ersatzkassen-Vertreters, wonach es angeblich keine datenschutzrechtliche Bedenken gegen die Herausgabe von Namen und Adressen der Auszubildenden gebe. Verwiesen wurde auf ein Schreiben dieser Ersatzkasse aus dem Jahre 1983. Nach diesem Schreiben sei die Übermittlung von Personaldaten für Zwecke der Werbung für Ersatzkassen zulässig.

Diese Auffassung ist falsch: Mangels spezieller Rechtsnormen greift das Sächsische Datenschutzgesetz ein. Bewerberdaten sind personenbezogene Daten nach § 3 Abs. 1 SächsDSG. Nach § 31 Abs. 1 Satz 1 SächsDSG dürfen öffentliche Stellen Daten von Bewerbern nur verarbeiten, soweit es zur Eingehung, Durchführung oder Beendigung des Dienst- oder Arbeitsverhältnisses *erforderlich* ist oder ein Gesetz, ein Tarifvertrag oder eine Dienstvereinbarung dies vorsieht. Eine solche Regelung bestand nicht. Die geschilderte Verarbeitung (Erstellung der Liste sowie deren Weitergabe) ist für die Eingehung des Ausbildungsverhältnisses auch *nicht* erforderlich. Die Aufbereitung und Übermittlung einer Liste mit Namen und Adressen von Auszubildenden an Vertreter von Ersatzkassen für Werbungszwecke ist damit unzulässig und verletzt das informationelle Selbstbestimmungsrecht derjenigen, deren Namen auf der Liste stehen. Die Listen hätten nur mit ausdrücklicher schriftlicher Einwilligung aller Betroffenen an die Vertreter weitergegeben werden dürfen (§ 4 Abs. 1 Nr. 2, Abs. 2 und 3 SächsDSG).

Die Verantwortlichen des Städtischen Krankenhauses haben unverzüglich Maßnahmen eingeleitet, die eine Wiederholung dieses Vorgangs ausschließen sollen.

10.2.4 Formular zur Verordnung von Rehabilitationssport

Rehabilitationssport dient dazu, Ausdauer, Beweglichkeit und Kraft eines Behinderten zu stärken. Der Sport ist eine ergänzende Leistung zur Rehabilitation gemäß § 43 SGB V, § 28 SGB VI, § 569 a RVO und eine Leistung nach den §§ 11 und 12 BVG.

Die Rehabilitationsträger (Krankenkasse, Rentenversicherungsträger) verordnen und bewilligen den Rehabilitationssport. Er wird in anerkannten Rehabilitationssportgruppen unter ärztlicher Aufsicht durchgeführt. Die Sportgemeinschaft erhält vom Rehabilitationsträger eine Vergütung.

Grundlage des Verfahrens war bisher die "Gesamtvereinbarung über den ambulanten Behindertensport" vom 1. Juli 1981. Am 1. Januar 1994 ist eine neue "Gesamtvereinbarung über den Rehabilitationssport und das Funktionstraining" in Kraft getreten.

Für die Verordnung werden unterschiedliche Formulare verwendet. Gegen ein mir zur Prüfung vorgelegtes Formular, das in der Vergangenheit zumindest in Sachsen, möglicherweise aber auch in anderen Bundesländern, verwendet wurde, bestehen erhebliche datenschutzrechtliche Bedenken. Vorgesehen ist auf einem einzigen Blatt die ärztliche Verordnung, die Bewilligung durch den Rehabilitationsträger, die Bestätigung des Vereins, daß der Versicherte Mitglied ist und auf der Rückseite ein Nachweis der Teilnahme.

Bei den Angaben, die vom Arzt gefordert werden, der den Rehabilitationssport ver-

schreibt, handelt es sich um sensible Daten, die dem von § 203 Abs. 1 und 3 StGB geschützten Arztgeheimnis unterliegen. Eine Befugnis zur Offenbarung kann sich aus einer Einwilligung des Patienten ergeben, die in diesen Formularen jedoch nicht vorgesehen ist. Befugt ist die Offenbarung auch, wenn sie in einer Rechtsvorschrift angeordnet oder erlaubt wird. Die Gesamtvereinbarung, also ein Vertrag, genügt nicht. Ich habe daher die Landesverbände der Krankenkassen um Auskunft gebeten, welche Rechtsvorschriften den Datenaustausch zwischen den Beteiligten, also Arzt, Verein und Rehabilitationsträger, regeln. Eine Antwort habe ich bisher nicht erhalten.

Selbst dann, wenn man die Gesamtvereinbarung ausreichen lassen will, ist damit in keinem Fall eine Grundlage für eine Offenbarung der Patientendaten gegenüber dem Behindertensportverein geschaffen. Über die Diagnose muß der betreuende Arzt, in einem gewissen Umfang möglicherweise auch der Übungsleiter, unterrichtet werden. Das hat durch einen vertraulichen Arztbrief zu geschehen. Das bisher übliche Verfahren führt jedoch dazu, daß z. B. auch der Vereinskassierer Kenntnis von Patientendaten erhält, ohne daß dafür die geringste Notwendigkeit besteht. Nicht einmal bei Vorliegen einer Einwilligung des Behinderten wäre dies zu rechtfertigen, da ihm, wenn er nicht auf den Behindertensport verzichten will, keine wirkliche Wahlfreiheit bleibt.

Verwendet wird auch das Formular "Antrag auf Förderung von Rehabilitationssport/ Funktionstraining" Muster 56. Angaben des Vereins sind in ihm nicht vorgesehen, sondern nur des verschreibenden Arztes und des Rehabilitationsträgers. Wenn es jedoch, wie von einer Krankenkasse bestätigt, dem Verein vorgelegt wird, ist der Effekt derselbe wie bei dem anderen Formular.

Ich habe den Landesverband der AOK, der BKK, der IKK und die Geschäftsstelle der Bundesknappschaft, ebenso die Kassenärztliche Vereinigung Sachsen und den Sächsischen Behinderten- und Versehrtensportverband, gebeten, sich bei ihren Spitzenverbänden für die Vereinbarung eines Formulars einzusetzen, das datenschutzrechtliche Anforderungen erfüllt.

Den Bundesbeauftragten für den Datenschutz habe ich über die Angelegenheit unterrichtet. Er hat unverzüglich eine Stellungnahme gegenüber dem AOK-Bundesverband abgegeben. Dieser teilte mit, die Spitzenverbände der Krankenkassen hätten sich darüber verständigt, den Antrag auf Förderung von Rehabilitationssport/Funktionstraining Anfang 1994 in Absprache mit dem Deutschen Behinderten-Sportverband und der Deutschen Rheumaliga zu bearbeiten. Hierzu würden die vom Bundesbeauftragten geäußerten Bedenken und Wünsche eingebracht und beraten.

Ich werde in Zusammenarbeit mit dem Bundesbeauftragten die Angelegenheit weiterverfolgen.

10.2.5 Freiwillige Patientenkarte

Spätestens bis zum 1. Januar 1995 muß die Krankenkasse für jeden Versicherten eine Krankenversichertenkarte ausstellen, die den Krankenschein ersetzt (§ 291 SGB V). Diese "Pflichtkarte" enthält nur die in § 295 SGB V abschließend genannten Angaben. Dies sind:

- Bezeichnung der ausstellenden Krankenkasse,
- Familienname und Vorname des Versicherten,
- Geburtsdatum,
- Anschrift,
- Krankenversichertennummer,
- Versichertenstatus,
- Tag des Beginns des Versicherungsschutzes, bei befristeter Gültigkeit der Karte das Datum des Fristablaufs.

Krankheitsdaten gehören also nicht dazu.

Ein Reihe unterschiedlicher Anbieter bemüht sich, neben dieser gesetzlich vorgeschriebenen Krankenversichertenkarte eine freiwillige Patientenkarte einzuführen, die erheblich mehr Angaben, insbesondere auch Krankheitsdaten, enthält. Auch der BKK-Landesverband Sachsen plant, eine "BKK-Gesundheits-Card" anzubieten. Ich begrüße sehr, daß er mich bei den Vorbereitungen beteiligt, um eine datenschutzgerechte Gestaltung zu erreichen.

Es handelt sich um eine Chipkarte. Sie soll als Impfkalender und Notfallpaß dienen. Weiterhin werden Bonus-Punkte für die Teilnahme an Aktionstagen, Kursen oder Trainingsprogrammen gespeichert. Bonus-Punkte werden ebenfalls vergeben, wenn keine Leistungen außer den Vorsorgeuntersuchungen in Anspruch genommen wurden. Weiterhin werden die im Rahmen von Aktionstagen oder bei einer ärztlichen Konsultation ermittelten, fest definierten körpereigenen Parameter (z. B. Blutdruck, Blutzucker, Cholesterolwert) gespeichert und aufgeschrieben. Dadurch wird eine Verlaufskontrolle ermöglicht. Entwicklungen und Gesundheitsrisiken werden früh erkennbar. Dem Versicherten können in Gesundheitsberatungen Empfehlungen gegeben werden. In bestimmten Fällen erfolgt der Ratschlag, einen Arzt aufzusuchen.

Vorgesehen sind weitere Funktionen, etwa die Reservierung eines Speicherbereichs für eine freie Texteingabe, die es ermöglicht, Informationen in Zusammenhang mit einer Krankheit oder Schädigung zu speichern.

Der Versicherte kann mit Lesegeräten die Daten bei der BKK und anderen, von ihr autorisierten Einrichtungen lesen und sich die Daten ausdrucken und dort speichern lassen. Der Versicherte bestimmt selbst, welche Daten aufgenommen werden.

Bereits diese Darstellung zeigt, daß eine solche Karte große Vorteile bietet, insbesondere dann, wenn in Notfällen Daten schnell zur Verfügung stehen müssen.

Gerade die hohe Speicherkapazität und die schnelle Verfügbarkeit der Daten bergen jedoch auch Gefahren des Mißbrauchs. Es müssen daher bei der Einführung bestimmte Voraussetzungen beachtet werden. Die 47. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 9./10.3.1994 hat zu diesen Fragen die im Anhang (16.2.6) abgedruckte Entschließung angenommen. Zu den Voraussetzungen gehören unter anderem:

- Da es sich um ein freiwilliges Angebot neben der gesetzlichen Krankenversichertenkarte handelt, muß die Freiwilligkeit wirklich gewährleistet sein. Eingeschränkt werden

könnte sie jedoch durch faktische Zwänge. Das ist schon der Fall, wenn die bisherige Abwicklung der Versicherungsleistung geändert wird, indem man z. B. für diejenigen, die nicht Karteninhaber sind, den Schriftverkehr erschwert oder Karteninhabern den Zugang zu bestimmten Leistungen erleichtert. Auch die Gewährung von Bonus-Punkten vermag bereits einen "sanften", aber effektiven Druck zum Erwerb der Karte auszuüben.

- Festzulegen ist auch, worauf sich die Freiwilligkeit bezieht. Es genügt nicht, daß der Versicherte darüber entscheidet, ob er die Patientenkarte erwerben will. Er muß auch darüber entscheiden können, welche Daten eingetragen werden, wer sie einträgt und wer sie liest. Diese Punkte werden im Konzept des BKK-Landesverbandes berücksichtigt. Der Versicherte muß auch bestimmen können, wer welche Daten in einen Datenbestand übernimmt.

- Fraglich ist auch, wie in Anbetracht der vielfältigen Funktionen eine ausreichende Information des Versicherten erreicht werden kann. Erforderlich ist also eine sorgfältig ausgearbeitete Information.

- Weiterhin muß der Versicherte jederzeit die Möglichkeit haben, die gespeicherten Daten zu lesen, zu ändern und zu löschen.

10.2.6 Antragsformulare für Zuwendungen an Familienberatungsstellen und Beratungsstellen im Bereich der Jugendhilfe

Die kommunalen und freien Träger von Familienberatungsstellen und Beratungsstellen in der Jugendhilfe werden staatlich gefördert, wenn sie die Förderungsbedingungen erfüllen. Dazu gehört, daß die personelle Ausstattung der Beratungsstellen ausreichend ist. Aus diesem Grunde müssen die Träger auf vorgeschriebenen Formularen detaillierte Angaben zum Personal machen.

Es ist sicherlich berechtigt, daß der Staat die Einhaltung personeller Standards kontrolliert. Die Frage ist allerdings, in welchem Ausmaße die Überprüfung stattfinden darf. Das Problem stellt sich im gesamten Bereich staatlicher Förderung.

Das Diakonische Werk der Evangelisch-Lutherischen Landeskirche Sachsens bat mich um datenschutzrechtliche Prüfung des Vordrucks "Förderung von Ehe- und Familienberatungsstellen/Beratungsstellen für Familien in sozialer Notlage" (SächsABl 1992, S. 283) und eines auf der "Richtlinie des Sächsischen Staatsministeriums für Soziales, Gesundheit und Familie für die Gewährung von Zuwendungen im Bereich der Jugendhilfe" beruhenden Formulars des Landesamts für Familie und Soziales (Az.: V 51-12400/1/93).

Bei den Angaben, die der Träger über die Mitarbeiter machen soll, handelt es sich um eine Datenerhebung bei Dritten. Grundsätzlich sind jedoch gemäß § 11 Abs. 1 SächsDSG Daten beim Betroffenen zu erheben. Eine durchaus praktikable Alternative zu dem hier vorgesehenen Verfahren ist die Aufforderung an die Träger, den Beschäftigten den Erhebungsbogen vorzulegen, den diese selbst ausfüllen und den Behörden

übergeben. Dieser Weg ist sicherlich ungewöhnlich, aber durchaus einer Prüfung wert. Falls man die Daten der Mitarbeiter beim Träger, also einem Dritten, erheben will, müssen die Voraussetzungen von § 11 Abs. 4 SächsDSG vorliegen. In Betracht kommt zunächst dessen Nr. 1. Die Richtlinie ist jedoch weder ein Gesetz noch eine Rechtsverordnung. Zumindest im hier interessierenden Bereich, also der Förderung von Ehe- und Familienberatungsstellen und Schuldnerberatungsstellen, bestehen solche Normen nicht.

Zweifelhaft ist, ob § 11 Abs. 4 Nr. 8 SächsDSG zutrifft: Weder ist ohne weiteres zu begründen, daß die Datenerhebung bei Betroffenen auf die oben skizzierte Weise einen unverhältnismäßigen Aufwand verursacht, noch, daß keine Anhaltspunkte für überwiegend schutzwürdige Interessen des Betroffenen bestehen.

Es bleibt also nur § 11 Abs. 4 Nr. 2 SächsDSG. Voraussetzung einer Einwilligung ist Freiwilligkeit. Bei einem Mitarbeiter, der von seinem Arbeitgeber aufgefordert wird, in die Datenübermittlung einzuwilligen, wird jedoch schwerlich Freiwilligkeit anzunehmen sein. Nicht zu verkennen ist allerdings, daß auch dann, wenn der Erhebungsbogen dem Mitarbeiter vorgelegt wird, der (faktische) Druck so stark ist, daß eine Verweigerung der Annahme kaum in Betracht kommt.

Abgesehen von diesem grundsätzlichen Problem ist es fraglich, ob alle Angaben erforderlich sind, etwa die Ablichtung der Lohnsteuerbescheinigung und eine sehr detaillierte Aufschlüsselung der Einkommensbestandteile im Antragsformular des Landesamts für Familie und Soziales.

Auch die "Richtlinie des Sächsischen Staatsministeriums für Soziales, Gesundheit und Familie für den Betrieb von Jugendhilfeeinrichtungen" gehen in Nr. 7.5.5 weit über die von § 47 Abs. 1 Satz 1 Nr. 1 SGB VIII geforderten Angaben hinaus.

Ich habe dem Diakonischen Werk und dem SMS meine Auffassung mitgeteilt und ein Gespräch zwischen dem Ministerium, Vertretern der Wohlfahrtsverbände, gegebenenfalls auch den kommunalen Trägern und dem Sächsischen Datenschutzbeauftragten angeregt. Ich hoffe, daß es in nächster Zeit stattfinden wird.

10.2.7 Einwilligungsformular bei Anträgen auf Leistungen nach dem Bundesversorgungsgesetz

Das Sächsische Landesamt für Familie und Soziales übersandte mir ein Formular "Einverständniserklärung" und bat um datenschutzrechtliche Prüfung. Mit seiner Unterschrift erklärt sich der Unterzeichnende einverstanden, daß das zuständige Amt zur Bearbeitung der Versorgungsanträge nach dem sozialen Entschädigungsrecht (einschließlich der Nebengesetze wie z. B. Bundesseuchengesetz), dem Strafrechtlichen Rehabilitierungsgesetz, dem Schwerbehindertengesetz sowie dem Landesblindengeldgesetz die für die Anerkennung/Feststellung erforderlichen Auskünfte einholt. Die bei Krankenanstalten und den Sozialleistungsträgern (Arbeitsamt, Kranken-, Renten- und Unfallversicherung, Sozial- und Jugendhilfe) sowie Pensionsbehörden und Gesundheitsämtern geführten Untersuchungsunterlagen (Krankenpapiere, Aufzeichnungen, Krankengeschichten, Untersuchungsbefunde, Röntgenbilder usw.) sollen zur Einsicht beigezogen werden

können. Ferner erklärt sich der Unterzeichnende damit einverstanden, daß das Amt in diesem Zusammenhang auch von behandelnden Ärzten die erforderlichen Auskünfte einholt und Aufzeichnungen über Befunde und Behandlungsmaßnahmen beizieht. Außerdem entbindet der Unterzeichnende die beteiligten Ärzte von ihrer Schweigepflicht und stimmt der Verwertung der Auskünfte und Unterlagen im Verwaltungsverfahren zu.

Diese umfassende und wenig aufschlußreiche "Einverständniserklärung" ist nach meiner Meinung mit dem Recht auf informationelle Selbstbestimmung nicht vereinbar.

Mit der umfassenden "Einwilligungserklärung" für unterschiedliche Zuständigkeitsbereiche wird den Versorgungsämtern ein *praktisch unbeschränkter Informationszugang* verschafft. Problematisch und für den Betroffenen wenig transparent ist es, wenn völlig unterschiedliche Sachverhalte in der Einwilligungserklärung zusammengefaßt sind und er über die Rechtsfolgen nicht aufgeklärt wird. Die Auskünfte nach dem Strafrechtlichen Rehabilitierungsgesetz unterscheiden sich erheblich von denen, die für die Feststellung des Grades der Behinderung nach dem Schwerbehindertengesetz erforderlich sind. Es ist zweifelhaft, ob bei dieser Art der Zusammenfassung noch von einer "informierten Einwilligung" gesprochen werden kann. Der Betroffene vermag am Ende nicht zu erkennen, wer welche seiner Daten zu welchen Zwecken preisgibt. Mit den im "Volkszählungsurteil" aufgestellten Grundsätzen des Bundesverfassungsgerichts ist dies nicht vereinbar.

Soweit es unvermeidlich ist, eine Einwilligungserklärung zu formulieren, die sich auf mehrere Stellen und unterschiedliche Unterlagen bezieht, muß der Betroffene die Möglichkeit haben, seine Einwilligung auf bestimmte Stellen der Unterlagen einzuschränken. Das erfordert auf dem Formular einen entsprechenden Platz z. B. für eine Auswahlmarkierung ("bitte ankreuzen") oder ergänzende Zusatzerklärungen. Über die möglichen Folgen seiner Einschränkung, z. B. geringere Versorgungsleistungen, muß der Betroffene ausdrücklich hingewiesen werden.

Überdies ergibt sich aus § 79 SGB X, § 13 BDSG, daß personenbezogene Daten vorrangig beim *Betroffenen* (und nicht bei Dritten) zu erheben sind.

Mit einer Datenerhebung ist zudem regelmäßig eine Offenbarung verknüpft. Wenn sich das Versorgungsamt Informationen bei einem Dritten verschafft, offenbart es zugleich, daß der Betroffene Antragsteller einer Sozialleistung ist oder sie bereits bezieht. Diese Offenbarung ist gemäß § 69 Abs. 1 Nr. 1 1. Fall SGB X nur zulässig, wenn sie zur Aufgabenerfüllung erforderlich ist. Zur Aufgabenerfüllung ist sie jedoch nicht erforderlich, wenn sich die Behörde die Auskünfte vom Betroffenen selbst beschaffen kann.

Wenn der Antragsteller die Auskünfte nicht geben will, darf die Behörde auch *nicht die Daten bei Dritten erheben*. Vielmehr hat sie unter den Voraussetzungen von § 66 SGB I die Möglichkeit, die Leistung zu versagen beziehungsweise zu entziehen. Wenn hingegen der Antragsteller zwar grundsätzlich bereit, aber selbst nicht in der Lage ist, die Auskunft zu erteilen, kann die Behörde mit seiner Einwilligung die Auskünfte bei Dritten einholen. Im Bereich der Versorgungsverwaltung, in der medizinische Unterlagen eine große Rolle spielen, wird dies sehr häufig der Fall sein.

Die Diskussion mit dem Landesamt werde ich bis zu einem abschließenden Ergebnis weiterführen.

10.2.8 Fragebogen zu einem Stundungsantrag in der Ausbildungsförderung

Der Fragebogen des Amtes für Ausbildungsförderung Freiberg "Stundungsantrag/Erklärung über die persönlichen und wirtschaftlichen Verhältnisse" wurde mir von einem ehemaligen Studenten mit der Bitte um datenschutzrechtliche Prüfung zugeleitet. Das Formular dient ausschließlich der Stundung von Rückforderungsansprüchen von Leistungen, die zu Unrecht erbracht wurden (§ 20 BAföG), nicht der Rückzahlung des Darlehens gemäß § 18 a BAföG.

Rechtsgrundlage für die Stundung ist § 59 SäHO. Sie wird konkretisiert in den "Richtlinien zur einheitlichen Anwendung des Landeshaushaltsrechts bei der Veränderung von Ansprüchen nach § 50 SGB X sowie den §§ 20, 37 und 47 a BAföG" vom Oktober 1981, geändert durch Runderlaß vom 29.11.1993, und den Stundungsrichtlinien des SMWK (veröffentlicht als Nr. 6.2 der "BAföG - Teilverfahren Kasse Arbeitsanweisung" vom 1. April 1993 beziehungsweise 11. März 1993).

Auf dem Fragebogen soll eine Reihe von sensiblen Daten offenbart werden.

So werden Angaben zum Familienstand gefordert, obwohl z. B. nicht erkennbar ist, welchen Einfluß die Tatsache, daß der Antragsteller verwitwet ist, auf die Entscheidung über die Stundung haben könnte.

Zweifelhaft ist ebenfalls, ob die Angabe des Arbeitgebers erforderlich ist, zumal die Adresse der Verdienstbescheinigung zu entnehmen ist und eine Rückfrage nur in Ausnahmefällen in Betracht kommt.

Bei der Frage nach dem Kindergeld bestehen Zweifel, ob sie in dieser undifferenzierten Form vereinbar ist mit § 21 Abs. 3 Nr. 3 BAföG, wonach eine Leistung, die der Auszubildende nach dem Bundeskindergeldgesetz für seine Kinder erhält, nicht als Einnahme gilt.

Der Antragsteller soll den Beleg eines Kreditinstituts beibringen, daß eine Kreditaufnahme nicht möglich ist.
Zwar ist es durchaus gerechtfertigt, wenn von demjenigen, der zu Unrecht Leistungen erhalten hat, gefordert wird, diese zur Not unter Inanspruchnahme eines Kredits zurückzuzahlen und nicht - wenn auch nur vorübergehend - die öffentliche Hand durch eine Stundung zu belasten. Problematisch ist es jedoch, den Antragsteller zu zwingen, sich seine fehlende Kreditwürdigkeit attestieren zu lassen. Zudem ist die Bescheinigung auch kein geeignetes Mittel, die Möglichkeit zu belegen, kein Darlehen zu erhalten. Wenn jemand gezielt zur Durchsetzung seines Antrags sein Bankguthaben abhebt, wird es keine Schwierigkeit sein, an die gewünschte Bescheinigung zu kommen.

Die Forderung nach einer Sicherheitsleistung bereits bei einem Betrag von 3000,- DM scheint unverhältnismäßig und findet in den Stundungsrichtlinien des SMWK keine Basis. Sie wird allerdings in den Bundesrichtlinien erwähnt, die jedoch keine Rechts-

grundlage für eine Datenerhebung sind.

Mißverständlich ist die Formulierung, daß der Antragsteller sein Einverständnis gibt, bei fehlenden oder unvollständigen Unterlagen Auskünfte über seine Einkommensverhältnisse beim Arbeitgeber, Leistungsträger u. a. einholen zu dürfen. Zunächst muß der Antragsteller zur Ergänzung der Unterlagen aufgefordert werden. Häufig wird bei ihm ein Irrtum zugrunde liegen, wenn die Unterlagen unvollständig sind. Die Datenerhebung beim Betroffenen hat gemäß § 79 SGB X, § 13 BDSG, wie im gesamten Datenschutzrecht, stets Vorrang.

Zu berücksichtigen ist weiterhin, daß mit der Anforderung von Auskünften bei Dritten zugleich ein Sozialgeheimnis offenbart wird, zumindest, daß der Betroffene Empfänger der (Sozial-)Leistung Ausbildungsförderung ist. Diese Offenbarung ist nur unter den Voraussetzungen der §§ 67 bis 77 SGB X zulässig. Die Voraussetzungen von § 69 Abs. 1 Nr. 1 1. Fall SGB X liegen vor, wenn die Offenbarung für die Erfüllung der gesetzlichen Aufgaben erforderlich ist. Gerade daran fehlt es, wenn der Antragsteller die Auskünfte selbst geben kann.

Das Amt für Ausbildungsförderung Freiberg bezweifelt, ob auf die Stundungsentscheidung das Sozialgesetzbuch anwendbar ist. Ich vertrete jedoch diese Auffassung, weil die Stundung der Rückforderungsansprüche im engen Sachzusammenhang mit der Sozialleistung Ausbildungsförderung steht. Wenn man der Gegenauffassung folgend das SGB X nicht anwenden will, ist das Sächsische Datenschutzgesetz zu beachten. Auch hier gelten die Grundsätze der Datenerhebung beim Betroffenen (§ 11 SächsDSG) und der Erforderlichkeit der Datenerhebung (§ 13 SächsDSG); an meiner Rechtsauffassung ändert sich im Ergebnis also nichts.

In Zusammenarbeit mit dem SMWK und dem Sächsischen Landesamt für Ausbildungsförderung soll ein Musterformular entworfen werden.

10.2.9 Mitwirkung des Sozialamtes bei der Zurückstellung vom Wehrdienst

Gemäß § 12 Abs. 4 WPflG soll ein Wehrpflichtiger auf Antrag vom Wehrdienst zurückgestellt werden, wenn die Heranziehung zum Wehrdienst für ihn wegen persönlicher Gründe eine besondere Härte bedeuten würde. Solche "besonderen Härten" kommen unter anderem dann in Betracht, wenn die Einberufung des Wehrpflichtigen die Versorgung seiner Familie oder Verwandter 1. Grades gefährden würde. Der Wehrpflichtige hat deshalb seinen Antrag auf Zurückstellung zu begründen. Diese Begründung soll gemäß § 20 Abs. 1 Satz 2 WPflG von der Erfassungsbehörde, d. h. der Meldebehörde, auf ihre sachliche Richtigkeit überprüft werden. Das Gesetz sieht also vor, daß die besondere soziale und wirtschaftliche Situation des Wehrpflichtigen und seiner Angehörigen von einer Behörde nachgeprüft werden darf.
Von dieser Möglichkeit machen Kreiswehrersatzämter - also Bundesbehörden - Gebrauch, indem sie im Wege der Amtshilfe unter anderem sächsische Sozialämter um Überprüfung der Angaben des Wehrpflichtigen ersuchen. Den Sozialämtern werden 12 Fragen zur familiären und sozialen Situation des Wehrpflichtigen und seiner Angehörigen, eine vom Wehrpflichtigen und der angeblich hilfebedürftigen Person unterschriebene Einverständniserklärung sowie eine Ablichtung des Zurückstellungsantrags des

Wehrpflichtigen übermittelt. Das Sozialamt einer sächsischen Stadt wandte sich mit der Bitte um datenschutzrechtliche Überprüfung eines solchen Amtshilfeersuchens an mich. Die Bedenken des Sozialamts rührten von der Verwendung einer Personenkennziffer (PK) auf den Einverständniserklärungen des Wehrpflichtigen und seiner Angehörigen her. Es hatte außerdem grundsätzliche Zweifel an der Rechtmäßigkeit seiner Heranziehung im Rahmen eines Amtshilfeersuchens.
Ich bin nur zuständig für sächsische Behörden, konnte also hier nur die Sozialämter prüfen.
Bei der verwendeten Personenkennziffer handelte es sich um die nur im Bereich der Bundeswehr für Soldaten verwendete Personenkennziffer. Diese hat mit dem Personenkennzeichen (PKZ) der DDR nichts zu tun. Die Bundeswehr-PK darf im öffentlichen Bereich außerhalb der Bundeswehr nicht verwendet werden.
Die Vorgehensweise der Kreiswehrersatzämter halte ich für problematisch:
Wehrpflichtige und deren Angehörige, bei denen die gesundheitlichen und sozialen Verhältnisse einen Zurückstellungsantrag begründen können, werden häufig schon Sozialleistungen in Anspruch genommen haben. In diesen Fällen werden die bereits beim Sozialamt vorhandenen Daten vom *Sozialgeheimnis* gemäß § 35 SGB I geschützt. Sie dürfen auch im Rahmen eines Amtshilfeverfahrens nur unter den Voraussetzungen der §§ 67 ff. SGB X offenbart werden. Eine gesetzliche Offenbarungsbefugnis nach §§ 68 bis 77 SGB X liegt nicht vor. Deshalb kann die Offenbarung nur durch Einwilligung des Betroffenen im Einzelfall gerechtfertigt werden.
Es entspricht einem Grundanliegen des Datenschutzes, daß Einwilligungen nicht "blind" erklärt werden dürfen. Gerade unter diesem Aspekt genügt das derzeit verwendete Einwilligungsformular nicht den Anforderungen. Die Angehörigen des Wehrpflichtigen und der Wehrpflichtige selbst werden nicht über Art und Umfang der zu offenbarenden Daten, insbesondere nicht über die Tatsache, daß gerade das *Sozialamt* um Auskunft ersucht wird, aufgeklärt. Das Einwilligungsformular sagt nicht, mit welchen Mitteln (Hausbesuche?) die Daten überprüft werden sollen. Schließlich habe ich auch Bedenken gegen die für jeden Fall einheitlich vorgesehenen Fragen; im Einzelfall können Daten erhoben werden, die zur Aufgabenerfüllung gerade nicht erforderlich sind. Dies gilt z. B. für den Fall, daß die Geschwister des Wehrpflichtigen so jung sind, daß sie für die Pflege der Angehörigen nicht in Frage kommen. In diesem Fall erübrigt sich die Frage nach dem Wohnort der Geschwister.
Ich habe bisher darauf verzichtet, die Datenübermittlung an die Kreiswehrersatzämter deshalb als rechtswidrig zu bemängeln. Werden die Angaben verweigert, führt dies nämlich zur Einziehung des Wehrpflichtigen, ohne daß dieser tatsächlich vorhandene Zurückstellungsgründe beweisen kann. Mir liegt jedoch an einem gerechten Ausgleich der Interessen des Wehrpflichtigen und der Wehrersatzverwaltung.
Ich habe mich deshalb sowohl mit der Wehrbereichsverwaltung VII als auch mit dem Bundesbeauftragten für den Datenschutz in Verbindung gesetzt, um den Fragenkatalog auf die für die Entscheidung des jeweiligen Einzelfalls erforderlichen Fragen zu beschränken und den Text der Einwilligungserklärung präziser zu gestalten.

10.3 Entwurf eines Sächsischen Bestattungsgesetzes

Dem Sächsischen Landtag liegt derzeit der Entwurf eines *Bestattungsgesetzes* vor, dem ich im wesentlichen unter zwei Gesichtspunkten meine besondere Aufmerksamkeit gewidmet habe:

Zum einen betraf dies die Frage, unter welchen Voraussetzungen z. B. wissenschaftliche Einrichtungen, insbesondere Hochschulen, Unfall- und Lebensversicherungen oder auch einzelne Bürger Einsicht in die bei den Gesundheitsämtern 30 Jahre lang aufzubewahrenden Todesbescheinigungen erhalten.

Die derzeit auf dem Gebiet des Freistaates Sachsen zumindest in Teilen weitergeltende "Leichenschauanordnung" (Anordnung über die ärztliche Leichenschau vom 4.12.1978, DDR-GBl. 1979 I S. 4) sieht eine Übermittlung der Totenscheine ausschließlich zu statistischen Zwecken (§ 13 Abs. 4 der Anordnung) oder zu Zwecken des vorbeugenden Gesundheitsschutzes an die für den Kreis zuständigen Betreuungsstellen (gemäß § 16 Abs. 1 Buchst. a der Anordnung) und bei Vorliegen bestimmter Voraussetzungen zusätzlich an die Fachkommission zur Senkung der Säuglings- und Kindersterblichkeit (§ 16 Abs. 1 Buchst. b der Anordnung) vor. Eine Übermittlung der Totenscheine an andere Stellen ist nicht vorgesehen.

Abgesehen davon, daß die genannten Stellen heute nicht mehr existieren, genügt die Leichenschauanordnung auch deshalb den heutigen Anforderungen an eine Übermittlungsregelung nicht mehr, weil sich der Kreis der Auskunftbegehrenden gegenüber der Praxis in der DDR stark vergrößert hat. So sind heute vor allem Berufsgenossenschaften als Träger der gesetzlichen Unfallversicherung (§§ 507 ff. RVO), aber auch Rentenversicherungen, Bundes- und Landesbehörden sowie private Lebensversicherungen zur Erfüllung ihrer Aufgaben regelmäßig auf Auskünfte aus den Todesbescheinigungen angewiesen, z. B. darüber, ob eine Erkrankung berufsbedingt war.

Für diese Antragsteller sieht § 11 Abs. 5 Satz 2 Nr. 1 des *Entwurfs* ein Einsichtnahme- oder Auskunfterteilungsrecht vor, wenn sie ein berechtigtes Interesse an der Kenntnis der Todesumstände glaubhaft machen und kein Grund zu der Annahme besteht, daß durch die Offenbarung schutzwürdige Belange des Verstorbenen oder seiner Hinterbliebenen beeinträchtigt werden. Mit dieser Regelung bin ich einverstanden.

Demgegenüber sah § 11 Abs. 5 Satz 2 Nr. 2 des ursprünglichen Gesetzentwurfs die Möglichkeit der Einsichtnahme in oder Auskunfterteilung aus Todesbescheinigungen vor, wenn "Hochschulen oder andere mit wissenschaftlicher Forschung beauftragte wissenschaftliche Stellen die Angaben für ein wissenschaftliches Vorhaben benötigen" und die in § 30 SächsDSG normierten besonderen Voraussetzungen für die Verarbeitung personenbezogener Daten durch Forschungseinrichtungen (Zweckänderungsverbot, Anonymisierungsgebot, etc.) vorgelegen hätten. Nicht vorgesehen war eine Güterabwägung zwischen dem wissenschaftlichen Interesse an der Durchführung der Forschungsvorhaben und den Belangen des Verstorbenen und seiner Hinterbliebenen, obwohl dies aus meiner Sicht wegen der im Einzelfall erheblichen schutzwürdigen Belange dieses Personenkreises zwingend erforderlich ist.

Auf meine Anregung hin ist nunmehr im Einzelfall eine Interessenabwägung vorzunehmen. Forscher können nur dann Einsicht in die Todesbescheinigungen nehmen, wenn dem "wissenschaftlichen Interesse an der Durchführung des Forschungsvorhabens größeres Gewicht als den Belangen des Verstorbenen oder seiner

Hinterbliebenen beizumessen ist". Ferner wurde ein ausdrücklicher Hinweis auf den einschlägigen § 30 SächsDSG aufgenommen.

Eine andere Bestimmung des Gesetzentwurfs sah vor, daß der Leichenschauarzt bei verstorbenen Frauen nicht nur Angaben über eine bis zu sechs Wochen zurückliegende Schwangerschaft, sondern auch über einen vorhergegangenen Schwangerschaftsabbruch oder einen Fruchtabgang machen müsse. Dementsprechend, jedoch mit einer auf drei Monate verlängerten Frist, war in dem Mustervordruck für den vertraulichen Teil der Todesbescheinigung folgende Frage vorgesehen: "Erfolgte in den letzten 3 Monaten eine Entbindung, eine Interruptio, ein Abort?".

Ich habe grundsätzliche Bedenken gegen die vorgesehene gesonderte Erhebung von Daten über einen zurückliegenden Schwangerschaftsabbruch oder Fruchtabgang geltend gemacht. Soweit Schwangerschaftsabbrüche oder Fruchtabgänge oder damit zusammenhängende Handlungen für den Tod der Frau mitursächlich waren, werden diese Umstände schon als "Todesursache, klinischer Befund" erfaßt. Soweit diese Umstände nichts mit der Todesursache zu tun haben, ist ihre Erhebung nicht erforderlich. Gründe, die eine gesonderte Erfassung dieser Daten rechtfertigen könnten, sind nicht ersichtlich. Insbesondere sehen auch die Empfehlungen der Weltgesundheitsorganisation (WHO; abgedruckt in: "Beitrag zur Abschätzung der Aussagekraft der amtlichen Todesursachenstatistik", Schriftenreihe des BMJ-FFG, Bd. 252) lediglich die Erfassung sogenannter "mittelbarer Müttersterbefälle" vor. Als mittelbare Müttersterbefälle gelten "solche, die von einer Vorerkrankung oder einer Erkrankung während der Schwangerschaft herrühren, die nicht unmittelbar geburtshilfliche Ursachen hatte, die aber durch physiologische Wirkungen der Schwangerschaft verschlimmert wurde" (Nr. 11 Definitionen und Empfehlungen). Ein Schwangerschaftsabbruch oder ein Fruchtabgang sind gerade keine Vorerkrankungen oder keine Erkrankungen während der Schwangerschaft, die durch die Wirkungen der Schwangerschaft verschlimmert werden. Die Frage nach diesen beiden Erhebungsmerkmalen ist daher nach den Empfehlungen der WHO sinnlos. Zum Zwecke der Durchführung einer Statistik über mittelbare Müttersterbefälle ist allerdings nicht zu beanstanden, daß nach einer vorhergehenden *Schwangerschaft* der Verstorbenen gefragt wird. Ich werde daher das Gesetzgebungsverfahren weiter mit dem Ziel einer ersatzlosen Streichung der Fragen nach Abbruch oder Abgang begleiten.

11 Landwirtschaft, Ernährung und Forsten

11.1 Allgemeines

Ich bin in diesem Bereich mit einigen Vorgängen befaßt, die sich datenschutzrechtlich zur Zeit noch nicht abschließend beurteilen lassen.
Das SML tut sich im Schriftverkehr mit meiner Dienststelle durch besonders lange Antwortzeiten hervor.

11.2 Das integrierte Verwaltungs- und Kontrollsystem der EU (InVeKoS)

Das im 1. Tätigkeitsbericht unter 11.1 erwähnte System befindet sich im Aufbau. Es soll gemäß der Verordnung (EWG) Nr. 3508/92 des Rates vom 27. November 1992 und der Verordnung (EWG) Nr. 3887/92 der Kommission vom 23. Dezember 1992 für eine ordnungsgemäße Durchführung des neuen EU-Systems der Landwirtschaftsförderung sorgen und insbesondere die mißbräuchliche Verwendung von Fördermitteln verhindern. Es sollen Daten über Flurstücke, die Art deren landwirtschaftlicher Nutzung sowie den Tierbestand erhoben und in großen Datenbanken verarbeitet werden.

Die befürchtete Fernerkundung mittels Satelliten- oder Flugzeugaufnahmen wird aus technisch-finanziellen Gründen vorerst nicht stattfinden.
Soviel will ich aber bereits jetzt sagen: Wer - wie die Landwirte in großem Umfang - aus welchen Gründen auch immer von Leistungen der Allgemeinheit, d. h. von Steuermitteln, lebt, wer also am Tropf des Staates hängt, der muß für die Richtigkeit seiner Angaben z. B. in Förderungsanträgen einstehen. Ähnlich wie im Sozialbereich muß er damit rechnen, aufmerksam kontrolliert zu werden. Denn falsche Angaben oder antragswidriges Verhalten muß dazu führen können, daß staatliche Leistungen eingestellt und zurückgefordert werden und bewußtes Fehlverhalten strafrechtliche Ermittlungen nach sich zieht.

Die Daten, die aus der Luft (per Satelliten oder Flugzeug) erhoben werden, sind allgemein zugänglich. Das Problem besteht in der zeitlichen Unbeschränktheit, der Flächendeckung, der fehlenden Kenntnis des Betroffenen von der konkreten Kontrolle, der - möglicherweise stattfindenden - Verknüpfung mit anderen Daten, der Zweckänderung (z. B. für die Bauaufsicht) und der rechtzeitigen Löschung der Daten.

All dies wird in Fachkreisen lebhaft diskutiert. Ich werde mich weiter dafür einsetzen, daß ein datenschutzgerechtes - aber auch wirksames - Kontrollverfahren auf EG-Ebene erarbeitet wird. Eine allzu starke Kompetenz der Regionen bei der Auswertung ist mir weniger recht (Bedenken gegen deren Zuverlässigkeit bei ihrer Tätigkeit konnte ich bislang nicht zerstreuen) als eine automatisierte Datenverarbeitung auf EG-Ebene mit einem exakten Programm, in dem alle technischen Vorkehrungen gegen zweckwidrige Verwendung sowie im Sinne des § 9 SächsDSG getroffen sind.

Ein wesentliches Problem ist der gegenüber Rechtsvorschriften der EG/EU sowie auf diesen beruhendem nationalem Verwaltungshandeln eingeschränkte Schutz der informationellen Selbstbestimmung.

12 Umwelt und Landesentwicklung

Rechtsvorschriften über den freien Zugang zu Informationen über die Umwelt

Wie in Kapitel 12 meines 1. Tätigkeitsberichts ausführlich dargestellt, bin ich an der Ausarbeitung einer (vorläufigen) Verwaltungsvorschrift des Umweltministeriums (Erlaß des Sächsischen Staatsministeriums für Umwelt und Landesentwicklung zur unmittelbaren Anwendbarkeit der Richtlinie des Rates der Europäischen Gemeinschaften vom 7. Juni 1990 über den freien Zugang zu Informationen über die Umwelt [90/313/EWG] vom 17.2.1993) in erfreulicher Weise beteiligt worden.

Der Erlaß ist so gestaltet, daß er *jeden* Eingriff in das Grundrecht auf informationelle Selbstbestimmung (und auch in andere Grundrechte!) zu unterlassen gebietet, also personenbezogene oder personenbeziehbare Umweltdaten von der Bekanntgabe *ausschließt.*

Auf diese Zurückhaltung hatte ich seinerzeit auch deswegen gedrungen, weil ich unter dem Gesichtspunkt der erforderlichen Normenklarheit gerade im Hinblick auf den möglichen Eingriff in das Grundrecht auf informationelle Selbstbestimmung - von den Eingriffen in andere Grundrechte abgesehen - entgegen der damals nahezu allgemeinen Meinung (z. B. auch des Bundesumweltministeriums) *erhebliche rechtliche Bedenken dagegen* angemeldet habe, daß die Richtlinie tatsächlich die Anforderungen erfüllt, die nach der Rechtsprechung des Europäischen Gerichtshofes an die - ausnahmsweise - unmittelbare Wirkung einer EG-Richtlinie zu stellen sind. Bestätigung gefunden haben diese Vorsicht und meine Zweifel an der unmittelbaren Geltung der Richtlinie durch eine der beiden bisher dazu vorliegenden verwaltungsgerichtlichen Entscheidungen, die nach überzeugenden Erwägungen zu dem Ergebnis kommt, es sei *offenkundig*, daß es der Richtlinie an der nötigen *Unbedingtheit* und *Bestimmtheit* fehle (VG Stade, 7. Kammer Lüneburg, Urteil vom 21.4.1993 - 7 A 79/92 - rechtskräftig; NVwZ 1994, 201).

Datenschutzrechtliche Probleme sind mir im Zusammenhang mit der Anwendung des Erlasses durch den dem SMU nachgeordneten Bereich (bei einigen hundert Anträgen im Jahr 1993) bisher nicht bekannt geworden.

Die Bundesregierung hat inzwischen endlich einen überarbeiteten Entwurf eines Gesetzes zur Umsetzung der Richtlinie des Rates vom 7. Juni 1990 über den freien Zugang zu Informationen über die Umwelt (90/313/EWG) - Umweltinformationsgesetz (UIG) beschlossen und dem Bundesrat zur Stellungnahme zugeleitet; der Bundesrat hat sich in seiner Sitzung am 17.12.1993 mit dem Entwurf befaßt. Ich habe gegenüber diesem Gesetzgebungsvorhaben im Interesse des gebotenen Schutzes des Grundrechts auf informationelle Selbstbestimmung mehr Vorbehalte geäußert als die meisten meiner Kollegen.
Der Gesetzentwurf ist zur Zeit dem Bundestag noch nicht zugeleitet worden, es ist jedoch zu erwarten, daß dies in den nächsten Wochen geschieht.

13 Wissenschaft und Kunst

13.1 Sächsisches Hochschulgesetz

Zu den wichtigsten Vorhaben im Bereich der Hochschulen gehörte die Verabschiedung des Sächsischen Hochschulgesetzes.

Der Sächsische Landtag hat nach gründlicher Beratung im Ausschuß für Wissenschaft und Hochschulen mit § 135 SHG eine bereichsspezifische Datenschutzregelung geschaffen, die von mir vorgeschlagen worden war.

Absatz 1 nennt die Zwecke, für die Daten der Studienbewerber, Studenten, Prüfungskandidaten und externen Nutzer von Hochschuleinrichtungen verarbeitet werden dürfen. Das sind insbesondere die Immatrikulation, Rückmeldung, Teilnahme an Lehrveranstaltungen, Prüfungen, Nutzung von Hochschuleinrichtungen und die Hochschulplanung. Das SMWK wird ermächtigt, durch Rechtsverordnung zu bestimmen, welche personenbezogenen Daten für diese Zwecke verarbeitet werden dürfen. Der Entwurf einer solchen Rechtsverordnung (vgl. 13.4) liegt bereits vor.

Absatz 2 regelt die Voraussetzungen einer Übermittlung personenbezogener Daten.

Das Sächsische Hochschulgesetz versucht, in einigen Bereichen neue Wege zu beschreiten. Dazu gehören gemäß § 108 Abs. 3 regelmäßige Befragungen der Studenten zur Qualität der Lehrveranstaltungen; sie werden von der Studienkommission im Zusammenwirken mit den studentischen Fachschaftsräten durchgeführt. Das Ergebnis findet Eingang in den von der Hochschule jährlich vorzulegenden Lehrbericht (§ 14).
So sehr der Versuch zu begrüßen ist, der Lehre ein größeres Gewicht zu verschaffen, so sind doch die mit solchen Aktionen verbundenen datenschutzrechtlichen Probleme nicht zu übersehen. Daher wurde auf meine Anregung in Absatz 3 eine Regelung aufgenommen, die einen Rahmen für die Befragungen setzt. Die Hochschulen können Daten des wissenschaftlichen und künstlerischen Personals zur Beurteilung der Lehrtätigkeit verarbeiten. Das SMWK wird ermächtigt, durch Rechtsverordnung zu regeln, unter welchen Voraussetzungen eine Auskunftspflicht besteht oder ob eine Erhebung ohne Einwilligung der Betroffenen durchgeführt werden darf. Zweck, Inhalt und Umfang der Auskunftspflicht, die Erhebungsmerkmale und das Verfahren sind in der Rechtsverordnung festzulegen. Dazu gehören insbesondere Regelungen über die Erhebung und Speicherung der personenbezogenen Daten, das Verfahren der Auswertung, die Übermittlung (insbesondere Bestimmung der berechtigten Empfänger), weiterhin über die Unterrichtung der Betroffenen und ihre Auskunftsrechte. Eine Verarbeitung der Daten für andere Zwecke ist unzulässig. Die personenbezogenen Daten befragter Studenten sind zum frühestmöglichen Zeitpunkt zu anonymisieren.

13.2 Entwurf des Sächsischen Graduiertengesetzes

§ 26 Abs. 7 SHG sieht ein Graduiertenstudium im Anschluß an das berufsqualifizierende Studium vor. Es soll in besonderer Weise zur selbständigen wissenschaftlichen Forschung oder künstlerischen Tätigkeit befähigen und der

Vorbereitung der Promotion oder künstlerischen Weiterentwicklung dienen. Die Besonderheit gegenüber dem üblichen Promotionsverfahren besteht darin, daß es aufgrund einer Studienordnung und in einer Regelstudienzeit durchzuführen ist.

Diese Trennung des Studiums in einen berufsqualifizierenden und in einen darauf aufbauenden forschungsorientierten Teil entspricht einer in der bildungspolitischen Diskussion häufig erhobenen Forderung. Zweck ist nicht zuletzt auch der Wunsch, das Promotionsverfahren durch eine stärkere Strukturierung zu beschleunigen.

Der Entwurf enthält in § 4 Abs. 6 eine sehr allgemein gehaltene Datenverarbeitungsbestimmung. Nach Maßgabe der Immatrikulationsordnung der Universität dürfen auf der Grundlage der datenschutzrechtlichen Bestimmungen von den Bewerbern die personenbezogenen Informationen erhoben werden, die für den Vollzug des Gesetzes und der auf dieses gestützten Rechtsvorschriften erforderlich sind.

Ich habe in Anlehnung an § 135 Abs. 1 SHG (vgl. vorstehend unter 13.1) angeregt, die Zwecke, für die eine Datenverarbeitung zulässig ist, im Gesetz zu nennen. Aufzunehmen ist außerdem eine Ermächtigung für das SMWK, durch Rechtsverordnung zu bestimmen, welche personenbezogenen Daten für diese im Gesetz - wenn auch leider nicht abschließend - genannten Zwecke verarbeitet werden dürfen. Im übrigen ist § 135 SHG entsprechend anzuwenden.

Die Gesetzgebungsarbeiten sind noch nicht abgeschlossen.

13.3 Promotions- und Habilitationsordnungen

Eine Promotionskommission einer sächsischen Hochschule legte mir eine Promotions- und eine Habilitationsordnung zur datenschutzrechtlichen Prüfung vor. Im Falle einer anderen Promotionsordnung war es das SMWK, das mich bat, diese datenschutzrechtlich "abzuklopfen".

Die Promotionsordnungen unterscheiden sich in zahlreichen Einzelregelungen, zu denen ich mich - soweit nötig - geäußert habe. Ein gemeinsames Problem ist jedoch die Frage, was nach Abbruch oder erfolgreicher Beendigung des Promotionsverfahrens mit den Unterlagen zu geschehen hat. Der Promovend muß mit dem Antrag zahlreiche Unterlagen einreichen, z. B. einen Lebenslauf und Zeugnisse. Die Vielzahl der Gründe für einen Abbruch, das unterschiedlich fortgeschrittene Verfahrensstadium und der Zweck einer weiteren Aufbewahrung erfordern eine differenzierte Lösung. Bei Abbruch ist gegen eine Aufbewahrung der Dissertation und der Antragsunterlagen bis zum rechtskräftigen Abschluß eines gegen die ablehnende Entscheidung gerichteten verwaltungsgerichtlichen Verfahrens nichts einzuwenden, weil die Unterlagen für die Beweissicherung erforderlich sind. Nach Abschluß des verwaltungsgerichtlichen Verfahrens beziehungsweise nach Ablauf der Rechtsmittelfristen ist es nicht mehr nötig, die Unterlagen aufzubewahren; sie sind dem Archiv anzubieten.

In den Promotionsordnungen ist eine Aufbewahrung durch das Archiv nach ordnungsgemäßem Abschluß des Promotionsverfahrens vorgesehen. Nach dem

Sächsischen Archivgesetz hat jedoch das Archiv im Benehmen mit der anbietenden Stelle, z. B. der Geschäftsstelle für Promotions- und Habilitationsangelegenheiten, über die Archivwürdigkeit zu entscheiden (§§ 14 Abs. 2, 13 Abs. 3, 5 Abs. 4 SächsArchG). Dies spricht gegen eine obligatorische Übernahme aller Unterlagen.

Diese Argumente habe ich dem SMWK vorgetragen, das sie im weiteren Genehmigungsverfahren berücksichtigen will.

13.4 Entwurf der Verordnung zur Verarbeitung personenbezogener Daten von Studenten

Das Sächsische Hochschulgesetz enthält eine Vielzahl - nach Ansicht mancher Kritiker eine zu hohe Zahl - von Verordnungsermächtigungen für das SMWK. Dazu gehört § 135 Abs. 1 S. 2 SHG. Das Ministerium wird ermächtigt, durch Rechtsverordnung zu bestimmen, welche personenbezogenen Daten für die in Satz 1 der Vorschrift genannten Zwecke verarbeitet werden dürfen (vgl. 13.1).

Das SMWK hat mir den Entwurf der "Verordnung des Sächsischen Staatsministeriums für Wissenschaft und Kunst zur Erhebung und Verarbeitung personenbezogener Daten der Studienbewerber, Studierenden und Prüfungskandidaten für Verwaltungszwecke der Hochschulen" vorgelegt, zu dem ich mich ausführlich geäußert habe.

An einigen Stellen habe ich auf eine Abweichung von der Systematik des Sächsischen Hochschulgesetzes hingewiesen. So unterscheidet z. B. der Verordnungsentwurf zwischen der Aufhebung der Immatrikulation und der Exmatrikulation, eine Differenzierung, die dem Sächsischen Hochschulgesetz fremd ist.

Weiterhin wurde in einigen Fällen eine Befugnis zur Verarbeitung von Daten eingeräumt, die keine Stütze im Sächsischen Hochschulgesetz findet. So wird nach dem Verlust des Prüfungsanspruchs in einem *verwandten* Studiengang gefragt, während nach den §§ 18 Abs. 1 Nr. 4, 20 Abs. 2 Nr. 5 SHG nur der Verlust des Prüfungsanspruchs im *gewählten* Studiengang von Bedeutung ist. Ein weiteres Beispiel ist die Frage nach Vorprüfungen und deren Note. Nach dem Sächsischen Hochschulgesetz sind diese Angaben für die Immatrikulation ohne Bedeutung (§§ 18 Abs. 1 Nr. 4, 20 Abs. 2 Nr. 3).

Der Entwurf wird zur Zeit auf meine Anregung im SMWK überarbeitet.

13.5 Personalakteneinsichtsrecht im Hochschulbereich

Bei Kontrollbesuchen und durch eine Eingabe habe ich festgestellt, daß im Bereich des SMWK Betroffenen oft eine nicht vollständige Einsicht in die zu ihrer Person geführten Personalakten gewährt wird. Auch werden diejenigen Bestandteile von Akten der Personalkommissionen, die z. B. die Interessen Dritter berühren, nicht in die bei den Hochschulen geführten Personalakten aufgenommen. Interessen Dritter sollen nach Auffassung des Ministeriums angeblich auch dann berührt sein, wenn der Dritte im Rahmen der Überprüfung auf Stasi-Vergangenheit eine belastende Aussage gegenüber dem Auskunftssuchenden gemacht hat, diese vertraulich behandelt haben wollte und

ihm dies auch zugesagt wurde. Zum Schutz des Dritten sollten diese Informationen dann nicht der belasteten Person zugänglich gemacht werden.

Diese Verfahrensweise des SMWK ist unzulässig. Nach § 13 Abs. 1 Satz 1 BAT hat der Angestellte ein Recht auf Einsicht in seine *vollständigen* Personalakten. Dieses Recht gilt uneingeschränkt. Ein Akteneinsichtsrecht gewährt weiterhin § 17 Abs. 3 Satz 1 SächsDSG. Dieses Recht kann nach § 17 Abs. 5 Satz 1 SächsDSG zwar beschränkt werden, wenn die Geheimhaltungsinteressen der speichernden Stelle oder eines Dritten die Interessen des Betroffenen an der Auskunftserteilung überwiegen. Soweit es sich um Personalakten handelt, geht jedoch § 13 Abs. 1 S. 1 BAT als bereichsspezifische Vorschrift dem SächsDSG vor (§ 2 Abs. 4 SächsDSG).

Bei den Akten der Personalkommissionen, die im Zusammenhang mit der Überprüfung von Hochschulbeschäftigten auf ihre Stasi-Vergangenheit tätig wurden, handelt es sich ihrem gesamten Inhalt nach um Personalakten. Nach ständiger Rechtsprechung sind Personalakten Sammlungen von Urkunden und Vorgängen, die die persönlichen und dienstlichen Verhältnisse des Bediensteten betreffen und in einem *inneren Zusammenhang mit dem Dienstverhältnis* stehen. Zu diesem in unmittelbarem Zusammenhang mit dem Dienstverhältnis stehenden Vorgängen gehören auch die Unterlagen, die die maßgebenden Hintergründe der jeweiligen Personalentscheidung erhellen. Deshalb handelt es sich bei den Akten der Personalkommission, deren Aufgabe es war, dem SMWK Empfehlungen zur Abberufung oder Kündigung von Mitarbeitern zu geben, grundsätzlich um Personalakten. Unter Beachtung des Grundsatzes der Vollständigkeit der Personalakten ergibt sich, daß zu den Personalakten auch für den Betroffenen nachteilige Mitteilungen Dritter gehören, die sich auf das persönliche Verhalten des Betroffenen beziehen.
Auf die physische Einfügung des Schriftstückes in die Akte kommt es dabei nicht an.

Festzuhalten ist somit, daß dem Betroffenen nach § 13 Abs. 1 Satz 1 BAT ein Recht auf Einsicht in seine vollständigen Personalakten einschließlich der für ihn nachteiligen Tatsachenbehauptungen Dritter zusteht. Die Interessen Dritter an einer vertraulichen Behandlung ihrer Mitteilung bleiben unberücksichtigt. Hieran ändert sich auch nichts, wenn die Behörde vorher Vertraulichkeit zugesagt hat. Solche Zusagen waren rechtswidrig.

Verwaltungs- oder Gerichtsentscheidungen können sich schon wegen des verfassungsrechtlich garantierten Rechtsstaatsprinzips nur in ganz seltenen, gesetzlich geregelten Ausnahmefällen auf - aus der Sicht des Betroffenen anonyme - Hinweise stützen: Im Rechtsstaat sind Roß und Reiter zu nennen. Wie soll sich der Betroffene sonst mit Aussicht auf Erfolg gegen geheime Anwürfe und Beschuldigungen wehren können?

13.6 Weitergabe von Personaldaten einer sächsischen Hochschule an den Deutschen Akademischen Austauschdienst (DAAD)

Aufgrund einer Eingabe habe ich festgestellt, daß der DAAD die Ergebnisse der Personalüberprüfungen nach §§ 75 ff. SHEG bei einer sächsischen Hochschule

angefordert hatte.

Als Selbstverwaltungsorganisation der Hochschulen in der Bundesrepublik Deutschland hat der DAAD die Rechtsform eines eingetragenen Vereins, dessen Mitglieder die in der Hochschulrektorenkonferenz vertretenen Hochschulen und deren Studentenschaften sind. Damit ist der DAAD eine nicht-öffentliche Stelle, an die nach § 31 Abs. 2 S. 1 SächsDSG Beschäftigtendaten nur aufgrund eines Gesetzes oder mit Einwilligung des Betroffenen übermittelt werden dürfen. Da im vorliegenden Fall weder eine gesetzliche Grundlage noch eine Einwilligung vorlag, durfte die Hochschule keine Auskünfte an den DAAD erteilen. Auch die Ausnahmevorschrift des § 31 Abs. 2 S.3 SächsDSG erlaubt keine Auskunftserteilung, da die Auskunft nicht im Dienstverkehr zwingend erforderlich war. Diese Vorschrift ist eng auszulegen und hat sich an § 31 Abs. 1 SächsDSG zu orientieren, wonach Daten von Beschäftigten generell nur dann verarbeitet werden dürfen, wenn dies zur Eingehung, Durchführung oder Beendigung des Dienst- oder Arbeitsverhältnisses erforderlich ist. Ein solcher Fall lag hier nicht vor.

Auf diese Rechtslage habe ich die Hochschule aufmerksam gemacht.

13.7 Entwurf des Sächsischen Berufsakademiegesetzes

Der Gesetzentwurf verknüpft das wissenschaftsorientierte Studium an der Staatlichen Studienakademie mit einer praktischen Ausbildung in einer Bildungsstätte der Praxispartner; dies sind gemäß § 1 Abs. 2 Betriebe der Wirtschaft, vergleichbare Einrichtungen außerhalb der Wirtschaft (insbesondere der freien Berufe) und soziale Einrichtungen.

§ 19 regelt die Datenverarbeitung. Da die Aufgaben der Staatlichen Studienakademie und der Hochschulen hinreichend ähnlich sind, habe ich empfohlen, die Vorschrift an § 135 SHG (vgl. unter 13.1) anzugleichen. Dieser Vorschlag wurde vom SMWK aufgegriffen.

13.8 Kerndokumentation Rheuma

Bundesweit werden 21 vom Bundesministerium für Gesundheit geförderte Zentren errichtet, deren Aufgabe die Verbesserung der Versorgung chronisch kranker Rheumapatienten ist. Zu diesen Einrichtungen gehört das Rheumazentrum der Universität Leipzig.

Ziel ist eine ständige Qualitätsverbesserung in der Diagnostik, der Therapie und der Rehabilitation. Ein Element der Qualitätsverbesserung stelle, wie mir die Universität Leipzig mitteilte, die *Kerndokumentation Rheuma* dar, die in allen 21 Modellregionen erstellt werden solle und die in Berlin bereits im zweiten Jahr eingesetzt werde.

Der Patient erhält einen Fragebogen; erbeten werden Angaben unter anderen über den Krankheitsbeginn und die Behandlung, aber auch darüber, ob er mit einem (Ehe-)Partner zusammenlebt oder allein lebt sowie zur beruflichen Situation. In einem Anschreiben wird der Patient über das Vorhaben unterrichtet.

Der behandelnde Arzt erhält einen Fragebogen mit Angaben zu Diagnose und Therapie.

Auf beiden Bögen erscheint der Name des Patienten nicht. Der Arzt gibt Geburtsjahr, Geschlecht und Staatsangehörigkeit an.

Auf die Bögen wird eine Identitätsnummer geklebt, um spätere Fragebögen desselben Patienten mit früheren Bögen zusammenführen zu können. Ein dritter Aufkleber ist für die Patientenakte vorgesehen. Auf diese Weise könne, so die Universität Leipzig, eine Verlaufskontrolle erfolgen.

Gegenüber dem ursprünglichen Entwurf sind im Patientenfragebogen einige datenschutzrechtliche Verbesserungen zu verzeichnen. Zunächst wurde die Angabe der Gemeinde mit Postleitzahl und bei Großstädten des Stadtteils erbeten. Gegen die Angabe der Postleitzahl haben die Landesdatenschutzbeauftragten Bedenken geäußert, weil die neue fünfstellige Postleitzahl kleine räumliche Einheiten erfaßt und damit die Gefahr einer Identifizierung steigt. Daher wird nun stattdessen lediglich die Angabe des Landkreises, zu dem der Wohnort gehört, erbeten, und bei Großstädten der Stadtteil.
Weiterhin wurde die Angabe der Nationalität auf "deutsch" und "andere" beschränkt. Die Frage nach Zwillingsgeschwistern entfällt.

Ich überlege gemeinsam mit der Universität Leipzig, welche datenschutzrechtlichen Verbesserungen erreicht werden können.

14 Technischer Datenschutz

14.1 Datenschutz beim Personalcomputer

Personalcomputer (PC) werden in allen Bereichen der öffentlichen Verwaltung - meist zur Textverarbeitung - eingesetzt.
Sie werden auch zu Tabellenkalkulationen (z. B. Planungsübersichten, Budgetberechnung) und zur Arbeit mit Datenbanken (z. B. Adreßverzeichnisse, Informationssysteme, Auswertung von Statistiken) genutzt. In diesen Fällen werden oft personenbezogene Daten verarbeitet. Deren Schutz ist jedoch meist nur mangelhaft gewährleistet.

14.1.1 Datenschutz im Betriebssystem MS-DOS

Das auf PC übliche Betriebssystem ist MS-DOS. Es ist weltweit mehr als 70 Millionen mal im Einsatz. Trotz dieser enormen Verbreitung ermöglicht MS-DOS nicht die Einhaltung der Mindestanforderungen des Datenschutzes.

Wichtigste Schwachstellen sind:

- Zugangs- und Benutzerkontrolle (keine Benutzerkennung, kein Paßwort)
- Zugriffs- und Speicherkontrolle (jeder Benutzer hat Zugriff auf alle Dateien, keine Unterscheidung von Lese-, Schreib- und Ausführungsberechtigung)
- Eingabekontrolle (keine Protokollierung)
- Übermittlungs- und Transportkontrolle (unkontrollierbarer Diskettenbetrieb, Zugang zu seriellen Schnittstellen, z. B. Maus)
- Datenträgerkontrolle (physisches Löschen nicht möglich).

Deshalb ist ein PC unter dem Betriebssystem MS-DOS ohne zusätzliche Sicherheitsvorkehrungen für eine Verarbeitung personenbezogener Daten nicht geeignet.

Erst mit zusätzlicher Hard- und Software kann ein Standard erreicht werden, der auch die datenschutzgerechte Verarbeitung personenbezogener Daten zuläßt.
Dies gilt nicht nur für den Einzelplatz-PC, sondern auch für den lokal vernetzten PC unter MS-DOS.

Aus den genannten Schwachstellen ergeben sich folgende *zusätzlich* zu erfüllenden Anforderungen an Datenschutz und Datensicherheit bei der Anwendung von MS-DOS:

- Zugriffssicherung
    - ° Identifikation und Authentifikation des Benutzers,
    - ° Sperren der Betriebssystemebene,
    - ° lückenlose Menüführung,
    - ° Sperren des PC nach drei aufeinander folgenden Anmeldefehlversuchen,
    - ° Sperren nicht benötigter Laufwerke,
    - ° Verschlüsseln und Sperren von Dateien und Verzeichnissen,
- Benutzerkontrolle
    - ° Benutzer ist auf Identität und Zugriffsrecht zu überprüfen, unberechtigte Benutzer sind abzuweisen (maximal drei Fehlversuche),
    - ° Benutzerprofile dokumentieren; Benutzerkreis muß überprüfbar sein

(z. B. über einen Zeitraum von drei Jahren); Zuweisen benötigter Ressourcen für einzelne Benutzer,

- Kopierschutz
  - ° Sichere Menüführung, die den Zugang zum Betriebssystem verhindert oder einschränkt (Sperren des COPY-Befehls),
  - ° diskettenlose PC einsetzen ,
- Bootschutz
  - ° Unberechtigtes Laden des Betriebssystems mittels Bootdiskette verhindern durch Sperren des Laufwerkes,
- Sperren des PC
  - ° Abschließen des PC bei Abwesenheit,
  - ° Sperren der Tastatur bei Abwesenheit,
  - ° Anhalten und Sperren des PC, wenn keine Tastaturaktivität erfolgt (time-out),
- Virenschutz
  - ° Lokalisieren, Erkennen und Beseitigen von Viren,
- Automatische Protokollierung aller sicherheitsrelevanten Ereignisse
  - ° Mindestprotokolldaten: Zeitpunkt An- und Abmeldung, genutzte Programme und Daten,
- Technische Sicherheitsvorkehrungen
  - ° Notstromversorgung (kurzzeitiger Stromausfall (z. B. Gewitter) kann zu Datenverlusten führen),
  - ° regelmäßige Datensicherung und Reorganisation,
  - ° Physisches Löschen von Dateien und Datenträgern durch Überschreiben.

Dazu werden gegenwärtig eine Vielzahl von MS-DOS-Sicherheitssystemen und -zusätzen auf dem Markt angeboten.
In der Mehrzahl der Fälle handelt es sich um Zugangsschutzsysteme, die mit gängigen Authentisierungsverfahren über USER-Identifikation (Benutzerkennung) und Paßwort (vereinzelt auch mit Chipkarte) den Zugang zur Festplatte schützen. Damit die Benutzeranmeldung nicht umgangen werden kann, muß der Systemstart ('booten') über das Diskettenlaufwerk durch zusätzliche Hardwareeinrichtungen verhindert werden. In der Regel sind solche "Boot-Protection-Einrichtungen" spezielle Steckkarten. Auch ein Abschließen des Laufwerkes mit einem Diskettenschloß kann unberechtigtes Booten verhindern.
Für den Zugriffsschutz bieten viele Sicherheitszusätze zwar oft durchaus wirksame, aber im Vergleich mit Multi-User-Systemen (wie z. B. UNIX) wenig flexible Mechanismen an. Es lassen sich zwar große Bereiche der Festplatte vor unberechtigtem Zugriff schützen, aber ein Schutz kleinerer ausgewählter Bereiche (z. B. Dateien) ist oft nicht möglich. Das Schutzraster ist folglich zu grob.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI, Godesberger Allee 183, 53175 Bonn, Telefon (02 28) 9 58 20, Telefax (02 28) 9 58 24 00) hat einige Sicherheitsprodukte geprüft und zertifiziert. Das Sicherheitsprodukt ist abhängig vom Schutzbedarf der Daten und der Sensibilität der zu verarbeitenden personenbezogenen Daten auszuwählen. Das BSI vergibt bei der Zertifizierung eines Produktes sog. "Funktionalitätsklassen" und "Qualitätsstufen". Die *Funktionalitätsklasse* gibt Auskunft über die Sicherheitsfunktionen, die ein Datenverarbeitungssystem erfüllt. Die *Qualitätsstufe* be-

schreibt, welchen Angriffen die einzelnen Sicherheitsfunktionen standhalten. Der Anwender kann hiernach das für ihn geeignete Sicherheitssystem auswählen.
Sicherheitssoftware muß mindestens folgende Anforderungen erfüllen:

Identifikation und Authentisierung des Benutzers,
Verwaltung der Zugiffsberechtigung, d. h. Einrichtung und Löschung von Zugriffsberechtigungen,
Prüfung der Berechtigung des Nutzers für jeden Zugriff,
Protokollierung.

Fachzeitschriften informieren ausführlich über den Einsatz und Test von Produkten zur PC-Sicherheit. Deren Wirksamkeit bleibt aber in erster Linie von der Sorgfalt des jeweiligen PC-Administrators (Systemverwalters) abhängig. Dieser muß eine Datenschutzkonzeption entwickeln und sie umsetzen.

14.1.2 Datenschutz im Umfeld des PC

Daten können verfälscht, zerstört, entwendet werden oder verloren gehen. Die Gefahren reichen von technischem und menschlichem Versagen über bewußtes Herbeiführen eines Schadens bis hin zu höherer Gewalt. In einer "Schwachstellenanalyse" sollen Risiken erkannt und organisatorische sowie technische Gegenmaßnahmen empfohlen werden:

Risiko : *Bedienungsfehler*
Maßnahmen : - sorgfältige Schulung
- Einsatz von Software mit lückenloser Menüführung

Nach Untersuchungen der Zeitschrift für Kommunikations- und EDV-Sicherheit (KES 1992, Heft 4 S. 268) sind über 83% aller Schadensfälle auf Irrtümer, Nachlässigkeit und Spieltrieb der Mitarbeiter, d. h. auf menschliches Versagen zurückzuführen. Ausgeklügelte Sicherheitstechnik bringt wenig, wenn sie wegen menschlicher oder organisatorischer Schwächen nicht oder nicht konsequent genutzt wird. Die menschliche und weniger die technische Seite spielt bei den Fragen von Datenschutz und -sicherheit nach wie vor die entscheidende Rolle.
Ein PC ist nur so sicher wie sein unzuverlässigster Benutzer.

Risiko : *Ausfall der Hardware* (Überspannung, Spannungsschwankungen, Stromausfall)
Maßnahmen : - USV-Geräte (unterbrechungsfreie Stromversorgung) für den einzelnen PC oder für Computer mit zentralen Aufgaben im PC-Netz (Server)

Risiko : *Wasserschäden*
Maßnahmen : - Installation von Wasser-/Feuchtigkeitsmeldern
- Auslagern der Datenträger z. B. in einen Sicherheitsschrank (Data Safe)

Risiko: *Zerstörung durch Brand- oder Hitzeeinwirkung*
Maßnahmen : - Installation von Brandmeldeeinrichtungen

- Auslagern von Datenträgern in Data Safe

Risiko: *Verlust der Daten und Programme durch Diebstahl oder Sabotage*
Maßnahmen :
- Sicherung der Räume, Türen und Fenster
- Befestigen der Geräte an Möbel oder Mauerwerk
- Installation des Servers in besonders geschütztem Raum

Die Gebäudesicherung wird im PC-Bereich häufig vernachlässigt. Jedoch kann ein wirksamer Schutz durch wenige bauliche und organisatorische Maßnahmen (z. B. Einbau von Sicherheitsschlössern, Tür mit Knauf nach außen, Überwachung der Schlüsselvergabe) erreicht werden.

Organisatorische Maßnahmen: Um bei allen Mitarbeitern das notwendige Bewußtsein für den Datenschutz zu bilden, sind organisatorische Maßnahmen erforderlich. Ihnen müssen von den Verantwortlichen genaue Regelungen (z. B. Dienstanweisungen) an die Hand gegeben werden.
Zu den organisatorischen Maßnahmen gehören:
- regelmäßige Schulungen der Mitarbeiter zum Datenschutz,
- Dateien- und Geräteverzeichnisse gemäß § 10 SächsDSG,
- Festlegen von Zutrittsberechtigungen,
- Schlüsselregelungen für Mitarbeiter,
- ausschließliche Verwendung inventarisierter Datenträger (z. B. Diskette),
- regelmäßige Datenträgerkontrolle,
- Archivierung der Datenträger in diebstahlsicheren und brandgeschützten Räumen/Schränken,
- revisionsfähiger Datenträgeraustausch,
- Verschließen von PC-Räumen bei Abwesenheit,
- zuverlässige Vernichtung nicht mehr benötigter Datenträger (wenn Archivverwaltung die Übernahme abgelehnt hat),
- Aufbewahrungsfristen für Dateien,
- Vorschreiben geeigneter Sicherheitssoftware,
- Nutzen von Anti-Virus-Programmen,
- Einsatz interner Datenschutzbeauftragter (siehe 1. Tätigkeitsbericht 16.1.2).

Da in vielen Fällen organisatorische Maßnahmen allein nicht ausreichen, ist es notwendig, zusätzliche *technische* Mittel einzusetzen. Welcher Aufwand gerechtfertigt ist, hängt von der "Sensibilität" der zu schützenden Daten und dem Grad der Gefahr für das Persönlichkeitsrecht ab.

Zu den technischen Maßnahmen gehören:
- Automatisches Zugangskontrollsystem,
- Paßwortverwaltung,
- Protokollierung aller oder besonders ausgewählter Benutzeraktivitäten,
- Erstellen von Sicherheitskopien,
- Abschließen des PC bei Abwesenheit,
- Sperren der Tastatur bei Abwesenheit,
- Einsatz von Verschlüsselungsmechanismen für sensible Dateien.

Der Paßwortschutz ist häufig nur unzureichend verwirklicht (das Paßwort ist zu kurz und wird nicht gewechselt, die Zahl der Anmeldefehlversuche ist nicht begrenzt). Mehr Sicherheit für besonders schutzwürdige Daten bietet zusätzlich zum Paßwort die Chip-Karte zur Überprüfung der persönlichen Identität oder der maschinenlesbare Ausweis, der durch die persönliche Kennzahl (PIN - personal identification number) geschützt ist (zur Paßwortgestaltung siehe 1. Tätigkeitsbericht 16.3.4).
Die Protokollierung erfordert in der Regel zusätzliche Sicherheitssoftware. Sie ermöglicht bei Bedarf die Überprüfung aller durchgeführten Benutzeraktivitäten.

Die PC-Sicherheit wird nicht allein durch den Einsatz von Sicherheitssoftware oder -hardware und die regelmäßige Sicherung der Datenbestände gewährleistet, sondern vor allem durch die persönliche Verantwortung und Motivation der Mitarbeiter für ihre Arbeit am PC.

14.2 Datenschutz bei Telefax-Übertragungen

Die Datenschutz-Risiken beim Telefax-Betrieb und die daraus abgeleiteten und zu beachtenden Hinweise sind in der Bekanntmachung des Sächsischen Datenschutzbeauftragten vom 14. Juni 1993 aufgeführt (SächsABl. S. 894; vgl. 16.1.1).

Ergänzend ist dazu zu sagen, daß Daten, die durch Abfangen von Telefax-Übertragungen gewonnen werden, für den Täter oft viel wertvoller sind als der Inhalt von Telefongesprächen. Daher ist das Risiko eines gezielten Abhörens größer als beim Telefonieren. Deshalb sollte bei Bedarf eine Datenverschlüsselung eingesetzt werden. Allerdings setzt dies voraus, daß auch der Telefaxempfänger ein Gerät besitzt, das dechiffrieren kann. Im Handel sind verschiedene Produkte zur Verschlüsselung als Ergänzung zu Telefax-Geräten der Gruppe 3 (CCITT-Standard) erhältlich.
Die Verschlüsselungstechnik, die die automatische Übertragung der Schlüssel zwischen Sender und Empfänger und die Authentisierung übernimmt, muß durch eine zugehörige Chipkarte aktiviert werden. Durch den Schlüsselaustausch zwischen Sende- und Empfangsgerät können außerdem Fehlverbindungen ausgeschlossen werden.
Daneben bietet die Einrichtung einer geschlossenen Benutzergruppe, die nur Kommunikationen mit Benutzern der gleichen Gruppe zuläßt, weitere Sicherheit. Allerdings können dann auch keine Nachrichten von Dritten empfangen oder an Dritte gesendet werden.

14.3 Digitale Telekommunikationsanlagen - ISDN

14.3.1 Anmeldung von TK-Anlagen

Nach § 31 Abs. 7 SächsDSG darf eine automatisierte Verarbeitung von Personaldaten nur im Benehmen mit dem Sächsischen Datenschutzbeauftragten eingeführt, angewendet, geändert oder erweitert werden. Um einen datenschutzgerechten Umgang mit den Telefondaten der Beschäftigten zu gewährleisten, sollten in einer Dienstvereinbarung für den Einsatz der ISDN-Telefon-Nebenstellenanlage die in meinem Merkblatt zum Betrieb digitaler Telekommunikationsanlagen vom 8. Januar 1993 (SächsABl. S. 102; abgedruckt im 1. Tätigkeitsbericht unter 16.1.4) enthaltenen datenschutzrechtlichen Hinweise

verbindlich festgeschrieben werden.

Außerdem sollte die Dienstvereinbarung folgendes regeln:
- Gegenstand und Geltungsbereich der Dienstvereinbarung,
- Zweck der automatisierten Personaldatenverarbeitung, Zweckbindung der Daten,
- Datenspeicherung (Art und Umfang, Auswertungsrahmen, Löschungsfristen),
- Rechte der Beschäftigten (insbesondere Auskunftsrecht nach § 31 Abs. 3 SächsDSG i. V. m. § 17 SächsDSG),
- Zugriffsberechtigungen für die Verfahrensbeteiligten im Rahmen ihrer sachlichen und personellen Zuständigkeit,
- Beteiligung der Personalvertretung bei der Weiterentwicklung oder Änderung des Verfahrens,
- Einsichtsrecht der Personalvertretung in Programmunterlagen und Benutzer-Handbücher,
- Festlegung eines Sicherheitsstandards gemäß § 9 SächsDSG, der als technisch-organisatorisches Sicherheitskonzept Bestandteil der Dienstvereinbarung sein sollte.

Die Telefonate des Personalrates in Personalratsangelegenheiten werden als Dienstgespräche geführt. Im Gegensatz zu der sonst üblichen Praxis sollte bei ihnen auf eine Speicherung der Zielnummer verzichtet werden, um jeden Eindruck einer (unzulässigen) Einwirkung der Behördenleitung auf die Arbeit des Personalrates zu vermeiden. Dies muß allerdings ausdrücklich in der Dienstvereinbarung geregelt werden.
In der Praxis läßt sich das am besten durch einen ausschließlich für Personalratsgespräche vorzusehenden Nebenstellenanschluß erreichen.

14.3.2 Mitwirkung der Personalvertretung nach § 80 Abs. 3 Nr. 16 SächsPersVG

Die Gesprächsdaten, die in einer TK-Anlage gespeichert werden, sind zur Verhaltens- und Leistungskontrolle der Bediensteten durch den Dienstherren geeignet. So können z. B. die Gespräche nach Dauer, Entfernung, Kosten und Teilnehmer aufgelistet oder Häufigkeitsstatistiken über die Anzahl der Gespräche je Anschluß geführt werden.
Deshalb kann die Personalvertretung bei der Einführung und Anwendung von TK-Anlagen mit Gesprächsdatenerfassung nach § 80 Abs. 3 Nr. 16 SächsPersVG mitbestimmen. Daher sollte vor der Beschaffung einer TK-Anlage der Personalrat über die Einzelheiten der geplanten Verarbeitung und Nutzung informiert werden, damit er seine Rechte wahrnehmen kann.
Die Dienstvereinbarungen zwischen Behördenleitung und Personalrat werden datenschutzrechtlich von mir *geprüft*; ich bin gern bereit, schon *vor* dem Abschluß der Vereinbarung meinen *Rat* zu geben.

14.3.3 Gefahren für das Persönlichkeitsrecht durch kritische ISDN-Leistungsmerkmale

Im 1. Tätigkeitsbericht habe ich unter 14.2 bereits auf die mit dem Einsatz digitaler Telekommunikationssysteme (ISDN) verbundenen Gefahren für das Persönlichkeitsrecht des Einzelnen aufmerksam gemacht. Besonders problematisch sind die in den

vorhandenen Systemen teilweise vorgesehenen Leistungsmerkmale "Aufschalten", "Lauthören/Freisprechen", "Konferenz", "Zeugenzuschaltung", "Aufzeichnung des Gesprächsinhaltes" und "Automatischer Rückruf".

- *Aufschalten*
  Mit dem Merkmal können sich die Fernsprechvermittlung der Telekom, die Telefonzentrale der Anlage oder ein "besonders berechtigter" Teilnehmer in bestehende Verbindungen einschalten. Der Aufschaltende kann direkt mit den Teilnehmern der bestehenden Verbindung sprechen. Das Aufschalten wird durch einen Signalton, in manchen Geräten allerdings lediglich durch Anzeige im Display mitgeteilt.

- *Lauthören und Freisprechen*
  Beim "Lauthören" kann der im Telefonapparat eingebaute Lautsprecher vor oder während eines Gespräches eingeschaltet werden. Das Gespräch wird über den Handapparat weitergeführt.
  "Freisprechen" ermöglicht es, ein Telefongespräch nicht über den Hörer, sondern über ein im Endgerät eingebautes Mikrofon zu führen. Dabei wird der Lautsprecher ebenfalls eingeschaltet.

- *Konferenz*
  Bei diesem Merkmal können zu einer bestehenden Verbindung weitere Teilnehmer (auch Amtsteilnehmer) hinzugeschalten werden, ohne daß dies erkennbar ist.

- *Zeugenzuschaltung*
  Die Zuschaltung von Zeugen ist eine besondere Form der Konferenz. Sie erlaubt die netzweite Zuschaltung eines "Zeugen" bei Intern- und Externgesprächen. Die Zuschaltung wird den anderen Gesprächspartnern weder optisch noch akustisch angezeigt. Der Zeuge kann mithören, jedoch nicht mitsprechen.

- *Aufzeichnen des Gesprächsinhaltes*
  Durch Einsatz eines automatischen Aufzeichnungsgerätes können Gesprächsinhalte aufgenommen werden.

Bietet eine Anlage eine dieser Möglichkeiten, besteht die Gefahr der unbemerkten Beteiligung Dritter an den geführten Telefongesprächen. Immer wieder eingehende Anfragen zur Zulässigkeit dieser Leistungsmerkmale veranlassen mich, folgende *Hinweise* zu geben:

Nach der Rechtsprechung des Bundesverfassungsgerichts umfaßt das Recht des Einzelnen am eigenen Wort als Bestandteil des allgemeinen Persönlichkeitsrechts grundsätzlich die Befugnis, selbst zu bestimmen, wem seine Worte zugänglich sein sollen (vgl. BVerfG NJW 1980, 2070). Dieser grundrechtliche Schutz des gesprochenen Wortes entfällt nicht schon durch die *Kenntnis* des Sprechenden vom Bestehen einer Mithörmöglichkeit (vgl. BVerfG NJW 1992, 815). Die Beteiligung Dritter an Telefongesprächen darf daher grundsätzlich nur nach eindeutiger und rechtzeitiger Ankündigung und fehlendem Widerspruch des Gesprächspartners gegeben oder aufrecht erhalten werden (vgl. 1. Tätigkeitsbericht Abschnitt 5.1.3). Demgegenüber erkennt der Bundesgerichts-

hof in seinem Urteil vom 8.10.1993 - 2 StR 400/93 - nur noch dann einen Verstoß gegen das Recht am eigenen Wort bei Telefongesprächen mit zugeschalteter Mithörgelegenheit an, wenn

1. der Gesprächspartner erklärt, daß er Wert auf Vertraulichkeit legt oder
2. der Inhalt vertraulichen Charakter hat oder
3. dem Gesprächsteilnehmer der Eindruck vermittelt wird, daß eine Mithörgelegenheit nicht besteht (Täuschung).

Diese einschränkende Auslegung wird im wesentlichen damit begründet, daß "angesichts der Entwicklung im Fernsprechbereich jeder, der sich eines Fernsprechers bedient, damit rechnen [muß], daß ... Telefonanschlüssen Mithörgeräte angeschlossen sind und benutzt werden."

Meines Erachtens steht diese Rechtsprechung nicht im Einklang mit den genannten Entscheidungen des Bundesverfassungsgerichts (und auch nicht mit § 11 Abs. 3 SächsDSG, wonach Daten *ohne Kenntnis des Betroffenen* nur dann erhoben werden dürfen, wenn ein Gesetz oder eine Rechtsverordnung dies vorsieht oder zwingend voraussetzt). Daher bleibt es nach meiner Auffassung bei der Verpflichtung der öffentlichen Stellen, das Bestehen oder Aktivieren der eingangs erläuterten Leistungsmerkmale grundsätzlich dem Gesprächsteilnehmer gegenüber rechtzeitig anzukündigen (gegebenenfalls auch durch geeignete technische Möglichkeiten, z. B. Signalton), damit dieser die Möglichkeit zum Widerspruch hat.

Einer Unterrichtung des Gesprächspartners bedarf es selbstverständlich dann nicht, wenn eine Mithörgelegenheit in einer *Notwehrlage* aktiviert werden soll. Eine Notwehrlage liegt beispielsweise bei telefonisch geäußerten *Bombendrohungen* oder *erpresserischen Anrufen* vor.

Da das *Mitschneiden* eines Anrufs einen besonders tiefen Eingriff in das Recht am gesprochenen Wort bedeuten kann (es besteht die Gefahr der späteren "Verbreitung"), hat der Gesetzgeber das unbefugte Mitschneiden des nichtöffentlich gesprochenen Wortes auf einen Tonträger sogar in § 201 Abs. 1 Nr. 1 StGB unter Strafe gestellt. Sofern keine Rechtsvorschrift die Aufzeichnung ausdrücklich gestattet, ist eine *Befugnis* zum Mitschneiden eines Telefongesprächs *nur* mit ausdrücklicher Einwilligung des Gesprächpartners oder in einer Notwehrlage (s. o.) in Verfolgung überwiegender berechtigter Interessen gegeben.

Eine andere Gefährdung besteht bei dem Merkmal *Automatischer Rückruf*:

Ist "besetzt" oder ist der Angerufene abwesend (ertönt also das Freizeichen - der sog. "Freifall"), kann die Rückruffunktion durch den Anrufer aktiviert werden. Der Rückrufwunsch wird von der Anlage in einer systeminternen Tabelle verwaltet. Ist das Gespräch, das der Angerufene geführt hat, beendet oder hat er nach seiner Abwesenheit das Gerät wieder benutzt, stellt die ISDN-Anlage durch automatische Wahl eine Verbindung zwischen Angerufenem und Anrufer her.

Der automatische Rückruf kann zur Kontrolle des Arbeitsverhaltens und der Anwesenheit von Beschäftigten eingesetzt werden. Durch das automatische Herstellen der Ver-

bindung ist nämlich eine relativ genaue Aussage über die An- oder Abwesenheit des Telefonpartners möglich. Dies kann unterbunden werden, indem der Rückruf nicht mehr automatisch erfolgt, sondern ein Rückrufwunsch hinterlegt wird (z. B. durch Anzeige im Display des angerufenen Gerätes), den der gerufene Teilnehmer beliebig abrufen und aktivieren kann. Beide Teilnehmer sollten zudem die Möglichkeit haben, einen Rückrufauftrag wieder zu löschen.

14.3.4 Gesprächsdatenübertragung mittels Modemwählverbindung

Gesprächsdaten werden in modernen TK-Anlagen, die zu einem Netzverbund gehören, innerhalb der Anlage erfaßt. Die gespeicherten Daten werden zum Zwecke der Gebührenabrechnung gesammelt in regelmäßigen Zeitabständen an den Zentralrechner des Netzverbundes übertragen. Dies geschieht üblicherweise durch Wählleitungen der Telekom. Dabei werden mit Hilfe eines Modems digitale Informationen in Tonsignale beziehungsweise Tonsignale in digitale Informationen umgewandelt. Da es sich bei dem Telekom-Netz um ein offenes Wählnetz handelt, können Unbefugte ("Hacker") den Anschluß der TK-Anlage anwählen, um die gespeicherten Daten abzurufen, zu manipulieren oder die Software zu beschädigen (z. B. durch "Viren").
Jede Behörde, die eine Modemwählverbindung nutzen will, muß sich deshalb von der Lieferfirma darlegen lassen, welche Sicherungsvorkehrungen vorgesehen sind, um solche Zugriffe zu verhindern:

- Möglich ist z. B. die Einrichtung eines automatischen Rückrufes. Wenn die TK-Anlage vom Zentralrechner angerufen wird, übermittelt sie nicht sofort die Daten, sondern beendet zunächst die Verbindung. Danach wählt sie selbst die Anschlußnummer des Zentralrechners und stellt erst dann die Verbindung mit diesem her. So kann der Zentralrechner eindeutig als Anrufer identifiziert werden.

- Wenn das Modem nur zu festgelegten Übertragungszeitpunkten (z. B. manuell durch die Betreiber der TK-Anlage) eingeschaltet wird, wird der Zeitraum, in dem ein Mißbrauch stattfinden kann, eingeschränkt.

- In der TK-Anlage sollte protokolliert werden, wann und durch wen die Gesprächsdaten abgefragt wurden.

- Nach Dienstschluß sind die Wählleitungen zu sperren, damit Unbefugte keine Verbindungsversuche starten können.

14.4 Nicht mehr genutzte PC's

Bei der Kontrolle einer Dienststelle, die ein neues DV-System eingeführt hatte, habe ich die Zugriffsmöglichkeiten überprüft. Die verwendeten PC's waren nur mit Passwort zu benutzen und genügten hohen Sicherheitsanforderungen. Der Raum, in dem sie standen, war allen Mitarbeitern der DV-Abteilung zugänglich und wurde im Vertrauen auf die Sicherheitsmaßnahmen von den zuständigen Mitarbeitern auch für längere Zeit verlassen. Im gleichen Raum befanden sich zwei nicht mehr genutzte PC's. Sie waren an das Netz angeschlossen und betriebsbereit. Was auf ihnen gespeichert war, war den Mitarbeitern

nicht mehr bekannt. Nachforschungen ergaben, daß unter dem Betriebssystem MS-DOS mehrere Dateien für Statistikzwecke gespeichert waren. Ein unbefugtes Kopieren der Dateien wäre über das vorhandene Diskettenlaufwerk möglich gewesen.

Dies ist zur Zeit kein Einzelfall, da viele öffentliche Stellen ihre DV-Technik, die oft unkoordiniert und zufällig angeschafft wurde, jetzt erneuern und damit Altgeräte ausmustern oder zwischenlagern. Dabei ist immer wieder ein fahrlässiger Umgang mit Altdaten zu beobachten. Deshalb sollte die verantwortliche Dienststelle folgende Regeln beachten, falls veraltete DV-Technik durch neue ersetzt wird:

- Es ist zu ermitteln, welche Daten auf dem Gerät gespeichert sind.
- Es muß entschieden werden, wie mit den Daten verfahren wird (z. B. bei Ausmusterung der Geräte gegebenenfalls Anbietung der Daten an das Archiv, § 5 SächsArchG i. V. m. § 2 Abs. 2 SächsArchG). Dabei hat die Dienststelle zu berücksichtigen, ob die Geräte und gegebenenfalls auch die Daten weiterverwendet werden sollen. Allerdings müssen personenbezogene Daten generell physikalisch auf den Geräten gelöscht werden. Bei Abgabe der Geräte an Dritte sollten alle Daten gelöscht werden.
- Die Geräte sind so zu lagern, daß eine schnelle Inbetriebnahme nicht möglich ist (z. B. ohne Netzkabel).
- Die Geräte sind in Räumen zu lagern, die nur bestimmten Personengruppen zugänglich sind.
- Erfolgt nach einem längeren Zeitraum der Lagerung eine Abgabe an Dritte, so sind gegebenenfalls die ersten zwei Schritte noch einmal zu wiederholen.

14.5 Softwareinstallierung durch Private in einem Einwohnermeldeamt

Ein Landratsamt teilte mir mit, daß einige Kommunen die Installation der Einwohnermeldesoftware durch eine Privatperson durchführen lassen wollen, die, wie es hieß, früher in einer Computerfirma gearbeitet habe. Das Amt fragte an, ob dies nach § 3 SächsMG zulässig sei.

§ 3 SächsMG schränkt für *Meldedaten* die grundsätzlich für Behörden bestehende Möglichkeit, Dritte mit der Datenverarbeitung zu beauftragen (sog. *Datenverarbeitung im Auftrag*, § 7 SächsDSG), auf solche Auftragnehmer ein, die juristische Personen des öffentlichen Rechtes sind, welche der Aufsicht des Freistaates Sachsen unterstehen (vgl. auch § 38 Abs. 2 SächsMG). Dies betrifft jedoch nur, wie es in der Vorschrift heißt, die Übertragung "*der automatisierten Führung des Melderegisters*".
Die bloße Installation der Software auf der von der Behörde selbst betriebenen Anlage wird davon *nicht* erfaßt. Sie fällt vielmehr in den Bereich der *Wartung*, denn sie dient dazu, die Anlage funktionsfähig zu machen beziehungsweise zu erhalten.
Wartung und Fernwartung befinden sich zur Zeit in einer datenschutzrechtlichen "Grauzone". Im Gespräch ist die rechtliche Einordnung als Datenübermittlung oder als allgemeine Auftragsdatenverarbeitung im Sinne der Landesdatenschutzgesetze, wobei die Tendenz stärker in die letzte Richtung geht. Die Installation der Software ist allerdings insofern ein Grenzfall der Wartung, als bei ihrer Durchführung unter Umständen noch gar keine personenbezogenen Daten (in der betreffenden Anlage) vorhanden sind, die durch sie (im weiten datenschutzrechtlichen Sinne dieses Wortes) *verarbeitet* werden könnten.

Mittlerweile gibt es dazu einen besonderen Gesprächskreis der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, der diese Streitfragen hoffentlich bald klärt.

Rechtlich belanglos ist die in der Anfrage des Landratsamtes anklingende Unterscheidung zwischen einer Computerfirma und einer "Privatperson", die früher in einer Computerfirma gearbeitet hat, denn auch bei der Computerfirma handelt es sich um ein privates Unternehmen. Maßgebend ist hier genauso wie bei der Auftragsdatenverarbeitung ausschließlich, ob der Auftragnehmer sorgfältig ausgewählt ist; vgl. hierzu Nr. 5 meiner diesbezüglichen Bekanntmachung vom 3. November 1993, hier abgedruckt unter 16.1.4.

Allgemein *empfehle ich* folgendes:
- Es ist dafür zu sorgen, daß dem "Installateur" keine Echtdaten bekannt werden.
- Der Auftraggeber hat die erforderlichen Maßnahmen zu treffen, um die personenbezogenen Daten vor unbefugtem Zugriff - z. B. einer Programmänderung, die eine spätere Manipulation ermöglicht - zu schützen (vgl. § 9 SächsDSG).
- Besteht ein Wartungs-Vertrag - der wie oben ausgeführt, als Vertragsverhältnis über Datenverarbeitung im Auftrag anzusehen sein und unter § 7 SächsDSG fallen dürfte -, so sollte die Installation der Software *diesem* Vertragspartner in Auftrag gegeben, also der Installations-Auftrag nicht einem Dritten erteilt werden.
- Wird, weil kein Wartungsvertrag besteht, ein bloßer Installations-Auftrag erteilt, so sollte der Auftragnehmer (der zivilrechtlich natürlich ein "Werkunternehmer" ist) gesondert auf Geheimhaltung verpflichtet werden, z. B. nach § 1 Verpflichtungsgesetz. Auch wäre eine Anstellung auf Zeit für die Dauer seiner Tätigkeit (damit würde er zum Amtsträger) möglich.

Sofern bei einer ordnungsgemäßen Installation (wie allgemein bei der Wartung) von Software personenbezogene Daten genutzt werden - dies hängt vom Einzelsachverhalt (z. B. Test mit Echtdaten) ab -, handelt es sich um einen Vorgang, der, wie gesagt, Ähnlichkeiten mit der Datenverarbeitung im Auftrag gemäß § 7 SächsDSG hat. Deshalb ist es angebracht, in diesem Fall die Vorschriften des § 7 SächsDSG zu beachten. Einzelheiten dazu ergeben sich aus meiner genannten Bekanntmachung.

14.6 Schreiben einer "Schutz-Gemeinschaft für Software" an Hochschulen

Ende 1993 wandte sich der Datenschutzbeauftragte einer sächsischen Universität mit folgendem Problem an mich:

Die Universität hatte von einer "Schutz-Gemeinschaft Software ..." ein Schreiben erhalten, mit dem auf wenig einleuchtende Weise urheberrechtliche Ansprüche geltend gemacht wurden; sie sollten sich auf nicht näher bezeichnete Software beziehen, von der angeblich die Gesamtheit der Studenten und der Mitarbeiter der Universität in nicht näher benannter Anzahl Kopien ohne eigenen Lizenzerwerb ("Raubkopien") verwendeten. Zur Abgeltung dieser behaupteten Ansprüche sollte die Hochschule sich in einem Vertrag mit der "Schutz-Gemeinschaft" dieser gegenüber zu einer Zahlung verpflichten. Eine - sehr genau bezifferte - Rechnung lag bei. Art und Weise des Schreibens ließen vermuten, daß mit ähnlichen Schreiben an einen größeren Adressatenkreis zu rechnen war. Deshalb habe ich Nachforschungen angestellt, obwohl sich das Problem mehr am

Rande meines Aufgabenbereiches bewegte. Ein Gespräch mit dem VSI (Verband der Softwareindustrie Deutschlands) ergab, daß dort seit Mitte Dezember bereits eine Reihe von Anfragen zu dieser "Schutz-Gemeinschaft für Software" eingegangen waren. Der VSI empfahl, auf die erhobenen Forderungen nicht einzugehen; ich solle Anfragende in diesem Sinne bestärken. Gegen die "Schutz-Gemeinschaft" laufe ein Ermittlungsverfahren wegen Betrugsverdachtes. Ein Gerichtsurteil, auf das die Schutzgemeinschaft sich in ihrem Anschreiben beruft, werde falsch zitiert und habe mit dem Sachverhalt nichts zu tun. Ich habe den Datenschutzbeauftragten der Universität von dieser Einschätzung des VSI unterrichtet und dem zuständigen SMWK den Sachverhalt mitgeteilt.
Kurz darauf erhielt ich von einer anderen Hochschule die gleiche Anfrage.

14.7 Verstoß gegen die Datensicherheit bei der Personalaktenführung

Im Januar 1994 war Pressemitteilungen zu entnehmen, daß angeblich einige Personalakten des SMI verschwunden seien.
Da ich gemäß § 24 Abs. 1 SächsDSG die Einhaltung des Sächsischen Datenschutzgesetzes und anderer Vorschriften über den Datenschutz zu kontrollieren habe, wurde sofort die Personalaktenführung des SMI durch Mitarbeiter meiner Geschäftsstelle überprüft. Insbesondere wurden die Sicherheitsmaßnahmen (hier § 9 Abs. 4 SächsDSG, § 117 Abs. 1 Satz 1 und Abs. 3 SächsBG) kontrolliert.
Folgende Mängel wurden dabei festgestellt:

1. Eine hausinterne Anordnung/Dienstanweisung über die datenschutzgerechte Personalaktenverwaltung war nicht vorhanden.
2. Die für den 2. Untersuchungsausschuß (oben Abschnitt 2.2) bereitgestellten Personalakten lagerten unverschlossen in Waschkörben.
3. Die Personalakten waren in offenen Regalen gelagert.
4. Sowohl die Personalkartei als auch die Kartei über die Fälle, in denen ein Rechtsstreit anhängig ist, standen in unverschließbaren Karteikästen auf einem Schreibtisch.
5. Der Zugang zu den Diensträumen war unzureichend gegen Zutritt Unbefugter (Besucher, unzuständige Mitarbeiter, Hilfskräfte) gesichert.
6. Eine Putzkolonne eines Privatbetriebes hatte nach Dienstschluß ungenügend kontrollierten Zugang zu den Diensträumen.

Die festgestellten Mängel waren insgesamt geeignet, den unbefugten Zugriff auf und den Verlust von Personalakten/Personalaktenteilen zu begünstigen.
Erst der Kontrollbesuch war Anlaß für das SMI, Sofortmaßnahmen zu treffen und Verbesserungen technisch-organisatorischer Sicherungsmaßnahmen, insbesondere in Bezug auf die Zugangssicherung, in die Wege zu leiten.
Die Verantwortlichen haben sofort reagiert: Sie haben insbesondere eine Anordnung zur Aufbewahrung und Versendung von Personalakten getroffen, die Lagerung der Personalakten in verschließbaren Schränken organisiert, den Zugangsschutz verbessert und dafür gesorgt, daß die Reinigung der Diensträume während der Dienstzeit unter Aufsicht der Bediensteten erfolgt.
Wegen der unverzüglichen Bereitschaft zur Beseitigung der festgestellten Mängel und zu einem kooperativen Verhalten der an der Prüfung beteiligten Bediensteten des SMI habe ich von einer Beanstandung abgesehen.

15 Vortrags- und Schulungstätigkeit

Das Bedürfnis nach Vorträgen zum Datenschutz und zur Datensicherheit hat unvermindert angehalten. Soweit die Arbeitsbelastung dies zuließ, haben meine Mitarbeiter und ich ihm entsprochen. Meine Dienststelle hat deshalb auch in diesem Jahr wieder zahlreiche allgemeine und fachspezifische Vorträge und Schulungsveranstaltungen im Freistaat Sachsen (z. B. in Leipzig, Dresden, Plauen, Schloß Lichtenwalde, Delitzsch, Eilenburg, Kändler, Görlitz) durchgeführt.

16 Materialien

16.1 Bekanntmachungen

16.1.1 (SächsABl. S. 894)

Bekanntmachung des Sächsischen Datenschutzbeauftragten zum Datenschutz bei Telefax-Übertragungen
Vom 14. Juni 1993

Telefax ermöglicht die schnelle elektronische Übertragung von Text- und Bildvorlagen. So hat sich Telefax nach dem Telefon zum zweitwichtigsten Kommunikationsmittel entwickelt. Der zunehmende Einsatz von Telefax-Geräten macht es erforderlich, hierbei auftretende Gefahren für das informationelle Selbstbestimmungsrecht näher zu untersuchen:

- Telefax-Geräte sind häufig an zentralen und damit leicht zugänglichen Orten aufgestellt. Dadurch sind unbefugtes Mitlesen, mißbräuchliche Nutzung oder Manipulation vorprogrammiert.
- Verwählen ist die Ursache, daß der gewünschte Empfänger das Telefax nicht erhält.
- Häufig weiß der Absender nicht, wer vom übertragenen Telefax-Schreiben Kenntnis erlangen kann. Dennoch bleibt er für den Schutz der übermittelten Daten verantwortlich.

Telefax-Geräte sind Rechner, die personenbezogene Daten automatisiert verarbeiten. Sie speichern nicht nur Verbindungsdaten (Sende- und Empfangskennung, Orts- und Zeitangabe, Anzahl der Seiten, Sendedauer), sondern bei einigen Geräten sogar Kommunikationsinhalte. Wegen ihrer hohen Sicherheitsrisiken sind Telefax-Übertragungen mit dem (strafbewehrten) Schutz des Arztgeheimnisses, des Steuergeheimnisses, des Sozialgeheimnisses und des Amtsgeheimnisses nicht zu vereinbaren. Damit den besonderen Gefahren durch unbefugtes Mitlesen, unbefugte Einsichtnahme, Manipulationen und Maskeraden begegnet werden kann und eine mißbräuchliche Nutzung verhindert wird, sind von den öffentlichen Stellen des Freistaates Sachsen folgende Hinweise zu beachten:

1. Telefax ist "abhörbar". Was am Telefon gesagt werden darf, darf noch lange nicht mit Telefax übermittelt werden.
2. Daten, die einem besonderen Berufs- oder Amtsgeheimnis unterliegen (Sozial-, Steuer- und Personaldaten), dürfen grundsätzlich nicht mit Telefax übermittelt werden.
3. Telefax-Geräte sind so aufzustellen, daß Unbefugte keinen Zugang haben.
4. Vor der Absendung einer Telefax-Mitteilung ist der Adressat über den konkreten Zeitpunkt der Übertragung zu verständigen, damit zugesichert werden kann, daß beim Empfänger keine unbefugten Personen Einblick nehmen können.
5. Die vom empfangenden Gerät abgegebene Kennung ist sofort zu überprüfen, damit die Verbindung bei Wählfehlern sofort abgebrochen werden kann.
6. Es ist zu kontrollieren , ob die Übertragung störungsfrei und vollständig den Empfänger erreicht hat.
7. Die Dokumentationspflicht ist zu beachten:

- Verwendung des Behördendeckblatts mit Angaben zu Adressat, Absender, Zahl der zu übertragenden Seiten und weiteren Nachrichten.
- Aufbewahrung der Protokolle

8. Eine schriftliche Dienstanweisung sollte die Bedienung und Nutzung von Telefax-Geräten regeln.
9. Vor dem Verkauf gebrauchter Telefax-Geräte müssen gespeicherte Daten unbedingt gelöscht werden.
10. Die allgemeinen materiellen Regeln zur Zweckbindung und Übermittlung personenbezogener Daten gelten uneingeschränkt auch im Telefax-Verkehr.

Dresden, den 14. Juni 1993

Der Sächsische Datenschutzbeauftragte
Thomas Giesen

16.1.2 **(SächsABl. S. 970)**

Bekanntmachung des Sächsischen Datenschutzbeauftragten zur Verpflichtung auf das Datengeheimnis Vom 22. Juli 1993

Nach § 6 Abs. 1 des Sächsisches Datenschutzgesetzes (SächsDSG) ist es allen bei der Datenverarbeitung der Behörden und sonstigen öffentlichen Stellen des Freistaates Sachsen beschäftigten Personen untersagt, personenbezogene Daten unbefugt zu verarbeiten oder sonst zu verwenden. Über diese Pflicht, das Datengeheimnis zu wahren, sind die Personen nach § 6 Abs. 2 SächsDSG zu unterrichten und hierauf sowie auf die Einhaltung sonstiger Vorschriften über den Datenschutz schriftlich zu verpflichten.

Von der Pflicht nach § 6 SächsDSG bleiben weitere Pflichten der Bediensteten unberührt. So sind die Bediensteten in der öffentlichen Verwaltung aufgrund der beamtenrechtlichen bzw. arbeitsvertraglichen Pflicht zur Amtsverschwiegenheit (Sächsisches Beamtengesetz bzw. BAT) und ggf. aufgrund der datenschutzrechtlichen Bestimmungen zum Schutz der Sozialdaten (z.B. § 35 SGB I), sonstiger bereichsspezifischer, auf den Amtsträger zielender Verschwiegenheitspflichten sowie des strafrechtlichen Geheimnisschutzes (§ 203 StGB) zur Verschwiegenheit verpflichtet.

Von § 6 SächsDSG werden sämtliche Personen erfaßt, deren Aufgabengebiet sie mit personenbezogenen Daten regelmäßig in Verbindung bringt. Hierbei kommt es entscheidend auf die Möglichkeit des Datenzugangs im Einzelfall an: Nicht nur die sachbearbeitende Person, sondern auch Schreibkräfte, Registratoren, Personalratsmitglieder sowie die Poststelle, der Botendienst und - wenn außerhalb der Dienstzeit tätig - auch das Reinigungspersonal unterliegen der Verpflichtung zur Wahrung des Datengeheimnisses. Damit wird deutlich, daß sämtliche Personen, deren Beschäftigungsverhältnis ihnen faktisch Zugang zu personenbezogenen Informationen ermöglicht, eine persönlich zu erfüllende Rechtspflicht trifft.

Mit der Verpflichtung auf das Datengeheimnis soll den Bediensteten nahegebracht wer-

den, daß sie **nur im Rahmen ihrer Befugnisse** Daten verarbeiten dürfen. Maßgebend sind hier zunächst die Regelungen im Sächsischen Datenschutzgesetz sowie in den für die Tätigkeit einschlägigen Spezialgesetzen. Dies sind z. B. Sozialgesetzbuch, Straßenverkehrsgesetz, Straßenverkehrszulassungsordnung, Meldegesetz, Ausländergesetz, Statistikgesetz, Gewerbeordnung, Grundbuchordnung. Darüberhinaus müssen die Bediensteten über die **sonstigen bei der Tätigkeit zu beachtenden Vorschriften über den Datenschutz** unterrichtet werden. Hierzu zählen alle für den konkreten Arbeitsplatz geschaffenen Regelungen: Dateienverzeichnisse mit Errichtungsanordnungen, Zuständigkeitsregelungen, Einzelanweisungen von Vorgesetzten, Anweisungen von auftraggebenden Stellen, Paßwortverwaltung.

Zur Unterrichtung der Beschäftigten im Sinne des § 6 Abs. 2 SächsDSG reicht ein bloßer Hinweis auf die zu beachtenden Vorschriften nicht aus. Vielmehr ist eine umfassende Einführung in die Probleme des Datenschutzes und seine Auswirkungen auf die Tätigkeit am konkreten Arbeitsplatz sowie eine Einweisung in die erforderlichen Schutz- und Sicherungsverfahren nötig.

Für die Verpflichtung auf das Datengeheimnis sollten die von § 2 SächsDSG erfaßten Behörden und sonstigen öffentlichen Stellen im Freistaat Sachsen das Muster in der **Anlage** verwenden.

Dresden, den 22. Juli 1993

Der Sächsische Datenschutzbeauftragte
In Vertretung
Dr. Wippermann

Dienststelle

Verpflichtung auf das Datengeheimnis

Vor der/dem Unterzeichner/in erschien heute zum Zwecke der Verpflichtung nach § 6 des Sächsisches Datenschutzgesetzes vom 11. Dezember 1991 (SächsGVBl S. 401)

Frau/Herr

Die/Der Erschienene, deren/dessen Aufgabengebiet sie/ihn mit personenbezogenen Daten regelmäßig in Verbindung bringt, wurde auf die Wahrung des Datengeheimnisses nach § 6 Sächsisches Datenschutzgesetz verpflichtet.

Sie/Er wurde darauf hingewiesen, daß sie/er - auch nach Beendigung der Tätigkeit - personenbezogene Daten nur im Rahmen der Befugnisse aufgrund des Sächsischen Datenschutzgesetzes und der für die Tätigkeit einschlägigen Spezialgesetze verarbeiten oder sonst verwenden darf. Darüberhinaus hat sie/er die sonstigen bei der Tätigkeit zu beachtenden Vorschriften über den Datenschutz zu befolgen. Dazu zählen auch arbeitsplatzspezifische Regelungen (z. B. der Inhalt der Dateienverzeichnisse mit Errichtungsanordnungen, Zuständigkeitsregelungen, Einzelanweisungen von Vorgesetzten, Anweisungen von auftraggebenden Stellen).

Sie/Er wurde weiter darüber belehrt, daß Verstöße gegen das Datengeheimnis nach §§ 32 und 33 Sächsisches Datenschutzgesetz und anderen einschlägigen Rechtsvorschriften mit Geldbußen bis 50.000 DM oder mit Geld- oder Freiheitsstrafen geahndet werden können; eine disziplinarrechtliche Verfolgung wird dadurch nicht ausgeschlossen. Eine Verletzung des Datengeheimnisses wird in den meisten Fällen auch eine Verletzung der Amtsverschwiegenheit bzw. einen Verstoß gegen die arbeitsvertragliche Schweigepflicht darstellen. Zugleich kann in ihr eine Verletzung spezieller Geheimhaltungspflichten (Arztgeheimnis, Sozialgeheimnis, Steuergeheimnis) liegen.

Sie/Er erklärt, nunmehr hinreichend über die Pflicht nach § 6 Sächsisches Datenschutzgesetz und die Folgen ihrer Verletzung unterrichtet zu sein.

Sie/Er bestätigt den Empfang einer Abschrift dieses Protokolls.

(Unterschrift der/des Verpflichteten)

(Unterschrift der/des Verpflichtenden)

, den

DS 6 VII/93

Auszug aus dem Sächsischen Datenschutzgesetz
(als Anlage zur Verpflichtung auf das Datengeheimnis)

§ 6

Datengeheimnis

(1) Den bei der Datenverarbeitung beschäftigten Personen ist es untersagt, personenbezogene Daten unbefugt zu verarbeiten oder sonst zu verwenden (Datengeheimnis). Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort.

(2) Die in Absatz 1 genannten Personen sind bei der Aufnahme ihrer Tätigkeit über ihre Pflichten nach Absatz 1 sowie die sonstigen bei ihrer Tätigkeit zu beachtenden Vorschriften über den Datenschutz zu unterrichten und auf deren Einhaltung schriftlich zu verpflichten.

§ 32

Ordnungswidrigkeiten

(1) Ordnungswidrig handelt, wer
1. unbefugt von diesem Gesetz geschützte personenbezogene Daten, die nicht offenkundig sind,
   a) speichert, verändert oder übermittelt,
   b) zum Abruf mittels automatisierten Verfahrens bereithält oder
   c) abruft oder sich oder einem anderen aus Dateien verschafft,
2. die Übermittlung von personenbezogenen Daten, die durch dieses Gesetz geschützt werden und nicht offenkundig sind, durch unrichtige Angaben erschleicht,
3. personenbezogene Daten ohne die nach § 13 Abs. 3 Satz 3 oder nach § 15 Abs. 4 Satz 3 erforderliche Einwilligung oder entgegen § 30 Abs. 1 für einen anderen Zweck nutzt,
4. entgegen § 30 Abs. 3 Satz 3 die in § 30 Abs. 3 Satz 2 bezeichneten Merkmale mit den Einzelangaben zusammenführt oder
5. entgegen § 15 Abs. 5 eine vollziehbare Auflage nicht, nicht rechtzeitig oder nicht vollständig erfüllt.

(2) Die Ordnungswidrigkeit kann mit einer Geldbuße bis zu 50 000 DM geahndet werden.

(3) Verwaltungsbehörden im Sinne von § 36 Abs. 1 Nr. 1 des Gesetzes über Ordnungs-widrigkeiten sind die Regierungspräsidien.

§ 33

Straftaten

Wer eine der in § 32 Abs. 1 Nr. 1 bis 4 bezeichneten Handlungen gegen Entgelt oder in der Absicht begeht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft. Der Versuch ist strafbar.

16.1.3 **(SächsABl. S. 1175)**

Bekanntmachung des Sächsischen Datenschutzbeauftragten zur Führung des Dateien- und Geräteverzeichnisses nach § 10 SächsDSG Vom 29. September 1993

Nach § 10 Abs. 1 Satz 1 des Sächsischen Datenschutzgesetzes (SächsDSG) führt **jede öffentliche Stelle ein Verzeichnis ihrer Dateien und der eingesetzten Datenverarbeitungsanlagen** (Gesamtheit der **Dateibeschreibungen**). Die Dateibeschreibungen sind für automatisierte **und** für nicht-automatisierte (manuelle) Dateien, z. B. Karteien, zu führen. § 3 Abs. 5 SächsDSG definiert eine **Datei** als

1. eine Sammlung personenbezogener Daten, die durch automatisierte Verfahren nach bestimmten Merkmalen ausgewertet werden kann (automatisierte Datei) oder
2. eine andere Sammlung personenbezogener Daten, die nach bestimmten Merkmalen geordnet oder ausgewertet werden kann (nicht-automatisierte Datei).

Die Verzeichnisse dienen der Eigenkontrolle der öffentlichen Stelle durch den Behördenleiter bzw. den behördlichen Datenschutzbeauftragten. Im übrigen sind sie Grundlage der Kontrolle durch den Sächsischen Datenschutzbeauftragten nach § 24 SächsDSG.

Zusätzlich dient das Dateienverzeichnis der Erteilung von **Auskünften**: Nach § 17 Abs. 1 SächsDSG ist dem Betroffenen von der speichernden Stelle auf Antrag kostenfrei Auskunft über die zu seiner Person gespeicherten Daten, den Zweck der Speicherung sowie die Herkunft und die Empfänger der Daten zu erteilen. Auch der Sächsische Datenschutzbeauftragte erteilt gemäß § 28 Abs. 2 SächsDSG auf Antrag im Einzelfall jedermann Auskunft über die Angaben nach § 10 Abs. 1 Nr. 1 bis 6 SächsDSG. Zu diesem Zweck kann er eine Kopie des Verzeichnisses von der öffentlichen Stelle einholen, § 28 Abs. 1 SächsDSG.

Öffentliche Stellen sind Behörden und sonstige öffentliche Stellen des Freistaates Sachsen, der Gemeinden und Landkreise sowie der sonstigen der Aufsicht des Freistaates Sachsen unterstehenden juristischen Personen des öffentlichen Rechts (§ 2 Abs. 1 SächsDSG). Natürliche und juristische Personen sowie Vereinigungen des privaten Rechts gelten als öffentliche Stellen, **soweit** sie Aufgaben der öffentlichen Verwaltung wahrnehmen und nicht als öffentliche Stellen des Bundes gelten (§ 2 Abs. 2 SächsDSG).

Das Verzeichnis wird durch die öffentliche Stelle geführt, die für die Verarbeitung der personenbezogenen Daten verantwortlich ist. Bei der Datenverarbeitung im Auftrag (§ 7 SächsDSG) ist dies der Auftraggeber, z. B. die Gemeinde als Auftraggeber eines Rechenzentrums. Gerichte führen die Verzeichnisse nur in Justizverwaltungsangelegenheiten (§ 10 Abs. 2 SächsDSG); ihre rechtsprechende Tätigkeit ist ausgenommen.

Zum **Standort der Verzeichnisse**: Die **Dateibeschreibungen** sollten bei den funktional zuständigen Stellen (Fachämter/Fachstellen innerhalb der Behörde) geführt werden, während sich das **Dateienverzeichnis** (Kopien der einzelnen Dateibeschreibungen) bei einer zentralen Stelle, zweckmäßigerweise beim behördlichen Datenschutzbeauftragten (falls ein solcher bestellt ist), befindet.

Es wird **empfohlen**, für die Dateibeschreibungen das in der **Anlage** zu dieser Bekanntmachung abgedruckte **Muster zu verwenden**. Beim Ausfüllen sollte beachtet werden:

1. Bezeichnung der Datei und ihre Zweckbestimmung

Als **Bezeichnung** der Datei ist ein möglichst "sprechender" Begriff (z. B. Schülerdatei; Datei der vom Wahlrecht oder von der Wählbarkeit Ausgeschlossenen) zu wählen, der bei automatisierten Dateien nicht mit dem systeminternen Dateinamen übereinstimmen muß.

Die **Zweckbestimmung** ergibt sich aus der jeweiligen Rechtsgrundlage, z. B. aus § 5 Abs. 2 Nr. 1 SächsMG (Datei der vom Wahlrecht oder von der Wählbarkeit Ausgeschlossenen).

2. Aufgaben und Rechtsgrundlage der Verarbeitung

Es sind die **Aufgaben** anzugeben, für die die Datei benötigt wird, z. B. Lohn- und Gehaltsabrechnung. Als Rechtsgrundlage ist die Textstelle (Paragraph, Absatz, Nummer) der einschlägigen Rechtsvorschrift (Gesetz, Rechtsverordnung, Satzung) sowie die Fundstelle (z. B. BGBl. I, SächsGVBl S. ...) aufzuführen. Ggf. ist zusätzlich die Textstelle der einschlägigen Verwaltungsvorschrift mit Fundstelle anzugeben.

3. Art der gespeicherten Daten

Es ist die Datenart unter Nennung der einzelnen Bestandteile des Datensatzes anzugeben, z. B. Einwohnermeldedaten - Name, Vorname, akademischer Grad, Familienstand etc. Eine möglichst präzise Beschreibung ist erforderlich.

4. Betroffener Personenkreis

Es sind die den betroffenen Personenkreis kennzeichnenden Merkmale aufzunehmen, z. B. "Wohngeldempfänger", "Fahrerlaubnisinhaber".

5. Regelmäßig zu übermittelnde und zu empfangende Daten

5.1 Art der regelmäßig zu übermittelnden Daten und deren Empfänger

Regelmäßige Datenübermittlungen liegen vor, wenn die Daten nach vorab bestimmten Regeln entweder in regelmäßigen Zeitabständen oder erst bei Vorliegen bestimmter sachlicher Voraussetzungen (anlaßbezogen) übermittelt werden, so daß über die Datenübermittlung im Einzelfall nicht nochmals zu entscheiden ist. Automatisierte Abrufverfahren werden als regelmäßige Datenübermittlungen behandelt.

Als **Empfänger** anzugeben sind diejenigen Dritten - nach 3 Abs. 4 SächsDSG jede Person oder Stelle außerhalb der datenverarbeitenden Stelle, ausgenommen Betroffene -, denen Daten übermittelt werden. Der Auftragnehmer bei der Datenverarbeitung im Auftrag nach § 7 SächsDSG ist nicht Dritter im Sinne des Gesetzes, da er nur als "verlängerter Arm" des Auftraggebers, also der speichernden Stelle, tätig ist. Ist der Empfänger eine einzelne Stelle oder Person, ist diese identifizierbar anzugeben; sind es mehrere, z. B. die Meldebehörden im Landkreis, genügt eine Gruppenbezeichnung. Verwenden Sie für jeden Datenempfänger eine Zeile und geben Sie links die Art der diesem zu übermittelnden Daten an.

Zusätzlich ist die **Rechtsgrundlage** der Datenübermittlung anzugeben, sofern sich diese nicht aus den zu Nr. 2 gemachten Angaben ergibt.

5.2 Art und Herkunft der regelmäßig zu empfangenden Daten

Herkunft bedeutet "Datenquelle". Es sind die Personen bzw. Stellen aufzuführen, bei denen die Daten erhoben bzw. von denen die Daten übermittelt werden. Werden die Daten von einer einzelnen Stelle oder Person übermittelt, ist diese identifizierbar anzugeben; erfolgt die Übermittlung durch mehrere, genügt eine Gruppenbezeichnung. Verwenden Sie für jede Datenquelle eine Zeile.

6. *Fristen für die Sperrung und Löschung sowie deren Prüfung*
   Nach § 20 Abs. 1 SächsDSG sind personenbezogene Daten in Dateien zu **sperren**, wenn ihre Richtigkeit vom Betroffenen bestritten wird und eine Feststellung über den Wahrheitsgehalt nicht möglich ist; ferner wenn eine an sich erforderliche Löschung zum Schutz berechtigter Interessen des Betroffenen unterbleibt (§ 19 Abs. 4 Nr. 1 SächsDSG) oder nur unter unverhältnismäßig hohem Aufwand möglich ist (§ 19 Abs. 4 Nr. 2 SächsDSG). Gesperrte personenbezogene Daten sind gesondert aufzubewahren. Bei automatisierten Verfahren kann die Sperrung anstelle einer gesonderten Aufbewahrung auch durch besondere technische Maßnahmen bewirkt werden. Ist dies nur mit unverhältnismäßig hohem Aufwand möglich, kann ein Sperrvermerk angebracht werden (§ 20 Abs. 3 SächsDSG). Sich auf Sperrungen beziehende Fristen sind zu vermerken.
   Nach § 19 Abs. 1 SächsDSG sind personenbezogene Daten in Dateien zu **löschen**, wenn ihre Speicherung unzulässig oder ihre Kenntnis zur Aufgabenerfüllung nicht mehr erforderlich ist. Die öffentlichen Stellen des Freistaates Sachsen haben jedoch vor einer Löschung dem zuständigen staatlichen Archiv, die Kommunen dem zuständigen kommunalen Archiv, alle zur Aufgabenerfüllung nicht mehr benötigten Unterlagen zur Übernahme anzubieten (§ 19 Abs. 3 SächsDSG, §§ 5 Abs. 1, 13 SächsArchG). Wird die Archivwürdigkeit bejaht, ist bei maschinell lesbaren Datenträgern die Form der Datenübermittlung mit dem Archiv zu vereinbaren, § 5 Abs. 8 SächsArchG. Wird die Archivwürdigkeit verneint, tritt die Löschungspflicht ein, vgl. §§ 5 Abs. 5 Satz 2, 13 Abs. 3 SächsArchG i. V. m. § 19 Abs. 1 Nr. 2 SächsDSG, sofern nicht § 19 Abs. 4 SächsDSG oder eine andere Rechtsvorschrift die Löschung verbietet. Eine Pflicht zur Löschung geht der Anbietungspflicht nur vor, wenn dies eine sonstige besondere Rechtsvorschrift bestimmt. So sind die kommunalen Archive nach § 27 SächsMG befugt, Meldedaten in das Gemeindearchiv zu übernehmen, soweit diese nicht nach § 26 SächsMG zu löschen sind.
   Die Voraussetzungen für die Sperrung und Löschung von personenbezogenen Daten ergeben sich in der Regel aus den Verwaltungsvorschriften des jeweiligen Aufgabenbereichs.
   Schließlich sind die Termine für die **Prüfung der Fristen** einzutragen.

7. *Zugriffsberechtigte Personen oder Personengruppen*
   Die zugriffsberechtigten Personen oder Personengruppen sind nach der **Art des Zugriffs** (schreibender bzw. lesender Zugriff) aufzuführen; ggf. sind Zugriffsbeschränkungen aufzunehmen. Die Berechtigung darf nur erteilt werden, wenn sie zur Aufgabenerfüllung erforderlich ist; sie sollte schriftlich festgelegt werden. Die Angaben müssen nicht namentlich erfolgen; es genügt in der Regel, wenn der Funktionsträger aufgeführt wird. Zu vermerken ist auch, ob die **Erteilung der Zugriffsberechtigung** dem Amtsleiter oder einer von diesem bestimmten Person oder Funktionsträger zusteht (Frage der Verantwortlichkeit).

8. *Personelle, technische und organisatorische Maßnahmen gemäß § 9 SächsDSG*
   Es ist die behördeninterne Dienstanweisung mit Datum und Kurzbezeichnung (z. B. "Dienstanweisung zum Datenschutz vom 14.1.1993") anzugeben. Die gemäß § 9 Abs. 2 Nr. 1 bis 10 SächsDSG getroffenen Kontrollmaßnahmen sind jeweils zu beschreiben.

9. *Weitere Angaben bei automatisierten Verfahren*
   Bei automatisierten Verfahren sind die **Betriebsart** (z. B. Dialogbetrieb oder Batchverarbeitung) und die **Art** der eingesetzten Geräte (z. B. Einzel-PC oder Abteilungsrechner, ggf. mit Angabe der Systemarchitektur/des Konfigurationsplanes) zu beschreiben. Als **Übermittlungsverfahren** ist anzugeben, mit welchen technischen

Mitteln und in welcher Form Daten üblicherweise übertragen werden, z. B. "Übertragung mittels Modem in verschlüsselter Form". Zum **Sperrungsverfahren** ist aufzuführen, durch welche Vorkehrungen die Daten gesperrt werden können, z. B. "Lese- und Schreibrechte werden verwehrt". Beim Verfahren zur **Löschung** ist konkret anzugeben, wie die Löschung bzw. Vernichtung der Daten, Protokolle und Datenträger durchgeführt wird, z. B. "Bei Disketten Benutzung des 'format a:/u'-Befehls" (erst ab MS-DOS 5.0 möglich) oder "Vollständiges Überschreiben der Dateien". Zur **Auskunftserteilung:** Gemeint ist die Auskunft an den Betroffenen nach § 17 SächsDSG. Hier ist anzugeben, in welcher Form diese Auskunft erteilt wird (z. B. Einsichtnahme am Bildschirm, Ausdruck der gespeicherten Daten, Übergabe eines Ausdrucks an den Betroffenen). Es ist auch anzugeben, ob der Betroffene auf seine Möglichkeit, den Sächsischen Datenschutzbeauftragten anzurufen, hingewiesen wird.

10. Eingesetzte Hardware und Betriebssystem-Software

Hier handelt es sich um gerätebezogene Angaben. Unter **Typ** ist die Gerätebezeichnung anzugeben, z. B. "PC 386/SX". **Hersteller** ist das Unternehmen, das das Endprodukt hergestellt hat oder unter seinem Namen vertreibt, z. B. "Technik AG". Unter **Art** und **Betriebssystem** ist anzugeben, ob es sich z. B. um einen Einzelplatzrechner/PC oder um einen vernetzten Arbeitsplatzrechner/PC handelt und welches **Betriebssystem** (Version) zur Anwendung kommt (z. B. MS-DOS 5.0). Bei der **Gerätenummer** handelt es sich um die vom Hersteller angebrachte Nummer des Rechners. Falls das eingesetzte Gerät **Funktionen für Datenfernverarbeitung und Datenübertragung** zur Verfügung stellt, sind Angaben zur Art der Übertragung (z. B. "X.25-Karte und Modem"), zum Typ (z. B. "Modem Typ 4, Technik GmbH"), zum Verfahren (z. B. X.25-Protokoll) und zum Träger der Übertragung (z. B. "Postdienst, öffentliches Wählnetz") zu machen. Werden mehrere Geräte eingesetzt, ist jedes einzelne Gerät zu beschreiben.

Dresden, den 29. September 1993

Der Sächsische Datenschutzbeauftragte
Dr. Giesen

Dateibeschreibung für das Dateien- und Geräteverzeichnis gemäß § 10 SächsDSG

Stempel der öffentlichen Stelle:

Das Verzeichnis wurde aufgestellt am:

Unterschrift:

Änderungen:

Behördlicher Datenschutzbeauftragter:

Bei nicht ausreichendem Platz Anlage für die jeweilige Ziffer beifügen

1. Bezeichnung der Datei und ihre Zweckbestimmung

2. Aufgaben und Rechtsgrundlage der Verarbeitung

3. Art der gespeicherten Daten

4. Betroffener Personenkreis

5. Regelmäßig zu übermittelnde und zu empfangende Daten

5.1 Art der regelmäßig zu übermittelnden Daten und deren Empfänger

Art	Empfänger	Rechtsgrundlage

5.2 Art und Herkunft der regelmäßig zu empfangenden Daten

Art	Herkunft

6. Fristen für die Sperrung und Löschung sowie deren Prüfung

Sperrungsfristen:

Löschungsfristen:

Prüfung der Fristen:

7. Zugriffsberechtigte Personen oder Personengruppen

Erteilung der Zugriffsberechtigung durch:

8. Personelle, technische und organisatorische Maßnahmen gemäß § 9 SächsDSG

Dienstanweisung:

Maßnahmen:

9. Weitere Angaben bei automatisierten Verfahren

Betriebsart:

Art der Geräte:

Übermittlungsverfahren:

Sperrungsverfahren:

Löschungsverfahren:

Auskunftserteilung:

10. Eingesetzte Hardware und Betriebssystem-Software

Typ: Art:

Hersteller: Betriebssystem:

Gerätenummer:

Funktionen für Datenfernverarbeitung/ Datenübertragung:

16.1.4 **(SächsABl. S. 1304)**

Bekanntmachung des Sächsischen Datenschutzbeauftragten zur Datenverarbeitung im Auftrag (§ 7 SächsDSG) und zur Rechtsstellung des beauftragten Unternehmers (§ 2 Abs. 2 SächsDSG) Vom 3. November 1993

Zur Datenverarbeitung im Auftrag und zur Rechtsstellung des beauftragten Unternehmers werden folgende Hinweise gegeben:

I. Datenverarbeitung im Auftrag (§ 7)

1. § 7 des Gesetzes zum Schutz der informationellen Selbstbestimmung im Freistaat Sachsen (Sächsisches Datenschutzgesetz - SächsDSG) vom 11. Dezember 1991 (SächsGVBl. 401) regelt die Rechtsverhältnisse bei der Übertragung von **Hilfsaufgaben** im Rahmen der Verarbeitung personenbezogener Daten durch öffentliche Stellen als Auftraggeber an öffentliche oder nicht-öffentliche Stellen als Auftragnehmer. Der Auftragnehmer wird lediglich als Erfüllungsgehilfe des Auftraggebers tätig: Er hat sich als **bloßer Helfer des Auftraggebers** bei der Erfüllung seiner Aufgaben stets im Rahmen der Anforderungen zu bewegen, die für den Auftraggeber gelten. Es steht ihm kein eigener Beurteilungs- oder Entscheidungspielraum zu. Auftragsdatenverarbeitung liegt nur dann vor, wenn der Auftragnehmer lediglich **technische Hilfe** im Rahmen der Datenverarbeitung leistet.

2. Für die Anwendbarkeit des § 7 SächsDSG ist Voraussetzung, daß die Datenverarbeitung in ihrer den Auftraggeber bei dessen Aufgabenerfüllung lediglich unterstützenden Funktion **ausgelagert** wird. Die Auftragsdatenverarbeitung kann sich auch auf einzelne Phasen der Datenverarbeitung beschränken (z. B. indem ein Schreibbüro die Daten speichert oder ein Aktenvernichtungsunternehmen die Daten löscht; § 3 Abs. 2 Nr. 2 bzw. Nr. 7 SächsDSG). Der Auftraggeber bleibt stets '**Herr der Daten'.** Er ist dafür verantwortlich, daß die Aufgaben den gesetzlichen Vorschriften entsprechend (Sächsisches Datenschutzgesetz oder diesem vorgehende besondere Rechtsvorschriften des Freistaates Sachsen oder des Bundes, § 2 Abs. 4 SächsDSG) erledigt werden.

3. § 7 SächsDSG trifft keine Aussage über die **Qualität der** dem Auftragsverhältnis zugrunde liegenden personenbezogenen **Daten**. In erster Linie ergeben sich Möglichkeiten und Grenzen für Aufträge, **bestimmte Datenarten** verarbeiten zu lassen, aus den **bereichsspezifischen Vorschriften (Spezialgesetzen)**, siehe Nr. 4. Falls solche speziellen Rechtsvorschriften nicht bestehen, müssen die Anforderungen an die Auswahl des Auftragnehmers und an Art und Umfang der zu treffenden Schutzmaßnahmen von der **Schutzwürdigkeit** (Sensibilität) der Daten abhängig gemacht werden. Dies gebietet der Grundsatz der Verhältnismäßigkeit. Als ein **Anhaltspunkt** für den Grad der Schutzwürdigkeit von Daten kann folgende, sich nach dem Grad der **möglichen** Auswirkung eines Mißbrauchs für den Betroffenen ergebende **Abstufung** dienlich sein:

Stufe A: Unerhebliche Beeinträchtigung
Beispiele: frei zugängliche Daten wie
Adreßbuchangaben,
Branchenverzeichnisse,
Gästeinformationen über Vermieter.

Stufe B: Beeinträchtigung in der gesellschaftlichen Stellung oder den wirtschaftlichen Verhältnissen
Beispiele: Mietverhältnisse,
Geschäfts- und Vertragsbeziehungen,
Zugehörigkeit zu Vereinen und Verbänden,
verwandtschaftliche Beziehungen,
Bekanntenkreis.

Stufe C: Erhebliche Beeinträchtigung in der gesellschaftlichen Stellung oder den wirtschaftlichen Verhältnissen
Beispiele (vgl. auch § 28 Abs. 2 Nr. 1 BDSG):
gesundheitliche Verhältnisse,
strafbare Handlungen,
Ordnungswidrigkeiten,
religiöse oder politische Anschauungen,
arbeitsrechtliche Verhältnisse,
Steuerdaten,
Sozialdaten,
Unterbringung in Anstalten,
Adoptionen,
Betreuungen,
Wahlausschlüsse,
Paßversagungsgründe.

Stufe D: Gefahr für Leib und Leben und für die persönliche Freiheit
Beispiele: Adressen von V-Leuten,
Adressen von Kronzeugen.

Die Zuordnung der Einzelfälle zu den Schutzstufen ist nicht schematisch möglich, sondern bleibt der Einzelbeurteilung überlassen. Die korrekte Einordnung ergibt sich immer aus dem Verwendungszusammenhang. Auch vermeintlich belanglose Daten können in einem bestimmten Zusammenhang wesentliche Auswirkungen haben.

Es ist der Grundsatz zu beachten, daß von einer Auftragsvergabe vorrangig stets die personenbezogenen Daten mit geringerer Schutzwürdigkeit (Sensibilität) betroffen sein sollten.

4. Wie unter Nr. 3 erwähnt, sind bei der Auftragsvergabe **bereichsspezifische Vorschriften** zu berücksichtigen. So dürfen die Meldebehörden nach § 3 des **Sächsischen Meldegesetzes** nur sächsische juristische Personen des öffentlichen Rechts mit der automatisierten Führung des Melderegisters beauftragen. Andere Auftragnehmer müssen insoweit nach § 38 Abs. 2 SächsMG ihre Tätigkeit bis Ende

1993 einstellen. Es ist möglich, daß die Gemeinden sich als Meldebehörden zu Zweckverbänden zusammenschließen; diese können auch private Unterauftragnehmer beauftragen.

Das **Sächsische Krankenhausgesetz** läßt eine Auftragsdatenverarbeitung von Patientendaten unter bestimmten Voraussetzungen zu, wobei es der Zustimmung der zuständigen Behörde bedarf, § 33 Abs. 10 SächsKHG.

Eine Besonderheit weist der **Sozialbereich** auf: Für die Verarbeitung dem Sozialgeheimnis unterliegender personenbezogener Daten im Auftrag gilt auch für öffentliche Stellen des Freistaates Sachsen nicht das Sächsische Datenschutzgesetz, sondern § 80 SGB X, § 11 BDSG (Hinweis: Die derzeitige Fassung des SGB bezieht sich noch auf das BDSG 1977, heute anzuwenden sind aber im Wege der dynamischen Verweisung die entsprechenden Bestimmungen des BDSG 1990). Nach § 80 Abs. 5 SGB X ist die Auftragsdatenverarbeitung durch nicht-öffentliche Stellen nur zulässig, wenn anders Störungen im Betriebsablauf nicht vermieden werden oder Teilvorgänge der Datenverarbeitung hierdurch erheblich kostengünstiger besorgt werden können. Diese Regelung umfaßt u. a. Leistungen der Arbeitsförderung, Vorruhestandsleistungen, Leistungen der Sozialversicherung (z. B. gesetzliche Krankenversicherung, Rentenversicherung), Kindergeld und Erziehungsgeld, Wohngeld, Leistungen der Kinder- und Jugendhilfe, der Sozialhilfe und nach dem Bundesausbildungsförderungsgesetz.

Einen strengen Schutz genießt das **Steuergeheimnis** (§ 30 AO), eine Regelung, die zum Teil auch in den Straftatbestand des § 355 StGB übernommen worden ist. Um zu vermeiden, daß dem Steuergeheimnis unterliegendes Daten privaten Auftragnehmern und deren Personal zur Kenntnis gelangen, sollte von einer Auftragsvergabe an Private, die nicht Amtsträger oder diesen gemäß § 30 Abs. 2 AO gleichgestellt sind, abgesehen werden. Eine Offenbarung liegt in jedem Verhalten, auf Grund dessen einem anderen Verhältnisse eines Dritten oder fremde Betriebs- und Geschäftsgeheimnisse bekannt werden oder bekannt werden könnten (Tipke-Kruse, Kommentar zur AO, Tz. 31 zu § 30). Die **befugte** Offenbarung ist abschließend in § 30 Abs. 4 AO geregelt.

Bei der Auftragsvergabe sind gegebenenfalls auch § 18 SächsStatG (**Statistikgeheimnis**), § 203 StGB (**Verletzung von Privatgeheimnissen**) und § 9 SächsMG (**Meldegeheimnis**) zu beachten.

5. Der Auftraggeber hat den Auftragnehmer (möglichst unter mehreren Anbietern; Hinweis: siehe auch § 55 Sächsische Haushaltsordnung) **sorgfältig auszuwählen**. Er hat sich vor Auftragserteilung gegebenenfalls zu erkundigen, ob das Unternehmen bisher vergleichbaren Aufträgen ordnungsgemäß nachgekommen ist. Er hat weiter zu prüfen, ob die Organisation und die Einrichtung des Unternehmens sich für eine Datenverarbeitung der vorgesehenen Art eignen. Insbesondere hat er sich das Datenschutzkonzept vor Ort im einzelnen nachweisen zu lassen. Insgesamt muß er sich davon überzeugen, daß der Datenschutz nach der Art der zu verarbeitenden Daten mindestens den Anforderungen genügt, die für ihn selbst gelten. Handelt es

sich um ein nicht-öffentliches Unternehmen, ist zu prüfen, ob der Auftragnehmer seiner Meldepflicht nach § 32 Abs. 1 Nr. 3 BDSG nachgekommen ist.

6. Der Auftrag ist **schriftlich** zu erteilen. Ein Auftragsverhältnis im Sinne des BGB dürfte in der Regel nicht vorliegen. Dies ergibt sich schon daraus, daß der Auftrag gemäß § 662 BGB Unentgeltlichkeit voraussetzt, was bei einem der Auftragsdatenverarbeitung entsprechenden Rechtsverhältnis nicht gemeint sein kann. Es wird sich in der Regel um einen Werkvertrag (§ 631 BGB) handeln.

7. **In dem schriftlichen Vertrag sollten in Bezug auf den Datenschutz geregelt werden:**
   - Gegenstand und Umfang der Datenverarbeitung,
   - die erforderlichen personellen, technischen und organisatorischen Maßnahmen nach dem Stand der Technik (§ 9 SächsDSG),
   - Verfahren bei Auskunft, Berichtigung, Löschung und Sperrung (§§ 17 bis 20 SächsDSG),
   - inhaltliche Vorgaben für Unterauftragsverhältnisse (z. B. Kurierdienste) oder Zustimmungsvorbehalt des Auftraggebers für künftige Unterauftragsverhältnisse,
   - alleiniges Weisungs- und Verfügungsrecht des Auftraggebers über die Daten im Rahmen des Vertrages,
   - Kontrollrechte des Auftraggebers,
   - Beginn der Datenverarbeitungsmaßnahmen erst nach Freigabe der Verfahren durch den Auftraggeber,
   - gegebenenfalls Vertragsstrafen,
   - Kündigungsrechte, insbesondere bei Verletzung von Datenschutzvorschriften durch den Auftragnehmer,
   - Unterwerfung unter die Kontrolle des Sächsischen Datenschutzbeauftragten (vgl. Nr. 11).

8. Nach § 7 Abs. 1 SächsDSG ist bei der Datenverarbeitung im Auftrag **auch** der Auftraggeber für die Einhaltung des Gesetzes und anderer Vorschriften über den Datenschutz verantwortlich. Mit dieser Fassung, die lediglich durch die Einbeziehung des Wortes "auch" von den Datenschutzgesetzen der anderen Bundesländer abweicht, soll zum Ausdruck gebracht werden, daß den Auftragnehmer im Rahmen des Auftrags eine spezielle Verantwortung trifft. Das Gesetz will jedoch keine selbständige Verantwortlichkeit des Auftragnehmers gegenüber dem Betroffenen begründen. Andererseits kann sich der Auftraggeber durch vertragliche Vereinbarung nicht von seiner gesetzlichen Verantwortung freizeichnen.

   Die sich aus der zusätzlichen Verantwortlichkeit des Auftragnehmers ergebenden Pflichten müssen im Vertrag konkret benannt werden:
   - Der Auftragnehmer hat die bei der Datenverarbeitung beschäftigten Personen auf Einhaltung des Datengeheimnisses zu verpflichten (vgl. hierzu die Bekanntmachung des Sächsischen Datenschutzbeauftragten vom 22. Juli 1993, SächsABl. S. 970).
   - Der Auftragnehmer ist gegebenenfalls verpflichtet, den Auftraggeber unverzüglich darauf hinzuweisen, daß die Ausführung des Auftrags gegen datenschutzrechtliche Vorschriften verstoßen würde (§ 7 Abs. 2 Satz 5 SächsDSG).

Daraus folgt: Kann der Auftraggeber den Auftragnehmer von der Rechtmäßigkeit der Datenverarbeitung nicht überzeugen, beispielsweise daß die Speicherung bestimmter personenbezogener Daten erforderlich ist, darf dieser den Auftrag nicht ausführen; zweckmäßigerweise sollte der Auftragnehmer in diesem Fall sich an den Sächsischen Datenschutzbeauftragten wenden und die Ausführung des Auftrags von dessen Stellungnahme abhängig machen.

Aufgeführt werden sollten außerdem etwaige weitere Pflichten, die sich aus den dem Auftrag zugrunde liegenden **bereichsspezifischen Rechtsvorschriften** ergeben.

9. **Die Verantwortlichkeit des Auftraggebers** für die Einhaltung der datenschutzrechtlichen Bestimmungen wird nicht dadurch gemindert, daß er einen Auftragnehmer als Hilfe hinzuzieht; Risiko und Haftung verbleiben beim Auftraggeber. Der Auftraggeber hat insbesondere darauf zu achten, daß sämtliche unter datenschutzrechtlichen Gesichtspunkten erforderlichen Modalitäten der Leistungserbringung durch den Auftragnehmer in den Vertragstext ('Pflichtenheft') aufgenommen werden. Ihm gegenüber können die Betroffenen ihre Rechte geltend machen (Rechte auf Auskunft, Berichtigung, Löschung, Sperrung und Schadensersatz §§ 17 bis 21 SächsDSG).

   Der Auftraggeber hat die Einhaltung der vereinbarten Maßnahmen durch **eigene Kontrollen** zu überprüfen, um zu gewährleisten, daß die Datenverarbeitung vom Auftragnehmer vertragsgemäß durchgeführt wird.

10. Der Auftragnehmer ist **nicht Dritter im Sinne des § 3 Abs. 4 SächsDSG**, da er die Daten im Rahmen des Vertrages nicht in eigener Zuständigkeit verarbeitet. Deshalb ist die auftragsgemäße Weitergabe von Daten zwischen Auftraggeber und Auftragnehmer kein Übermitteln im Sinne des § 3 Abs. 2 Satz 2 Nr. 5 SächsDSG. Die §§ 13 und 15 SächsDSG (Übermitteln an öffentliche bzw. nicht-öffentliche Stellen) sowie § 8 Abs. 1 SächsDSG (Übermitteln durch Abruf) finden daher keine Anwendung. Dagegen ist § 8 Abs. 2 SächsDSG zu beachten, weil es sich hier um ein automatisiertes Abrufverfahren **innerhalb** einer öffentlichen Stelle handelt. **Vor** Einrichtung des Abrufverfahrens ist der Sächsische Datenschutzbeauftragte zu unterrichten, § 8 Abs. 3 SächsDSG.

11. **Kontrolle durch den Sächsischen Datenschutzbeauftragten bei der Datenverarbeitung im Auftrag**
    Ist der Auftragnehmer öffentliche Stelle i. S. des § 2 Abs. 1 SächsDSG, hat er sich durch den Sächsischen Datenschutzbeauftragten kontrollieren zu lassen und diesen im Rahmen der Kontrollbefugnis nach § 24 SächsDSG zu unterstützen, insbesondere Auskünfte zu erteilen sowie Einsicht in alle Unterlagen und Akten zu gewähren, § 25 SächsDSG.

    Ist der Auftragnehmer nicht-öffentliche Stelle, besteht keine unmittelbare Kontrollbefugnis nach dem Vierten Abschnitt des Sächsischen Datenschutzgesetzes. Deshalb hat der Auftraggeber dafür zu sorgen, daß ein den §§ 24 und 25 SächsDSG entsprechendes Kontrollrecht des Sächsischen Datenschutzbeauftragten mit Unterstützungspflicht des Auftragnehmers in den Vertrag aufgenommen wird, wobei

sich der Auftragnehmer der Kontrolle durch den Sächsischen Datenschutzbeauftragten unterwirft. Unterläßt dies der Auftraggeber, setzt er sich der Gefahr einer Beanstandung nach § 26 SächsDSG aus, da er gemäß § 25 SächsDSG dafür zu sorgen hat, daß der Sächsische Datenschutzbeauftragte jederzeit uneingeschränkt kontrollieren kann.

Soweit die Datenverarbeitung vom Auftragnehmer in einem anderen Bundesland durchgeführt wird, hat der Auftraggeber ebenfalls dafür zu sorgen, daß sich der Auftragnehmer der Kontrolle durch den Sächsischen Datenschutzbeauftragten unterwirft. Es bleibt sodann dem Sächsischen Datenschutzbeauftragten überlassen, ob er die Kontrolle selbst durchführt oder sich der Amtshilfe des zuständigen Landesdatenschutzbeauftragten bedient.

II. Der beauftragte Unternehmer (§ 2 Abs. 2)

12. Keine Datenverarbeitung im Auftrag liegt vor, wenn öffentliche Stellen als Auftraggeber natürlichen und juristischen Personen oder (nichtrechtsfähigen) Vereinigungen des privaten Rechts **die Wahrnehmung von Aufgaben der öffentlichen Verwaltung** übertragen. Hier handelt es sich im Innenverhältnis um einen in der Regel zivilrechtlichen Geschäftsbesorgungsvertrag mit Dienst- oder Werkvertragscharakter. Dem Auftragnehmer wird eine ansonsten von der öffentlichen Stelle wahrgenommene **Funktion zur selbständigen Erledigung** übertragen. Im Vordergrund eines solchen Vertrages steht nicht die Verarbeitung personenbezogener Daten, sondern die eigenständige, nach außen gerichtete Tätigkeit. Der Auftragnehmer nutzt die Datenverarbeitung nur als Hilfsmittel für die eigene Tätigkeit. **Er wird** durch die Fiktion des § 2 Abs. 2 Satz 1 SächsDSG **selbst öffentliche Stelle.**
Beispiel: Eine Gemeinde benötigt statistische Informationen zur Entscheidung , ob ein Gewerbegebiet geplant werden soll. Führt die Gemeinde die Statistik (die gemäß § 8 Abs. 1 SächsStatG der Satzung bedarf) selbst durch, wobei sie sich zur technischen Aufbereitung der Daten eines Rechenzentrums bedient, handelt es sich um Auftragsdatenverarbeitung. Beauftragt die Gemeinde dagegen ein Meinungsforschungsinstitut, diese Erhebung nach bestimmten Vorgaben durchzuführen, liegt eine Funktionsübertragung i. S. des § 2 Abs. 2 Satz 1 SächsDSG vor. Das Meinungsforschungsinstitut gilt, soweit es die Statistik durchführt, für die Anwendung des Sächsischen Datenschutzgesetzes als öffentliche Stelle.

13. Die natürlichen und juristischen Personen sowie Vereinigungen des privaten Rechts, die -wie unter Nr. 12 dargelegt - Aufgaben der öffentlichen Verwaltung gemäß § 2 Abs. 2 Satz 1 SächsDSG wahrnehmen, können als **beauftragte Unternehmer** bezeichnet werden. Vom **beliehenen Unternehmer** (z. B. Bezirksschornsteinfegermeister, TÜV, öffentlich bestellte Vermessungsingenieure) unterscheiden sich die beauftragten Unternehmer dadurch, daß sie lediglich **auf Grund einer Vereinbarung** Aufgaben der öffentlichen Verwaltung erledigen, die nicht hoheitlicher Natur sind. Der **beliehene Unternehmer** übt dagegen hoheitliche

Funktionen in eigenem Namen aus, ohne Teil der staatlichen oder kommunalen Organisation zu sein. Ihm werden **auf Grund Gesetzes** hoheitliche Aufgaben übertragen; mit seiner Bestellung ist der beliehene Unternehmer **sonstige öffentliche Stelle** des Landes oder einer Kommune, § 2 Abs. 1 SächsDSG.

14. **Vereinigungen des privaten Rechts** sind diejenigen Zusammenschlüsse, die keine juristischen Personen sind, also u. a. BGB-Gesellschaften, nichtrechtsfähige Vereine, Offene Handelsgesellschaften nach § 105 HGB, die beispielsweise von der Gemeinde als Sanierungsbeauftragte gemäß § 138 Abs. 1 BauGB eingeschaltet werden.

    Mitglieder einer Vereinigung privaten Rechts können auch öffentlich-rechtliche Körperschaften sein.
15. Die Fiktion des § 2 Abs. 2 Satz 1 SächsDSG greift gemäß § 2 Abs. 2 Satz 2 SächsDSG nicht Platz, sofern es sich um **öffentliche Stellen des Bundes im Sinne des § 2 Abs. 3 und 4 BDSG** handelt. Hier handelt es sich um Bund-Länder-Mischvereinigungen gemäß § 2 Abs. 3 BDSG (vgl. Nr. 16) und um nicht-öffentliche Stellen gemäß § 2 Abs. 4 BDSG (vgl. Nr. 17).

16. Das **Bundesdatenschutzgesetz** findet bei **Bund-Länder-Mischvereinigungen**, die Aufgaben der öffentlichen Verwaltung wahrnehmen (und sich nicht am Wettbewerb beteiligen) Anwendung, wenn sie länderübergreifend tätig werden **oder** wenn dem Bund die absolute Mehrheit der Anteile oder der Stimmen zusteht, § 2 Abs. 3 Satz 1 BDSG. In der Regel handelt es sich um privatrechtlich organisierte Einrichtungen, z. B. Verband deutscher Rentenversicherungsträger bzw. ein Verkehrsverbund.

17. Das **Bundesdatenschutzgesetz** ist ferner anzuwenden bei nicht-öffentlichen Stellen **des Bundes**, **soweit** diese **hoheitliche** Aufgaben der öffentlichen Verwaltung wahrnehmen. Es handelt sich hier um beliehene Unternehmer, die ihre Bestellung von einer Bundesbehörde erhalten haben, § 2 Abs. 4 BDSG.

18. Der beauftragte Unternehmer unterliegt uneingeschränkt den Bestimmungen des Sächsischen Datenschutzgesetzes, soweit dies den öffentlichen Stellen Pflichten auferlegt.

Dresden, den 3. November 1993

Der Sächsische Datenschutzbeauftragte
Dr. Giesen

16.2 Entschließungen der Datenschutzbeauftragten des Bundes und der Länder

16.2.1 Entschließung der 46. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 26./27. Oktober 1993 in Berlin zu regelmäßigen Datenübermittlungen an die öffentlich-rechtlichen Rundfunkanstalten und die Gebühreneinzugszentrale (GEZ)[1]

Die öffentlich-rechtlichen Rundfunkanstalten drängen seit langem auf die Schaffung einer Rechtsgrundlage für die regelmäßige Übermittlung von Meldedaten aller Einwohner an die gemeinsame Gebühreneinzugszentrale (GEZ). Sie verweisen dazu auf bereits bestehende Regelungen in den Ländern Hessen und Nordrhein-Westfalen. Auf Bitten der Konferenz der Regierungschefs der Länder hat deshalb nunmehr der zuständige Arbeitskreis der Innenministerkonferenz einen Musterentwurf für eine bundesweite Lösung im Melderecht erarbeitet. Der Entwurf sieht vor, daß künftig alle Meldebehörden in der Bundesrepublik im Fall der Anmeldung, Abmeldung oder des Todes eines volljährigen Einwohners bis zu acht Kerndaten an die GEZ übermitteln dürfen.

Die Datenschutzbeauftragten des Bundes und der Länder lehnen eine derartige Regelung aus folgenden Gründen ab:

Die Regelung könnte im Ergebnis zu einem bundesweiten Melderegister bei Volljährigen führen. Sie könnte außerdem gegen das verfassungsrechtlich garantierte Verhältnismäßigkeitsprinzip verstoßen. Den Rundfunkanstalten stünde möglicherweise der unkontrollierte Zugriff auf Millionen personenbezogener Daten volljähriger Einwohner der Bundesrepublik zu, obwohl es für die Rundfunkanstalten nur von Interesse ist, welcher Einwohner bei ihnen gebührenpflichtig ist und bislang seine Gebührenpflicht nicht angemeldet hat. Das vorgesehene generelle Übermittlungsverfahren kennt keine Unterscheidung zwischen erforderlichen und nicht erforderlichen Daten, sondern überläßt diese Unterscheidung der GEZ. über die Frage, ob ein Volljähriger überhaupt gebührenpflichtig ist, geben die Meldedaten keine Auskunft. Das muß nach wie vor im herkömmlichen Verfahren durch Befragung ermittelt werden.

Die Datenschutzbeauftragten des Bundes und der Länder sind bereit, an geeigneten und verfassungskonformen Lösungen der Landesregierungen zur Sicherung des Gebührenaufkommens der Rundfunkanstalten mitzuwirken.

16.2.2 Entschließung der 46. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 26./27. Oktober 1993 in Berlin zum Datenschutz bei der Privatisierung der Deutschen Bundespost Telekom und bei der europaweiten Liberalisierung des Telefonnetzes und anderer Telekommunikationsdienste

Im Zuge der sog. Postreform II soll die Deutsche Bundespost Telekom - nach der dafür notwendigen Änderung des Grundgesetzes - in Form einer Aktiengesellschaft priva-

[1] gegen die Stimme Bayerns und bei Stimmenthaltung Sachsens

tisiert werden. Zugleich hat der Ministerrat der Europäischen Gemeinschaften in seiner Entschließung vom 22. Juli 1993 (Amtsblatt der EG Nr. C 213 vom 6. 8. 1993) seine Entschlossenheit bekräftigt, die Monopole im öffentlichen Sprachtelefondienst (Festnetz) der Mitgliedstaaten bis zum 1. Januar 1998 zu beseitigen.

In absehbarer Zeit werden daher in Deutschland neben der "Telekom AG" auch im Telefondienst andere private Unternehmen Telekommunikationsdienstleistungen anbieten. Diese Privatisierung hat Konsequenzen für den Datenschutz, der bisher für die Deutsche Bundespost Telekom auf einem vergleichsweise hohen Niveau geregelt ist. Insbesondere das grundgesetzlich garantierte Fernmeldegeheimnis würde für private Netzbetreiber und Diensteanbieter jedenfalls nicht mehr unmittelbar gelten.

Die Datenschutzbeauftragten des Bundes und der Länder halten es für unabdingbar, daß durch die Privatisierung und Liberalisierung der Schutz der Bürger insbesondere in solchen Bereichen nicht verringert wird, die - wie der Telefondienst - der Daseinsvorsorge zuzurechnen sind. So wie bisher die konkurrierenden privaten Betreiber der Mobilfunknetze einen gleichmäßig hohen Datenschutzstandard gewährleisten müssen, hat dies auch zu gelten, wenn in Zukunft private Unternehmen im Wettbewerb miteinander stationäre Telefonnetze betreiben und entsprechende Dienste anbieten. Die Einhaltung von datenschutzrechtlichen Bestimmungen bei Telekommunikationsnetzen und -diensten muß zukünftig von einer unabhängigen Stelle nach bundesweit einheitlichen Kriterien und von Amts wegen kontrolliert werden können.

Da der Wettbewerb zwischen privaten Netzbetreibern und Diensteanbietern nicht nur national begrenzt, sondern im europäischen Binnenmarkt stattfinden wird, sind auch Rechtsvorschriften der Europäischen Gemeinschaften erforderlich, die einen möglichst hohen, einheitlichen Datenschutzstandard in der Telekommunikation gewährleisten.

16.2.3 Entschließung der 46. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 26./27. Oktober 1993 in Berlin zur Gewährleistung des Datenschutzes bei der Mobilkommunikation

Die Verbreitung mobiler Sprach- und Datenübertragungsdienste hat in jüngster Vergangenheit stark zugenommen. So gibt es bereits jetzt in Deutschland mehr als eine Million Teilnehmer der Funktelefonnetze C und D; mit der Aufnahme des Regelbetriebs von MODACOM ist seit Juni dieses Jahres auch ein öffentlicher mobiler Datenübertragungsdienst in Deutschland verfügbar. Es ist zu erwarten, daß sich die Teilnehmerzahl mobiler Kommunikationsdienste in Zukunft weiter vergrößern wird.

Die mit der Nutzung von Mobilfunkdiensten verbundenen Vorteile gehen mit Gefährdungen für den Datenschutz einher. Neben den auch bei anderen Telekommunikationsdiensten gespeicherten Angaben, wer wann mit wem in Verbindung war, wird bei der Mobilkommunikation auch erhoben, wo sich der mobile Teilnehmer jeweils aufhält. Die Speicherung dieser Daten ermöglicht die Bildung von problematischen Bewegungsprofilen.

Darüber hinaus ist vielfach auch die Vertraulichkeit der Kommunikationsinhalte gefährdet, insbesondere dann, wenn Daten unverschlüsselt per Funk übertragen werden. Dies

gilt sowohl für die analogen Funktelefon-Netze B und C als auch für den von der Deutschen Bundespost Telekom betriebenen mobilen Datenübertragungsdienst MODACOM. Bei satellitengestützten Diensten ist es sogar möglich, die übertragenen Daten im gesamten teilweise viele tausend Quadratkilometer umfassenden Abstrahlbereich des Satelliten unbemerkt abzuhören und aufzuzeichnen.

Von den Herstellern und Betreibern mobiler Kommunikationsdienste ist zu fordern, daß sie diesen Gefahren für das Fernmeldegeheimnis und für den Datenschutz durch eine entsprechende Gestaltung entgegenwirken und technische Vorkehrungen für eine sichere Kommunikation treffen.

Die Teilnehmer mobiler Kommunikationsdienste müssen von den Anbietern, Herstellern und Betreibern über die mit der Nutzung verbundenen Risiken und das erreichte Sicherheitsniveau aufgeklärt werden. Sofern bei bestimmten Diensten Sicherheitsmerkmale realisiert sind - wie z.B. in den digitalen D-Netzen -, muß die Sicherheit für die Aufsichts- und Kontrollorgane auch nachprüfbar sein. Falls durch den Dienstbetreiber nicht die erforderliche Sicherheit gewährleistet werden kann, ist eine Übertragung personenbezogener oder sonstiger sensibler Daten mit dem jeweiligen Dienst nur dann vertretbar, wenn der Benutzer zusätzliche Sicherheitsvorkehrungen trifft, also z.B. die übertragenen Daten anwendungsseitig verschlüsselt.

Zusätzlich kompliziert wird die Datenschutzproblematik bei der Mobilkommunikation dadurch, daß unter Umständen bei verschiedenen Dienst- und Netzbetreibern, aber auch bei anderen Unternehmen - den sogenannten Service-Providern, die lediglich Dienste vermarkten - personenbezogene Daten gespeichert werden.

Hier muß im Zuge der anstehenden Überarbeitung des Telekommunikationsrechts dafür Sorge getragen werden, daß sich die Verarbeitung der Kommunikationsdaten auf das wirklich erforderliche Maß beschränkt und daß die Nutzer darüber aufgeklärt werden, bei welcher Stelle welche personenbezogenen Daten gespeichert oder sonst verarbeitet werden.

Besonders problematisch ist es, wenn bei der internationalen Mobilkommunikation auch in solchen Staaten personenbezogene Daten gespeichert werden, in denen kein ausreichendes Datenschutzniveau gewährleistet ist oder in denen das Fernmeldegeheimnis nicht sichergestellt wird. Deshalb ist es erforderlich, auf internationaler Ebene Regelungen zu treffen, die den Datenschutz bei mobilen Kommunikationsdiensten gewährleisten.

Die Konferenz unterstreicht aus diesem Grunde ihre Forderung, die Arbeiten an der EG Richtlinie über Datenschutz im ISDN und in öffentlichen digitalen Mobilfunknetzen zu einem datenschutzrechtlich befriedigenden Abschluß zu bringen. Auch für den noch gänzlich datenschutzrechtlich ungeregelten Bereich der Satellitenkommunikation müssen endlich völkerrechtlich verbindliche Regelungen getroffen werden.

16.2.4 Entschließung der 46. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 26./27. Oktober 1993 in Berlin zu kartengestützten Zahlungssystemen im Öffentlichen Nahverkehr

Mit der Weiterentwicklung von Chipkarten werden kartengestützte Zahlungssysteme zunehmend auch im Verkehrsbereich eingesetzt. Damit besteht die Gefahr, daß sehr detaillierte Bewegungsprofile entstehen, die den persönlichen Bereich jedes Einzelnen einschränken und z.B. auch für Strafverfolgungsbehörden, Finanzämter und für die Werbewirtschaft von Interesse sein könnten. Da sämtliche Fahrten für einen gewissen Zeitraum aufgelistet werden können, hat jeder Kontoinhaber die Möglichkeit, Fahrten sämtlicher Familienmitglieder jederzeit nachzuvollziehen.

So sind im Öffentlichen Nahverkehr zahlreiche sogenannte Postpaid-Verfahren in Erprobung, bei denen dem Fahrgast am Monatsende die aufsummierten Fahrpreise vom Konto abgebucht werden. Diese Zahlungsweise erfordert die Speicherung umfangreicher personenbezogener Daten: Neben der Konto-Nr. und Bankleitzahl des Fahrgastes werden sowohl Datum und Uhrzeit des Fahrscheinkaufs bzw. des Fahrantritts als auch Automatennummer und Preisstufe der jeweiligen Fahrt erhoben.

Eine solche Vorgehensweise ist umso problematischer, als technische Alternativen existieren, die weitaus datenschutzfreundlicher sind. Im Öffentlichen Nahverkehr können - wie skandinavische und auch deutsche Projekte aufzeigen - Wertkartensysteme eingesetzt werden, bei denen im voraus bezahlt wird und die daher gänzlich ohne personenbezogene Daten auskommen.

Die Datenschutzbeauftragten halten es daher für dringend erforderlich, daß mehr als bisher bei der Einführung kartengestützter Zahlungssysteme darauf geachtet wird, die "datenfreie Fahrt" zu ermöglichen. Im öffentlichen Nahverkehr sollte weiterhin auch die datenschutzfreundlichste Lösung angeboten werden: Der Kauf einer Fahrkarte am Automaten mit Bargeld.

Die Konferenz fordert weiter, daß noch vor der Pilotierung der dargestellten Technikvorhaben im Verkehrsbereich eine Untersuchung möglicher Alternativen, eine Analyse der von ihnen ausgehenden Gefahren für das informationelle Selbstbestimmungsrecht und eine Darstellung der technischen und organisatorischen Möglichkeiten zur Gewährleistung des Persönlichkeitsschutzes zu erstellen ist (Technikfolgen-Abschätzung). Nur Verfahren mit dem geringsten Eingriff in das allgemeine Persönlichkeitsrecht sollten eine Chance zur Erprobung erhalten.

16.2.5 Entschließung der 46. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 26./27. Oktober 1993 in Berlin zur Gefährdung der Vertraulichkeit der Funkkommunikation von Sicherheitsbehörden und Rettungsdiensten

Durch die Aufhebung der bisher gültigen Beschränkungen der zulässigen Empfangsbereiche für Rundfunkempfänger zum 30. Juni 1992 werden zunehmend Empfangsgeräte betrieben, die das Abhören des Funkverkehrs ermöglichen. Dies stellt eine erhebliche

Bedrohung des Fernmeldegeheimnisses dar.

Die Datenschutzbeauftragten des Bundes und der Länder beobachten die damit verbundene Gefährdung der Vertraulichkeit der Funkkommunikation von Behörden und Organisationen mit Sicherheitsaufgaben (BOS) mit Sorge. Sie erkennen die Bemühungen der Polizeiverwaltungen der Länder an, durch zusätzliche technische Maßnahmen die Sicherheit des Sprechfunkverkehrs zu erhöhen. Sie stellen jedoch fest, daß die erforderliche Vertraulichkeit bisher nicht gewährleistet werden konnte. Auch Sprachverschleierungssysteme erreichen diese nicht hinreichend.

Daher begrüßt die Konferenz die im Rahmen des Schengener Abkommens getroffene grundsätzliche Entscheidung, im BOS-Bereich eine europäische Normierung zu erarbeiten, die die Digitalisierung und eine Verschlüsselung des BOS-Funkverkehrs vorsieht.

Die Konferenz hält es für erforderlich, daß das Normierungsverfahren so zügig wie möglich durchgeführt wird und auch schon vor der Umsetzung dieser Norm alle Möglichkeiten für einen effektiven Schutz der Vertraulichkeit des BOS-Funkverkehrs entsprechend dem jeweiligen Stand der Technik genutzt werden.

Die Konferenz weist weiter darauf hin, daß nicht nur bei den Behörden der Polizei, sondern auch in anderen BOS-Bereichen, wie z.B. dem Rettungswesen, eine Vertraulichkeit des Funkverkehrs zu gewährleisten ist. Daher sind auch in den übrigen BOS-Bereichen frühestmöglich entsprechende Absicherungen zur Vertraulichkeit des Funkverkehrs gefordert.

16.2.6 Entschließung der 47. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 09./10. März 1994 in Potsdam zu Chipkarten im Gesundheitswesen[1]

Die Datenschutzbeauftragten von Bund und Länder verfolgen die zunehmende Verwendung von Chipkarten im Gesundheits- und Sozialwesen mit kritischer Aufmerksamkeit.

Chipkarte als gesetzliche Krankenversicherungskarte

Die Krankenversicherungskarte, die bis Ende des Jahres in allen Bundesländern eingeführt sein wird, darf nach dem Sozialgesetzbuch nur wenige Identifikationsdaten enthalten. Die Datenschutzbeauftragten überprüfen, ob

- die Krankenkassen nur die gesetzlich zulässigen Daten auf den Chipkarten speichern und
- die Kassenärztlichen Vereinigungen dafür sorgen, daß nur vom Bundesamt für Sicherheit in der Informationstechnik zertifizierte Lesegeräte und vom Bundesverband der Kassenärztlichen Vereinigungen geprüfte Programme eingesetzt werden.

[1] Baden-Württemberg war in der Sitzung nicht vertreten, trägt den Beschluß jedoch inhaltlich mit.

Chipkarte als freiwillige Gesundheitskarte

Sogenannte "Gesundheitskarten", etwa "Service-Karten" von Krankenversicherungen und privaten Anbietern, "Notfall-Karten", "Apo(theken)-Cards" und "Röntgen-Karten" werden neben der Krankenversicherungskarte als freiwillige Patienten-Chipkarte angeboten und empfohlen. Während die Krankenversicherungskarte nach dem Sozialgesetzbuch nur wenige Identifikationsdaten enthalten darf, kann mit diesen "Gesundheitskarten" über viele medizinische und andere persönliche Daten schnell und umfassend verfügt werden.

Gegenüber der konventionellen Ausweiskarte oder einer Karte mit einem Magnetstreifen ist die Chipkarten-Technik ungleich komplexer und vielfältig nutzbar. Damit steigen auch die Mißbrauchsgefahren bei Verlust, Diebstahl oder unbemerktem Ablesen der Daten durch Dritte. Anders als bei Ausweiskarten mit Klartext können Chipkarten nur mit technischen Hilfsmitteln gelesen werden, die der Betroffene in der Regel nicht besitzt. So kann er kaum kontrollieren, sondern muß weitgehend darauf vertrauen, daß der Aussteller der Karte und sein Arzt nur die mit ihm vereinbarten Daten im Chip speichern, das Lesegerät auch wirklich alle gespeicherten Daten anzeigt und der Chip keine oder nur eindeutig vereinbarte Verarbeitungsprogramme enthält.

Die Freiwilligkeit der Entscheidung für oder gegen die Gesundheitskarte mit Chipkarten-Technik ist in der Praxis bisweilen nicht gewährleistet. So wird ein faktischer Zwang auf die Entscheidungsfreiheit des Betroffenen ausgeübt, wenn der Aussteller - etwa ein Krankenversicherungsunternehmen oder eine Krankenkasse - mit der Einführung der Chipkarte das bisherige konventionelle Verfahren erheblich ändert, z. B. den Schriftwechsel erschwert oder den Zugang zu Leistungen Karten-Inhabern vorbehält bzw. erleichert.

So stellt beispielsweise eine Kasse ihren Mitgliedern Bonuspunkte in Aussicht, wenn sie auf sog. Aktionstagen der Kasse Werte wie Blutzucker, Sauerstoffdynamik, Cholesterol sowie weitere spezielle medizinische Daten ohne ärztliche Konsultation messen und auf der Karte speichern und aktualisieren lassen. In Abhängigkeit von der Veränderung dieser Werte wird von der Kasse gegebenenfalls ein Arztbesuch empfohlen. Die Vergabe solcher Bonuspunkte widerspricht dem Prinzip der Freiwilligkeit bei der Erhebung der Daten für die Patienten-Chipkarte. Der Effekt wird noch verstärkt, indem die Kasse die "Möglichkeit einer Beitragsrückerstattung" in Aussicht stellt. Die Datenschutzbeauftragten des Bundes und der Länder sehen in dieser Art der Anwendung der Chipkarten-Technik das Risiko eines Mißbrauchs, solange der Inhalt und die Nutzung der Daten nicht mit den zuständigen Fachleuten - wie den Medizinern - und den Krankenkassen abgestimmt ist.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hält für den Einsatz und die Nutzung freiwilliger Patienten-Chipkarten zumindest - vorbehaltlich weiterer Punkte - die Gewährleistung folgender Voraussetzungen für erforderlich:

- Die Zuteilung einer Gesundheitskarte und die damit verbundene Speicherung von Gesundheitsdaten bedarf der schriftlichen Einwilligung des Betroffenen. Er ist vor der Erteilung der Einwilligung umfassend über Zweck, Inhalt und Verwendung der angebotenen Gesundheitskarte zu informieren.

- Die freiwillige Gesundheitskarte darf nicht - etwa durch Integration auf einem Chip - die Krankenversichertenkarte nach dem Sozialgesetzbuch verdrängen oder ersetzen.
- Die Karte ist technisch so zu gestalten, daß für die einzelnen Nutzungsarten nur die jeweils erforderlichen Daten zur Verfügung gestellt werden.
- Der Betroffene muß von Fall zu Fall frei und ohne Benachteiligung - z. B. gegenüber dem Arzt, der Krankenkasse oder der Versicherung - entscheiden können, die Gesundheitskarte zum Lesen der Gesundheitsdaten vorzulegen und ggf. den Zugriff auf bestimmte Daten zu beschränken. Er muß ferner frei entscheiden können, wer welche Daten in seinen Datenbestand übernehmen darf. Der Umfang der Daten, die gelesen oder übernommen werden dürfen, ist außerdem durch die gesetzliche Aufgabenstellung bzw. den Vertragszweck der Nutzer beschränkt.
- Der Kartenaussteller muß sicherstellen, daß der Betroffene jederzeit vom Inhalt der Gesundheitskarte unentgeltlich Kenntnis nehmen kann.
- Der Betroffene muß jederzeit Änderungen und Löschungen der gespeicherten Daten veranlassen können.

Die Datenschutzbeauftragten des Bundes und der Länder sprechen sich dafür aus, daß der Gesetzgeber dies durch bereichsspezifische Rechtsgrundlagen sicherstellt.

16.2.7 Entschließung der 47. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 09./10. März 1994 in Potsdam zum Abbau des Sozialdatenschutzes[1]

Der Gesetzgeber hat in den vergangenen Monaten die Möglichkeit der Überprüfung von Sozialleistungsempfängern ohne deren vorherige Befragung oder Kenntnis in drastischem Umfang vermehrt. Insbesondere durch das seit dem 1. Juli 1993 geltende Gesetz zur Umsetzung des Föderalen Konsolidierungsprogramms ist das Kontrollinstrumentarium von Sozial- und Arbeitsämtern noch einmal erheblich erweitert worden. Ohne Rücksicht auf konkrete Anhaltspunkte für einen unberechtigten Leistungsbezug im Einzelfall sind künftig automatisierte Datenabgleiche zwischen Sozialhilfeträgern sowie zwischen diesen und der Arbeitsverwaltung bzw. der Kranken-, Unfall- und Rentenversicherung gestattet.
Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder ist sehr besorgt über diese Entwicklung, die zu einem immer dichteren Datenverbundsystem im Sozialleistungsbereich und zu immer nachhaltigeren Eingriffen in das Recht auf informationelle Selbstbestimmung aller Betroffenen, d. h. auch und gerade der großen Mehrheit rechtstreuer Antragsteller und Leistungsbezieher, führt.
Mit Nachdruck wenden sich die Datenschutzbeauftragten gegen Versuche von Sozialverwaltungen, bei der Umsetzung der neuen Kontrollregelungen durch extensive Interpretation über den gesetzlich vorgegebenen Rahmen hinauszugehen. So erlaubt beispielsweise der neu gefaßte § 117 Abs. 3 des Bundessozialhilfegesetzes entgegen der

[1] gegen die Stimme Bayerns; Baden-Württemberg war in der Sitzung nicht vertreten, trägt den Beschluß jedoch inhaltlich mit.

Handhabung einzelner Kommunen keinen automatisierten Datenabgleich zwischen Sozialhilfedatei und Kraftfahrzeug-Register, sondern nur den Vergleich von Angaben in Verdachtsfällen.
Die dargestellte Entwicklung macht es erneut notwendig, auf die verfassungsrechtliche Qualität des Grundsatzes der Datenerhebung beim Betroffenen hinzuweisen. An dem Prinzip, daß bei der Überprüfung der Leistungsberechtigung und der Nachweise Auskünfte zunächst beim Antragsteller anzufordern sind und nur aufgrund konkreter Verdachtsmomente Nachfragen bei dritten Stellen oder Datenabgleiche erfolgen dürfen, muß für den Regelfall festgehalten werden, soll der einzelne mündige Bürger bleiben und nicht zum bloßen Objekt staatlicher Verhaltenskontrolle werden.
Sorge äußert die Konferenz auch über die hartnäckigen Bestrebungen, Datenbestände der Sozialverwaltung für immer neue Zwecke und Adressaten zu öffnen. Beispiele dafür sind die im Gesetzgebungsverfahren zum 2. SGB-Änderungsgesetz im letzten Augenblick gescheiterten Anträge, Polizei und Staatsschutz in unvertretbarem Umfang Zugriff auf Daten Arbeitsloser und sonstiger Sozialleistungsempfänger zu geben. Das Sozialgeheimnis muß ein wirksamer Sonderschutz für die besonders sensiblen Daten in der Sozialverwaltung bleiben. Nur dies entspricht der Abhängigkeit des einzelnen von staatlichen Leistungen und der sich daraus ergebenden speziellen Verletzlichkeit seines Rechts auf informationelle Selbstbestimmung.

16.2.8 Entschließung der 47. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 09./10. März 1994 in Potsdam zum Gesetzentwurf der Bundesregierung zur Neuordnung des Postwesens und der Telekommunikation[1] (Postneuordnungsgesetz - PTNeuOG, BR-Drs. 115/94 = BT-Drs. 12/6718) und zu der dafür erforderlichen Änderung des Grundgesetzes (BR-Drs. 114/94 = BT-Drs. 12/6717)

I.
Die Datenschutzbeauftragten des Bundes und der Länder weisen darauf hin, daß mit der Umwandlung der Deutschen Bundespost POSTDIENST in die Deutsche Post AG und der Deutschen Bundespost TELEKOM in die Deutsche Telekom AG zwei staatliche Einrichtungen aufhören zu existieren, gegenüber denen sich der Bürger bisher unmittelbar auf das Post- und Fernmeldegeheimnis berufen kann. Sie treten deshalb dafür ein, in der Verfassung sicherzustellen, daß jeder, der Post- und Fernmeldedienstleistungen erbringt, das Post- und Fernmeldegeheimnis zu wahren hat.

II.
Im Gesetz zur Neuordnung des Postwesens und der Telekommunikation ist ein den Vorgaben des Bundesverfassungsgerichts in seinem Volkszählungsurteil vom 15. Dezember 1983 und in seinem Fangschaltungsbeschluß vom 25. März 1992 entsprechender Schutz von Individualrechten zu gewährleisten. Die Datenschutzbeauftragten halten insbesondere folgende Änderungen des Gesetzentwurfs für erforderlich:

[1] Baden-Württemberg war in der Sitzung nicht, Sachsen bei der Beschlußfassung nicht mehr vertreten; beide tragen den Beschluß jedoch inhaltlich mit.

a) Der Umfang der zulässigen Verarbeitung personenbezogener Daten im Post- und Telekommunikationswesen ist im Gesetz selbst festzulegen; lediglich deren konkrete Ausgestaltung kann der Regelung durch Rechtsverordnungen überlassen bleiben.

b) Die Gewährleistung des Datenschutzes und des Post- und Fernmeldegeheimnisses muß in den Katalog der Ziele der Regulierung aufgenommen werden.

c) Das Post- und Telekommunikationswesen muß auf Dauer - auch nach dem Wegfall der Monopole - einer effektiven, unabhängigen datenschutzrechtlichen Kontrolle von Amts wegen nach bundesweit einheitlichen Kritierien unterworfen bleiben, auch soweit personenbezogene Daten nicht in Dateien verarbeitet werden.

d) Die Frist für die Speicherung von Verbindungsdaten zur Ermittlung und zum Nachweis der Entgelte ist präzise festzulegen.

e) Die vorgesehene Vorschrift zum Einzelentgeltnachweis schränkt den Kreis der Einrichtungen, die Telefonberatung durchführen und die nicht auf Einzelentgeltnachweisen erscheinen sollen, in unakzeptabler Weise ein. Dem Schutz des informationellen Selbstbestimmungsrechtes und des Fernmeldegeheimnisses der Angerufenen würde es dagegen am ehesten entsprechen, wenn jeder inländische Anschlußinhaber selbst entscheiden kann, ob und gegebenenfalls wie seine Rufnummer auf Einzelentgeltnachweisen erscheinen soll. Damit wäre auch die Anonymität von Anrufen bei Beratungseinrichtungen unbürokratisch sicherzustellen. Ein entsprechendes Verfahren wird in den Niederlanden bereits praktiziert.

f) Es wäre völlig unangemessen, wenn in Zukunft erlaubt würde, daß die Telekommunikationsunternehmen Nachrichteninhalte über die Befugnisse des § 14 a Fernmeldeanlagengesetz hinaus auch für die Unterbindung von Leistungserschleichungen und sonstiger rechtswidriger Inanspruchnahme des Telekommunikationsnetzes und seiner Einrichtungen sowie von Telekommunikations- und Informationsdienstleistungen erheben, verarbeiten und nutzen dürften.

III.

Die Datenschutzbeauftragten betonen, daß angesichts der neuen technischen Möglichkeiten digitaler Kommunikations- und Informationsdienste und der mit ihrer Nutzung zwangsläufig verbundenen Datenverarbeitung eine grundlegende Überarbeitung des § 12 Fernmeldeanlagengesetz, der die Weitergabe vorhandener Telekommunikationsdaten in Strafverfahren erlaubt, überfällig ist. Sie erinnern an die Umsetzung der entsprechenden Entschließung des Bundesrates vom 27. August 1991 (BR-Drs. 416/91).

16.2.9 Beschluß der 47. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 09./10. März 1994 in Potsdam zum Ausländerzentralregistergesetz[1]

Das Ausländerzentralregister beim Bundesverwaltungsamt in Köln existiert seit 40 Jahren

[1] gegen die Stimme Bayerns; Baden-Württemberg war in der Sitzung nicht vertreten, trägt den Beschluß jedoch inhaltlich mit.

ohne gesetzliche Grundlage. Derzeit stehen den verschiedenen Benutzern des Registers Daten zu mindestens 8 Millionen Ausländern, die sich in der Bundesrepublik aufhalten oder aufgehalten haben, zur Verfügung. Gespeichert sind neben Daten zur Identifizierung und weiteren Beschreibung der Person insbesondere Angaben zum Meldestatus, Aufenthaltsrecht und Asylverfahren.

Die Datenschutzbeauftragten des Bundes und der Länder haben immer wieder darauf hingewiesen, daß die Führung eines derartigen Registers ohne gesetzliche Regelung mit dem vom Grundgesetz Deutschen wie Ausländern gleichermaßen garantierten Recht auf informationelle Selbstbestimmung unvereinbar ist. Sie begrüßen daher, daß mit dem am 02. März 1994 vom Bundeskabinett beschlossenen Entwurf für ein Ausländerzentralregistergesetz eine gesetzliche Grundlage geschaffen werden soll.

Zwar enthält dieser Gesetzentwurf gegenüber früheren Entwürfen eine Reihe datenschutzrechtlicher Verbesserungen, Bedenken bestehen jedoch weiterhin: Die Datenschutzbeauftragten wenden sich insbesondere dagegen, daß das Ausländerzentralregister nicht nur als Informations- und Kommunikationssystem für die mit der Durchführung ausländer- und asylrechtlicher Vorschriften betrauten Behörden dienen, sondern darüber hinaus als Informationsverbund für Aufgaben der Polizei, Strafverfolgungsorgane und Nachrichtendienste zur Verfügung stehen soll.

Die Funktionserweiterung wird deutlich durch die Speicherung von Erkenntnissen der Sicherheitsbehörden zu Ausländern in das Register. So soll der INPOL-Fahndungsbestand des BKA, soweit er Ausschreibungen zur Festnahme und zur Aufenthaltsermittlung von Ausländern enthält, in das Ausländerzentralregister übernommen werden. Gleiches gilt für die vorgesehene Speicherung von Angaben zu Personen, bei denen Anhaltspunkte für den Verdacht bestehten, daß sie im einzelnen bezeichnete Straftaten planen, begehen oder begangen haben. Diese Informationen dienen nicht einem Informationsbedarf zur Erfüllung ausländerbehördlicher Aufgaben, sondern - worauf die Entwurfsbegründung hinweist - der Kriminalitätsbekämpfung. Für diese Zwecke stehen den Sicherheitsbehörden aber eigene Informationssysteme zur Verfügung. Nach Auffassung der Datenschutzbeauftragten dürfen deshalb derartige Erkenntnisse nicht in das Register aufgenommen werden.

Die im Entwurf vorgesehenen Voraussetzungen unter denen u.a. für Polizeibehörden, Staatsanwaltschaften und Nachrichtendienste automatisierte Abrufverfahren eingerichtet werden können, stellen keine wirksamen Vorkehrungen für eine Begrenzung der Abrufe dar. Besonders problematisch ist der geplante automatisierte Zugriff durch die Nachrichtendienste auf einen - wenn auch reduzierten - Datensatz. Für die Dienste ist in den jeweiligen bereichsspezifischen Gesetzen der automatisierte Abruf aus anderen Datenbeständen ausgeschlossen. Die Erforderlichkeit derartiger Abrufe ist in keiner Weise belegt. Die Datenschutzbeauftragten sprechen sich deshalb dafür aus, zumindest auf den automatisierten Abruf durch Nachrichtendienste zu verzichten.

16.2.10 Entschließung der 47. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 09./10. März 1994 in Potsdam zur Informationsverarbeitung im Strafverfahren[1]

Die Datenschutzbeauftragten des Bundes und der Länder erinnern an ihre Vorschläge zu gesetzlichen Regelungen der Informationsverarbeitung im Strafverfahren, die sie seit 1981 unterbreitet haben.

Während die Befugnisse von Polizei und Staatsanwaltschaft zur Datenerhebung bei Ermittlungen mittlerweile in weitreichender Form gesetzlich abgesichert wurden, fehlen weiterhin Regelungen in der Strafprozeßordnung, wie die erhobenen Daten in Akten und Dateien weiter verarbeitet werden dürfen.

Die Datenschutzbeauftragten des Bundes und der Länder halten die Beachtung folgender Grundsätze für notwendig, die in den Entwürfen des Bundes (Art. 4 §§ 474 ff. StPO des Entwurfs für ein Verbrechensbekämpfungsgesetz - BT-Drucksache 12/6853) und der Länder (Entwurf eines Strafverfahrensänderungsgesetzes 1994 des Strafrechtsausschusses der Justizministerkonferenz) nicht ausreichend berücksichtigt sind:

1. Strafrechtliche Ermittungsakten enthalten eine Vielzahl höchstsensibler Daten insbesondere auch über Opfer von Straftaten und Zeugen, die deshalb eines wirksamen Schutzes bedürfen. Es würde den Besonderheiten der im Strafverfahren - auch mit Zwangsmitteln - erhobenen Daten nicht entsprechen, wenn Strafakten als Informationsquelle für jegliche Zwecke anderer Behörden oder von nicht am Strafverfahren Beteiligten dienten. Die einzelnen Zwecke und die zugriffsberechtigten Stellen sind daher abschließend normenklar festzulegen.

1.1 Ingesamt ist sicherzustellen, daß der in anderen Zweigen der öffentlichen Verwaltung verbindlich geltende Standard des Datenschutzes für Übermittlungen keinesfalls unterschritten wird.

1.2 Soweit ein unabweisbarer Bedarf anderer Stellen an Informationen aus Strafverfahren besteht, ist er in erster Linie durch Erteilung von Auskünften zu befriedigen. Akteneinsichtnahmen oder Aktenübersendungen können erst dann zugelassen werden, wenn eine Auskunftserteilung nicht ausreicht. Nicht erforderliche Aktenteile müssen ausgesondert werden. An Privatpersonen dürfen Informationen aus strafrechtlichen Ermittlungen nur weitergegeben werden, wenn deren rechtliche Interessen davon abhängen.

2. Bei Regelungen zur dateimäßigen Speicherung ist zu unterscheiden zwischen Systemen zur Vorgangsverwaltung (wie z. B. zentrale Namensdateien) und Dateien, die der Unterstützung strafprozessualer Ermittlungen dienen (z. B. Spurendokumentations- und Recherchesysteme).

2.1 Der Datensatz zur Vorgangsverwaltung ist auf die Angaben zu beschränken, die zum Auffinden der Akten und zur Information über den Verfahrensstand erforderlich sind. Daten über Personen, die keine Beschuldigten sind, dürfen nur dann erfaßt werden,

[1] bei Stimmenthaltung Bayerns; Baden-Württemberg war in der Sitzung nicht vertreten, trägt den Beschluß jedoch inhaltlich mit.

wenn dies zur Vorgangsverwaltung zwingend erforderlich ist. In diesen Fällen bedarf es besonderer Zugriffs- und Verwendungsbeschränkungen.

In jedem Fall sind die Daten entsprechend dem Verfahrensstand zu aktualisieren. Vom Gesetzgeber sind konkrete Löschungsfristen vorzusehen. Die Speicherung ist längstens auf den Zeitpunkt zu begrenzen, für den die Akte aufbewahrt wird. Vorgangsverwaltungssysteme können so auch für eine wirksame Kontrolle der Aufbewahrungsfristen genutzt werden.

2.2 Die Staatsanwaltschaft kann sich zur Verwaltung ihres konventionell gespeicherten Datenmaterials grundsätzlich eines behördeninternen, automatisierten Nachweissystems bedienen. Länderübergreifende automatisierte Informationssysteme dürfen in Beachtung des Erforderlichkeitsprinzips demgegenüber allenfalls für solche Vorgänge errichtet werden, bei denen bestimmte Tatsachen die Prognose begründen, daß auf die erfaßten Daten zur Erfüllung durch Rechtsnorm zugewiesener Aufgaben (erneut) zugegegriffen werden muß.

Eine solche Prognose wird in der Regel dann nicht gerechtfertigt sein, wenn das zugrundeliegende Verfahren mit einer Einstellung nach § 170 Abs. 2 StPO oder einem rechtskräftigen Freispruch abgeschlossen worden ist, sofern nicht auch nach Abschluß des Verfahrens noch tatsächliche Anhaltspunkte dafür vorliegen, daß der Beschuldigte eine strafbare Handlung begangen hat. Eine Bereitstellung von Daten jedenfalls zu Zwecken der Strafverfolgung wird ferner grundsätzlich dann nicht in Betracht kommen, wenn die Ermittlungen konkrete Anhaltspunkte dafür bieten, daß der Beschuldigte nicht erneut strafbare Handlungen begehen wird. Dies kann z. B. bei Fahrlässigkeitstaten der Fall sein. Bei laufenden Verfahren kann die Zulässigkeit der Aufnahme von Daten im Hinblick auf die Möglichkeiten einer Verbindung von Verfahren, die Einstellung nach § 154 StPO oder die Gesamtstrafenbildung gegeben sein.

2.3 Für einen Informationsverbund zwischen verschiedenen speichernden Staatsanwaltschaften mit der Möglichkeit eines Direktzugriffs auf die Daten der jeweils anderen Behörden ergibt sich als Voraussetzung, daß die Weitergabe aller dem Zugriff unterliegenden Daten zumindest bei abstrakter Betrachtung zur Erfüllung durch Rechtsnorm zugewiesener Aufgaben der übermittelnden oder der zugriffsberechtigten Stellen geeignet und angemessen sein muß.

Für den Bereich der Strafverfolgung gilt ein umfassendes Aufklärungsgebot (§§ 152 Abs. 2, 160 StPO). Die Staatsanwaltschaft kann im Rahmen ihrer Ermittlungen grundsätzlich ohne Rücksicht auf das Gewicht des Tatvorwurfs von allen öffentlichen Behörden - also auch von anderen Staatsanwaltschaften - Auskunft verlangen (§ 161 Satz 1 StPO). Diese Auskunftspflicht besteht über das Ermittlungsverfahren hinaus bis zum Abschluß des Strafverfahrens. Daten, die im Falle einer entsprechenden Anfrage zu mit einem Strafverfahren zusammenhängenden Zwecken offenbart werden müßten, können damit - ungeachtet der besonderen Voraussetzungen für die Errichtung eines Direktabrufverfahrens - von jeder Staatsanwaltschaft für andere Staatsanwaltschaften grundsätzlich auch in einem Informationssystem mit Direktabrufmöglichkeit bereitgestellt werden, sofern nur bestimmte Tatsachen die Annahme rechtfertigen, daß die Daten in einem Verfahren einer anderen Behörde verwertet werden müssen. Eine solche Annahme wird regelmäßig wiederum in den unter 2.2 dargestellten Fällen nicht zu

begründen sein. Eine Bereitstellung von Daten wird darüber hinaus auch dann nicht erfolgen können, wenn diese einem besonderen Amtsgeheimnis unterliegen und deshalb auch auf Anforderung nicht ohne weiteres übermittelt werden dürften. Auf § 78 SGB X ist in diesem Zusammenhang hinzuweisen. Ein Direktabruf durch andere Stellen als Staatsanwaltschaften ist schon nach der Zweckbestimmung des Systems ausgeschlossen.

2.4 In der Praxis dienen derzeit die bestehenden polizeilichen Informationssysteme auch den Zwecken der Strafverfolgung. Eine Abstimmung der polizeilichen und der staatsanwaltschaftlichen Informationssysteme ist geboten. Eine weitere Abstimmung wird im Hinblick auf das Bundeszentralregister zu erfolgen haben, das ebenfalls Daten zu Zwecken der Strafverfolgung, aber auch der Strafvollstreckung speichert.

Die Datenschutzbeauftragten halten daher eine grundlegende Überarbeitung dieser Entwürfe für notwendig und bieten hierfür ihre Unterstützung an (vgl. Beschlüsse der Datenschutzkonferenzen vom 28./29. September 1981 zu "Mindestanforderungen für den Datenschutz bei den Zentralen Namenskarteien der Staatsanwaltschaften", vom 24./25. November 1986 "Überlegungen zu Regelungen der Informationsverarbeitung im Strafverfahren" und vom 05./06. April 1989 zum Entwurf eines Gesetzes zur Änderung und Ergänzung des Strafverfahrensrechts vom 03. November 1988).

16.3 Sonstiges

16.3.1 Zur Auswertung von nach § 35 Abs. 2 SächsDSG dem Sächsischen Datenschutzbeauftragten gemeldeten Altdatenbestands-Verzeichnissen

§ 35 Abs. 2 S. 1 SächsDSG verpflichtet jeden Inhaber personenbezogener Datenbestände, die während des Bestehens der DDR im Bereich von Staat, volkseigener Wirtschaft und gesellschaftlichen Organisationen auf dem Gebiet des heutigen Freistaates Sachsen zustandegekommen sind, dem SächsDSB ein Verzeichnis dieser Datenbestände zur Auswertung zuzuleiten. Mit seiner Bekanntmachung vom 20. Februar 1992 (SächsABl. S. 211) hat der SächsDSB auf diese Pflicht hingewiesen und sie konkretisiert.

In den daraufhin eingegangenen *Meldungen* waren von den meldenden Stellen die Ausdrücke, mit denen der Inhalt eines sachlich zusammengehörenden Datenbestandes (in der Regel einer vorhandenen Schriftguteinheit) bezeichnet wurde - im folgenden "*Sachbegriffe*" oder "*Stichworte*" genannt -, frei zu wählen. Infolgedessen sind die verwendeten Sachbegriffe uneinheitlich und teilweise auch inhaltlich nicht so bestimmt, wie es wünschenswert wäre (Beispiel: "Umsiedlung"). Überhaupt sind die gemeldeten Bestandsverzeichnisse selbst nach Umfang, Klarheit und Differenziertheit von Stelle zu Stelle äußerst unterschiedlich: Vom lakonischen Ein-Blatt-Verzeichnis mit wenigen Sachbegriffen bis hin zu höchst detailliert gegliederten Übersichten, aufgefächert gegebenenfalls nach Ämtern, Abteilungen und Sachgebieten der meldenden Stelle.

Ich habe die Meldungen nicht nur in geordneter Weise gesammelt, sondern darüber hinaus auch *ausgewertet* und informationstechnisch *in einem Register erschlossen*.

Auszugehen war von den in den Meldungen verwendeten Stichworten. In Einzelfällen habe ich sehr unbestimmte Ausdrücke ("Schriftverkehr", "Lageberichte", "Protokolle") an Hand anderer in den Meldungen enthaltener Anhaltspunkte in inhaltlich bestimmtere Kennzeichnungen übergeführt, ansonsten die von der meldenden Stelle beziehungsweise Person verwendeten Sachbegriffe originalgetreu, allenfalls leicht standardisiert in das Register übernommen. Synonymitätsbeziehungen zwischen verschiedenen Stichworten (akteninhaltskennzeichnenden Ausdrücken) wurden durch Verweisungen berücksichtigt.

Dem Zweck des Registers entsprechend blieben solche Stichworte, die in nahezu allen Meldungen vorkommen (z. B. Personalakten) oder für bestimmte Arten von Stellen selbstverständlich sind (z. B. Steuer- oder Verstaatlichungsakten bei Finanzämtern, Krankenakten bei Krankenhäusern, Strafvollzugsakten bei Justizvollzugsanstalten), *unberücksichtigt.*
Bestände, die an für sie untypischen Standorten lagern, habe ich *ohne* die nachfolgenden Einschränkungen erfaßt.

Dem Zweck des § 35 SächsDSG entsprechend habe ich die Registrierung in zweierlei Hinsicht *eingeschränkt*:
Altdaten, die sich bereits in staatlichen Archiven befinden, blieben unberücksichtigt. Der Sicherungszweck des § 35 SächsDSG ist insoweit ja bereits erfüllt.
Von der Registrierung ausgenommen blieben ferner diejenigen Stichworte, welche für die mit ihnen gemeldeten Daten keinen *Persönlichkeitsbezug mit einem für die politischen Verhältnisse der DDR spezifischen Gehalt* erkennen ließen.

Mit der durch diese Auswahl bewirkten Einschränkung ermöglicht das Register einen Gesamtüberblick über die eingegangenen Meldungen. Es lassen sich z. B. auch Meldungsprofile gleichartiger Stellen anfertigen.
Zum anderen soll das Register Interessierten die Auffindung bestimmter einzelner Datenbestände erleichtern, die für die Aufarbeitung der DDR-Geschichte beziehungsweise für Verwaltungs- oder Gerichtsverfahren benötigt werden.

Das Register ist als zweiteilige Datenbank eingerichtet. Der eine Teil ("W") enthält die Meldungen der Wirtschaftsunternehmen, der andere ("Ö") diejenigen der öffentlichen Stellen, und zwar jeweils nach *Standorten* (W: ca. 40; Ö: ca. 400) und *Stichworten* (W: ca. 160; Ö: ca. 380).

Standorte sind die Stellen (oder Personen), welche die Datenbestände als in ihrer tatsächlichen Gewalt befindlich gemeldet haben: Also z. B. das Landratsamt Plauen, die kreisfreie Stadt Leipzig, die Polizeidirektion Grimma, die TU Dresden. Dabei sind die Standorte nach *Standorttypen* geordnet (nach der organisatorischen Form oder dem Fachgebiet, auf dem die Stellen tätig sind): Also z. B. Landratsämter, kirchliche Einrichtungen, Schulen/Schulämter, Wirtschaftsunternehmen.

Stichworte sind Kurzangaben über den Inhalt des Datenbestandes: Also z. B. "Ausreiseanträge", "Eigentumsverzicht", "NVA-Werbung". Stichworte sind nach Sachzusammenhang einem *Oberbegriff* (vgl. nachstehend Übersicht A) zugeordnet: Also z. B. "Republikflucht", "Reisegenehmigungen" u. a. zu "Ausreiseprobleme" oder "Vermögenseinzug", "Erbausschlagung" u. a. zu "Eigentumsfragen" (vgl. nachstehend

Übersicht B).

Im Register kann folgendermaßen recherchiert werden:

1. Vorgabe *eines Stichwortes* oder *Oberbegriffes* (letzteres wirkt wie die Eingabe sämtlicher ihm zugeordneter Einzel-Stichworte).
   Ausgabe der betreffenden *Standorte.*
   (Recherche *Was ist wo ?*).
2. Vorgabe *eines Standortes.*
   Ausgabe der betreffenden *Stichworte.*
   (Recherche *Wo ist was ?*).
3. Erstellung *tabellarischer Übersichten*.
   Vorgabe *eines oder mehrerer Stichworte* oder *Oberbegriffe* (Zeilen) sowie *Standorte* bzw.
   Standorttypen (Spalten).
   Ausgabe speziell aufbereiteter Übersichten.
   Dies ist aus Darstellungsgründen jeweils nur für eine begrenzte Anzahl gleichartiger *Standorte* möglich (Beispiel zu den zwei Oberbegriffen "Ausreiseprobleme" und "Eigentumsfragen" für kreisfreie Städte und Landratsämter in Übersicht C; im Unterschied zu Übersicht B enthalten die Teilübersichten C nur die von den in der Übersicht aufgeführten Stellen tatsächlich gemeldeten Stichworte).

(IT-Grundlage: PC / MS-DOS und Datenbanksystem FoxPro)

Übersicht A:

Liste der Stichwort-Oberbegriffe

Abteilung Inneres, allgemein
Anliegen, Beschwerden, Eingaben
Ausländerfragen
Ausreiseprobleme
Eigentumsfragen
Einreiseprobleme
Grenze, Sperrgebiet
Hochschulen
Kaderfragen
Kirchenprobleme
Medizinische Probleme
Paramilitärische Probleme
Parteien außer SED
Polizeiliche Vorgänge
Rechtsfragen
Rückkehrer und Zuzügler
SED-Akten
Volksvertreter
Vorbestrafte und Wiedereingliederung
Wahlen
Zivilverteidigung
Überwachung und Spitzelei

Übersicht B: (Teil 1)

Liste der Stichworte zum Oberbegriff »Ausreiseprobleme«

Abstandsnahmen
Aus-/Einreisen
Ausreise
Ausreise, Rücknahmen
Ausreise, Schülerunterlagen
Ausreise, illegal
Ausreiseablehnungen
Ausreiseakten, ständige Ausreise
Ausreiseakten, vernichtete
Ausreiseanträge
Ausreiseverfügungen, Erlaß von
Aussiedlung
Besuchsreisen nach der BRD und Westberlin
Gespräche mit Ausreisewilligen
NSW, Ausreise
Reiseanträge
Reisegenehmigungen
Reisen
Reisetätigkeit
Republikflucht
Republikflüchtige, Neuvergabe der Wohnung
Umsiedler
Umsiedlung
Verzugsakten
Wohnsitzänderung ins Ausland (außer BRD)
Übergesiedelte, Berichte über
Übersiedlungen nach der BRD
Übersiedlungsakten

Übersicht B: (Teil 2)

Liste der Stichworte zum Oberbegriff »Eigentumsfragen«

Apothekenverstaatlichung
Beschlagnahmungen
Beschlagnahmungen durch Sowjetarmee
Bodenflächen, Nutzung von
Bodenreformangelegenheiten
Bodenreformverzichte
Devisen
Eigenheime
Eigenheime und 2-Familien-Häuser, Verkauf v.
Eigentum
Eigentumsverzicht
Enteignung
Enteignung von Kriegs- und Naziverbrechern
Entschädigung
Erbausschlagung
Erbgut
Flurstücke
Grundbuchakten
Grundbuchumschreibungen
Grundstücke von BRD-Bürgern
Grundstücke, Nutzungsrechte
Grundstücke, Rechtsträger
Grundstücksangelegenheiten
Grundstückspreise
Grundstücksverkehr
Grundstücksverträge, landwirtschaftliche
Inanspruchnahmen
Kataster
Konten, staatlich verwaltet
LPG, Werbung für
Liegenschaften
Mietverträge
Nachlässe
Nachlässe, erbenlose
Nutzungsrechte
Nutzungsverträge, landwirtschaftliche
Pacht- und Kaufverträge
Pflichtablieferung
Landwirtschaft
Raub, Vergewaltigungen durch Sowjetarmee
Rechtsträger
Schenkungen und Überlassungen
Staatliches Eigentum
Treuhänderische Verwaltung
Umwandlungen
Umzugs- und Erbgut
Valutagenehmigungen
Vermögen
Vermögen Ausgereister
Vermögen, Verwaltung von
Vermögenseinzug
Vermögenseinzug, 17. Juni 1953
Vermögensrechtliche Angelegenheiten
Verstaatlichung
Verzichte
Verzichtserklärungen
Volkseigentum, Überführung in
Wismut-Akten
Wohnungen und Gebäude
Zwangsaussiedlungen, -umsiedlungen
Zwangsverpachtung
Zwangsversteigerungen

Übersicht C: (Teil 1)
Stadtverwaltungen kreisfreier Städte

C	GR	PL		<--- Zur Kennzeichnung der kreisfreien Städte dienen die jeweiligen Kfz-Kennzeichen
	DD	L	Z	
	*			Aus-/Einreisen
*		*	*	Ausreise
		*		Ausreise, illegal
*	*	*	*	Ausreiseanträge
*				Aussiedlung
*			*	Beschlagnahmungen
*			*	Besuchsreisen nach der BRD und Westberlin
			*	Bodenreformangelegenheiten
			*	Eigenheime
				Eigentumsverzicht
			*	Enteignung
		*		Enteignung von Kriegs- und Naziverbrechern
				Erbausschlagung
		*		Flurstücke
				Gespräche mit Ausreisewilligen
*			*	Grundstücksangelegenheiten
*				Grundstücksverkehr
				Inanspruchnahmen
		*		Konten, staatlich verwaltet
				Liegenschaften
			*	Mietverträge
*			*	Nachlässe
			*	Nutzungsrechte
			*	Nutzungsverträge, landwirtschaftliche
			*	Pacht- und Kaufverträge
		*	*	Rechtsträger
		*	*	Reiseanträge
	*		*	Reisen
			*	Reisetätigkeit
			*	Republikflucht
				Schenkungen und Überlassungen
		*	*	Staatliches Eigentum
*			*	Treuhänderische Verwaltung
				Umwandlungen
			*	Umzugs- und Erbgut
		*	*	Vermögen, Verwaltung von
		*	*	Vermögenseinzug
*				Vermögensrechtliche Angelegenheiten
*	*	*	*	Wohnungen und Gebäude
			*	Zwangsversteigerungen
	*	*		Übersiedlungen nach der BRD
*				Übersiedlungsakten

Übersicht C: (Teil 2)
Landratsämter im Regierungsbezirk Chemnitz

AE	ANA	AU	BED	C	FG	FLÖ	GC	HC	HOT	KLI	MAB	OEL	PL	RC	RL	STL	SZB	WDA	Z	ZP	Zur Kennzeichnung der Landratsämter <-- dienen die jeweiligen Kfz-Kennzeichen (außer bei KLIngenthal und OELsnitz/V.)
								*								*	*				Aus-/Einreisen
	*	*		*		*		*		*		*	*	*		*	*		*	*	Ausreise
		*		*	*											*	*				Ausreise, illegal
		*																			Ausreise, Rücknahmen
	*																				Ausreiseakten, ständige Ausreise
	*	*		*	*		*	*	*							*	*		*		Ausreiseanträge
		*			*				*							*					Beschlagnahmungen
									*												Beschlagnahmungen durch Sowjetarmee
		*																			Bodenflächen, Nutzung von
		*			*			*		*	*			*		*	*		*	*	Bodenreformangelegenheiten
													*								Eigenheime
														*			*				Eigentum
				*					*				*								Eigentumsverzicht
		*			*				*								*				Enteignung
				*													*				Entschädigung
				*																	Erbausschlagung
				*																	Gespräche mit Ausreisewilligen
				*																	Grundstücke, Nutzungsrechte
				*																	Grundstücke, Rechtsträger
				*	*				*				*				*				Grundstücksangelegenheiten
				*									*								Grundstücksverkehr
								*					*								Grundstücksverträge, landwirtschaftl.
					*																Inanspruchnahmen
				*					*												Konten, staatlich verwaltet
									*												Liegenschaften
													*								LPG, Werbung für
				*																	Nachlässe
																	*				NSW, Ausreise
				*					*				*	*				*			Nutzungsrechte
								*	*	*			*	*				*	*		Pacht- und Kaufverträge
		*															*				Pfändungen
				*					*				*				*				Rechtsträger
	*	*		*				*					*				*				Reiseanträge
								*													Reisegenehmigungen
		*		*				*					*	*			*	*			Republikflucht
																	*				Schenkungen und Überlassungen
				*				*		*			*								Staatliches Eigentum
									*				*				*				Treuhänderische Verwaltung
	*	*			*	*			*				*				*	*		*	Umsiedler
		*																			Umsiedlung
	*																				Umwandlungen
		*						*					*				*				Umzugs- und Erbgut
				*																	Valutagenehmigungen
				*				*					*								Vermögen Ausgereister
				*				*										*			Vermögen, Verwaltung von
								*					*				*				Vermögenseinzug
	*																				Verstaatlichung
								*													Verzichtserklärungen
				*																	Verzugsakten
													*								Zwangsaussiedlungen, -umsiedlungen
														*							Zwangsverpachtung
		*			*				*												Übersiedlungen nach der BRD
				*	*								*				*				Übersiedlungsakten

Übersicht C: (Teil 3)
Landratsämter im Regierungsbezirk Dresden

BIW / BZ / DD	DW / FTL / GR	GRH / HY / KM	LÖB / MEI / NY	PIR / RIE / SEB	WSW / ZI	<--- Zur Kennzeichnung der Landratsämter dienen die jeweiligen Kfz-Kennzeichen
				*		Abstandsnahmen
	*				*	Aus-/Einreisen
* *	* *	* * *	* *	* *	*	Ausreise
				*	*	Ausreise, illegal
			*			Ausreiseakten, vernichtete
* *	*	* *	* *	*	*	Ausreiseanträge
			*			Beschlagnahmungen
	*					Besuchsreisen nach der BRD und Westberlin
*			* * *		*	Bodenreformangelegenheiten
*						Bodenreformverzichte
			*			Eigenheime
*						Eigenheime und 2-Familien-Häuser, Verkauf
* *			*			Eigentumsverzicht
*		*		*	*	Enteignung
*						Erbausschlagung
		*				Erbgut
			*			Flurstücke
			*		*	Gespräche mit Ausreisewilligen
		*				Grundbuchakten
		*	*			Grundbuchumschreibungen
*						Grundstücke, Nutzungsrechte
*						Grundstücke, Rechtsträger
		* *		*		Grundstücksangelegenheiten
		*				Grundstückspreise
*		* *			*	Grundstücksverkehr
*					*	Grundstücksverträge, landwirtschaftliche
*			*			Inanspruchnahmen
*						Konten, staatlich verwaltet
*			*			Nachlässe, erbenlose
*		*	*			Nutzungsrechte
*			*		*	Nutzungsverträge, landwirtschaftliche
*	*	* *	*		*	Pacht- und Kaufverträge
					*	Pflichtablieferung, Landwirtschaft
*		*				Rechtsträger
			*			Reisen
			*			Republikflucht
					*	Republikflüchtige, Neuvergabe der Wohnung
			*			Schenkungen und Überlassungen
*						Staatliches Eigentum
* *		*	*			Treuhänderische Verwaltung
*			*			Umsiedler
					*	Umzugs- und Erbgut
	*	*				Vermögen
			*			Vermögen Ausgereister
*					*	Vermögen, Verwaltung von
			*			Vermögenseinzug, 17. Juni 1953
			*			Verstaatlichung
			*			Verzichte
			*			Volkseigentum, Überführung in
		*				Wohnsitzänderung ins Ausland (außer BRD)
*						Übersiedlungen nach der BRD
	*	*	* * *	*	*	Übersiedlungsakten

Übersicht C: (Teil 4)
Landratsämter im Regierungsbezirk Leipzig

BNA	DL	DZ	EB	GHA	GRM	L	OZ	TG	WUR	<--- Zur Kennzeichnung der Landratsämter dienen die jeweiligen Kfz-Kennzeichen
									*	Aus-/Einreisen
*	*	*		*	*	*			*	Ausreise
		*								Ausreise, illegal
									*	Ausreiseablehnungen
*	*			*		*	*		*	Ausreiseanträge
	*									Ausreiseverfügungen, Erlaß von
		*								Aussiedlung
									*	Beschlagnahmungen
									*	Beschlagnahmungen durch Sowjetarmee
	*	*							*	Bodenreformangelegenheiten
					*				*	Eigentum
									*	Eigentumsverzicht
		*							*	Enteignung
									*	Erbausschlagung
									*	Gespräche mit Ausreisewilligen
									*	Grundbuchumschreibungen
*										Grundstücksangelegenheiten
									*	Konten, staatlich verwaltet
*	*			*						Pacht- und Kaufverträge
									*	Raub, Vergewaltigungen durch Sowjetarmee
									*	Reiseanträge
*									*	Republikflucht
	*								*	Staatliches Eigentum
*										Treuhänderische Verwaltung
*									*	Umsiedler
				*						Vermögensrechtliche Angelegenheiten
									*	Wohnungen und Gebäude
							*			Übersiedlungsakten

16.3.2 Gefahren und Risiken beim Telefonieren, insbesondere mit dem Mobiltelefon

Mobiltelefone sind begehrt wie nie zuvor. Man will überall erreichbar sein, von überall anrufen können, frei beweglich und nicht wie bisher an die Telefonschnur "gebunden" sein. Die Zahl der neuen Kunden für die modernen D-Netze erreichte allein im Dezember 1993 die Rekordhöhe von 120 000. Insgesamt wurden im vergangenen Jahr für die D-Netze 360 000 neue Telefonkunden gewonnen. Darüber hinaus gibt es für das ältere C-Netz über 800 000 Teilnehmer (die Fachbegriffe wie C- und D-Netz werden weiter unten erklärt). 1996 wird mit bis zu 3 Mio Teilnehmern gerechnet.

Im Unterschied zu anderen Wirtschaftsbereichen verzeichnen mobile *Telefondienste* starken Zuwachs. Ganz abgesehen von den Kosten des Mobilfunks für die Nutzer ist dieses neue Angebot für manche aber auch verwirrend und beunruhigend. Die Anbieter informieren nur unzureichend über Probleme und Risiken des Mobilfunks.

Gefahren für das Fernmeldegeheimnis
Neben Vorteilen sind mit dieser neuen Kommunikationstechnik auch *Nachteile und Risiken* verbunden, beispielsweise für die Vertraulichkeit des Telefongesprächs, die zu Recht jeder Nutzer eines Telefons erwartet. Unter dem Schutz des Grundgesetzes stehen nicht nur der Inhalt des geführten Telefongespräches, sondern auch die näheren Umstände des Fernmeldeverhältnisses (z. B. die Telefonnummer des Anrufers und des Angerufenen, die Dauer des Gesprächs). Nach Art. 10 des Grundgesetzes ist das *Fernmeldegeheimnis* unverletzlich. Nur in gesetzlich vorgesehenen Ausnahmefällen sind Beschränkungen, meist auf richterlichen Beschluß, zugelassen (Gesetz zu Art. 10 GG, sogenanntes G10, SächsAG G10, §§ 100 a, 100 b StPO).

Kann man sich mit Hilfe der neuen mobilen Telefontechnik vertraulich unterhalten oder ist beim Gebrauch dieser Kommunikationstechnik das Fernmeldegeheimnis gefährdet? Besteht insoweit ein Unterschied zum traditionellen drahtgebundenen Telefonieren? Ist man beim mobilen Telefonieren davor geschützt, daß Unbefugte das private Gespräch zufällig mithören oder gezielt abhören? Wie soll man sich verhalten, wenn man ein vertrauliches Ferngespräch führen möchte?

Um diese Fragen beantworten zu können, muß auf einige physikalisch-technische Hintergründe der modernen Kommunikationstechnik eingegangen werden, denn die Abhörsicherheit hängt ab von den dabei benutzten physikalisch-technischen Verfahren:

Schnurloses Telefon: Der Handapparat ist ohne Kabel (Schnur) mit dem Grundgerät über Funk verbunden und ermöglicht ungehindertes Telefonieren im Nahbereich, z. B. im Haus oder aus dem Garten. Die Übertragung erfolgt analog. Die maximale Reichweite beträgt 300 m. Abhören ist ohne weiteres möglich. Ein Gebrauch ist daher für vertrauliche Gespräche riskant. (Zuweilen werden auch schnurlose Telefone von Anbietern irreführend als Funktelefone bezeichnet.)

Mobiltelefon: In einem größeren Bereich relativ frei bewegliches kabelloses Telefon, bei

dem die Übertragung drahtlos, also per Funk, erfolgt, daher auch *Funktelefon* genannt.

Handy: Sehr kompaktes Mobiltelefon im Taschenformat, das nur aus einem Handapparat mit kleiner Antenne besteht.

Mobiltelefonnetz: Gesamtheit von Übertragungsstationen, welche die Sprachübertragung über ein größeres Gebiet ermöglicht. Die beweglichen Stationen (*Mobilstationen*) sind per Funk mit - in der Regel ortsfesten - *Basisstationen* verbunden.

Arten von Mobiltelefonnetzen: Man unterscheidet heute die schon älteren *B-* und *C-Netze* sowie die moderneren *D1-, D2- und E-Plus-Netze* und als Typbezeichnung die *GSM-Netze*

B- und C-Netze: Die Übertragung erfolgt bei diesen (nationalen) Netzen mittels analoger Technik. Diese Netze sind relativ leicht abhörbar. Ein Gebrauch ist für vertrauliche Gespräche riskant. Das B-Netz wurde 1977 eingeführt, ist technisch überholt und läuft in der Anwendung aus. Das C-Netz ist für maximal 800 000 Teilnehmer ausgelegt.

D1- und D2-Netze ermöglichen ein drahtloses Telefonieren über Funk sogar über Landesgrenzen hinweg mittels digitaler Technik (wie sie im Computer benutzt wird) und sind relativ abhörsicher. Die Sprache wird für die Übertragung in Impulsfolgen umgewandelt. Vertrieben wird das D1-Netz von der Telekom der Deutschen Bundespost, das D2-Netz von der Firma Mannesmann.

E-Plus-Netz (kurz E1-Netz): Ein neues privates digitales Mobilfunknetz mehrerer um die Firma E-Plus Mobilfunk GmbH gruppiertes Unternehmen. Es soll ab 1994 in den neuen Bundesländern flächendeckend angeboten werden, beginnend in Ballungsgebieten. Relativ abhörsicher.

GSM-Netze sind nach der *GSM-Norm* für ein einheitliches europaweites digitales Funknetz benannt. Immer mehr Länder in Europa schließen sich dieser Norm an, so daß künftig auf dieser Grundlage mit digitalem Mobilfunk europaweit telefoniert werden können wird. Das D1-, D2- und E-Plus-Netz verwenden diese Form.

Bündelfunk mittels Checker-Netz, eine neue Alternative zu den früher in Lizenz betriebenen privaten Netze (z. B. privater Landfunk in der Ex-DDR); bestimmt für spezielle Nutzergruppen, z. B. Funktaxi. Ein abhörsicheres digitales Netz. Auch das "Einloggen" (wahlweise Zuschalten in das Netz) geschieht digital.

Die Aufzählung zeigt, daß hier nur *telefonartige* mobile Kommunikationstechnik betrachtet wird. Unberücksichtigt bleibt andere drahtgebundene oder drahtlose Technik, die *nicht* telefonartig ist. Dazu zählen z. B. Wechselsprechanlagen, wie die jetzt von Warenhäusern und Versandhäusern angebotenen "Babyüberwacher".

Abhören und Mithören - der Unterschied
Abhören geschieht zielgerichtet mit speziellen Abhörgeräten (z. B. mit sogenannten

Minispionen). Nach § 201 Abs. 2 StGB macht sich strafbar (Geldstrafe oder Freiheitsstrafe bis zu drei Jahren), wer unbefugt das private, also nicht öffentlich gesprochene, Wort mit einem Abhörgerät abhört. Ein zufälliges *Mithören* z. B. von Gesprächen des Wohnungsnachbarn, weil die Wände zu dünn sind oder ein Gespräch sich plötzlich "in der Leitung befindet", ist demzufolge *kein* Abhören. Auch das "Lauschen" an der Tür und Wand (mit dem Ohr) fällt nicht unter das Abhören (mit Abhörgeräten). Auf dieses Lauschen bezieht sich das Sprichwort "Der Lauscher an der Wand hört seine eigene Schand."

Mithörer

Bei einem Telefongespräch denkt man zunächst nur an den Partner, den man angerufen hat. Aber es sind auch andere, die von uns unbemerkt unser Gespräch "mitkriegen" können. Das kann zufällig oder absichtlich passieren, wie sich aus folgenden Beispielen ergibt:

Zufällig:

- Anwesende in der Nähe, die zufällig oder absichtlich im Raum oder nebenan zuhören und nicht "in der Leitung sind". Dazu zählt auch der neugierige Nachbar oder Mitarbeiter.
- Zufällige Teilnehmer von Gesprächen (Privatpersonen, Mitarbeiter von Unternehmen oder Behörden), weil sie durch technische Mängel des Telefonnetzes plötzlich zugeschaltet werden.
- Installations- und Wartungstechniker, die bei ihrer technischen Arbeit Gespräche "mitbekommen".
- Bastler und Unkundige, die unabsichtlich nicht-postzugelassene Geräte betreiben.

Absichtlich:

- Unbefugte, die sich bei modernen Telefonanlagen (ISDN-Anlagen) bewußt zuschalten.
- Mitarbeiter von Privatunternehmen, die aus Geschäftsinteresse den Sprechfunk oder das C-Netz abhören.
- Täter, die zur Vorbereitung von Straftaten oder zu dem Zweck, Verfolgungsmaßnahmen zu entgehen, abhören.

Zwar stellt § 201 StGB das Abhören unter Strafe, aber nicht jede Straftat wird angezeigt. Die Wahrscheinlichkeit des Mithörens oder Abhörens ist meist gering. Völlig ausschließen läßt es sich mit heutigen Mitteln nicht.

Technische Defekte und Risiken

Aus Alltagserfahrungen im Umgang mit der Technik weiß man, daß sie nie absolut fehlerlos ist. Auch beim Telefonieren kann es passieren, daß plötzlich ein anderes Gespräch mit in der Leitung ist und wir unbeabsichtigt sogenannte Nebengespräche hören. Diese Fehler entstehen insbesondere bei der alten *analogen* Vermittlungstechnik im Telefonnetz mit *elektromagnetischen* Schaltern, die jedoch jetzt zunehmend durch die moderne *digitale* Vermittlungstechnik (Computertechnik) ersetzt wird.

Was technisch übermittelt wird, kann auch technisch abgehört werden. Völlig mithör- und abhörsichere Technik kann es deshalb nicht geben, ebenso wie es ein völlig ausfallfreies Fahrzeug nie geben wird. *Mithören* und *Abhören* sind aus der Sicht des *Nutzers* eines Telefons solche *Defekte*. Durch modernere Kommunikationstechnik läßt sich das Risiko des Mithörens und Abhörens bei entsprechendem technischen Aufwand verringern, aber *prinzipiell nicht* ausschließen: Wer sich heute des technischen Mittels

Telefon bedient, riskiert dabei grundsätzlich, daß jemand mithört oder abhört.

Mit den Risiken der Kommunikationstechnik leben
In dieser Situation ist es das Vernünftigste, wenn sich jeder Teilnehmer am Telefonverkehr auf die *Risiken beim Telefonieren einstellt*. Ist das unvermeidliche *Restrisiko* beim drahtlosen Mobiltelefon kleiner oder größer als bei dem drahtgebundenen herkömmlichen Telefon? Muß man sich beim Gebrauch der modernen Mobiltechnik - wegen der Gefahren für die Vertraulichkeit des Gesprächs - mehr oder gar weniger in acht nehmen? Um diese Frage beantworten zu können, müssen die aufgrund der benutzten Techniken bestehenden Mithör- und Abhörrisiken näher betrachtet werden.

Risiken verschiedener Techniken
Die Übertragung des Gesprächs kann mittels *analoger* oder *digitaler* Technik geschehen. Bei analoger Technik werden mit dem Mikrofon die Schwingungen der Sprache in Schwankungen des elektrischen Stromes umgesetzt. Bei digitaler Technik, wie sie im Computer benutzt wird, werden die Schwingungen in einzelne Impulse (entsprechend der 0 oder 1 der digitalen Technik) verwandelt. Solche 0-1-Impulse können mit Computerschaltkreisen auch leicht weiter verarbeitet werden, z. B. zum Schutz des Fernmeldegeheimnisses verschlüsselt werden. Demzufolge läßt sich im allgemeinen ein digital übermitteltes Gespräch schwerer abhören als ein analog übermitteltes. Wenn also das bestehende Fernmeldenetz von herkömmlicher analoger Technik auf digitale Technik umgestellt wird, so wird damit im allgemeinen das Mit- und Abhörrisiko *verringert*.

Das gesprochene Wort kann - analog oder digital - entweder mit einer *Leitung* (herkömmlich Kupferdraht, neuerdings auch Glasfaser) oder über *Funk* mit elektromagnetischen Wellen übertragen werden. Wie wirkt sich der Unterschied auf das Abhör- und Mithörrisiko aus?

Wenn das Gespräch nur auf einer *Leitung* "transportiert" wird, dann ist die Möglichkeit, daß jemand unbefugt mithört oder abhört, wesentlich geringer, als wenn es durch einen "Sender" abgestrahlt wird. Nichts ist leichter, als ein Funksignal zu empfangen und auszuwerten. Dazu stellt man eine Antenne auf und nimmt ein geeignetes Empfangsgerät. Das funktioniert aber nur im *Empfangsbereich* des Gesprächssenders. Die Gesprächsübermittlung ist vergleichbar einem Gespräch über Lautsprecher vor aller Ohren. Seit dem 30.6.1992 ist das Risiko, daß mit- oder abgehört wird, stark gestiegen, weil seitdem Rundfunkempfänger betrieben werden dürfen, mit denen teilweise der analoge Funkverkehr, z. B. von Polizei oder Rettungsdiensten, abgehört werden kann.

Das Risiko des Mit- und Abhörens ist bei einer Funkübertragung mit nur kurzer *Reichweite* (im Nahbereich z. B. 300 m) wesentlich geringer als bei größerer Reichweite (beispielsweise in einem ganzen Land). Wenn eine Funkübertragung über Satellit gewählt wird, die in ganz Europa empfangen werden kann, so ist das Risiko für die Vertraulichkeit des persönlichen Gesprächs natürlich beträchtlich.

Ein *Vergleich* ergibt folgendes:

Die Gefährdung der Vertraulichkeit eines Gesprächs ist bei analoger Funkübertragung am *größten*; im *mittleren Bereich* liegt sie bei digitaler Funkübertragung oder analoger Drahtübertragung. Am geringsten ist die Gefährdung bei digitaler drahtgebundener, also modernisierter klassischer Übertragungstechnik.

Konkret bedeutet das:

Die *größte* Gefahr, daß jemand mithört oder abhört zu wird, läuft also derjenige, der ein schnurloses Telefon oder das B- oder C-Funknetz benutzt. Geringer ist das Risiko beim Mobiltelefon mit D1-, D2- oder E-Netz (sogenannte GSM-Netze) oder bei analoger drahtgebundener Übertragung. *Am geringsten* ist das Risiko bei digitaler drahtgebundener Technik, wie sie zunehmend bei der Modernisierung des Telefonnetzes installiert wird.

Aus diesen grundsätzlichen Feststellungen leiten sich sehr einfach praktische Regeln für den Umgang mit der Möglichkeit ab, mobile Telefone zu benutzen.

Entscheidend ist, *wie vertraulich* das gewünschte Gespräch sein soll. Wenn mehrere Möglichkeiten zum Telefonieren bestehen, dann muß der Betreffende im Hinblick auf die gewünschte Vertraulichkeit den für das Gespräch *geeignetesten* Kommunikationsweg wählen. Maßgebend sind die Schutzbedürftigkeit und der Wert des Inhalts und der Umstände des Gesprächs, also die möglichen Nachteile, falls Unbefugte das Gespräch mithören. Gespräche ohne jede Vertraulichkeit und Schutzwürdigkeit, wenn also das Risiko eines Schadens zu vernachlässigen ist, können natürlich mit jeder Kommunikationstechnik geführt werden.

Wer ein sehr vertrauliches Telefongespräch führen möchte, sollte dafür *kein Funktelefon* benutzen. Besonders riskant ist der Gebrauch *schnurloser Telefone,* die jetzt überall angeboten werden. Unverantwortlich wäre ein Gebrauch schnurloser Telefone in Bereichen, in denen naturgemäß vertrauliche Telefongespräche geführt werden, z. B. bei Behörden oder beim Arzt oder in einer Klinik. Wer das Bedürfnis hat, ein vertrauliches Ferngespräch per Telefon mit jemandem zu führen und neben sich (z. B. im Auto) ein C-Netztelefon stehen hat, sollte prüfen, ob er dieses Gespräch nicht besser von der nächsten drahtgebundenen öffentlichen Telefonzelle aus führt.

Die Umstellung auf abhörsichere digitale Telefonnetze ist nicht von heute auf morgen zu schaffen. Dort, wo das herkömmliche Telefonnetz erneuert oder ausgebaut wurde (vornehmlich in Großstädten), ist das Telefonieren abhörsicherer als in solchen Gegenden, in denen noch veraltete analoge Leitungs- und Vermittlungstechnik der 20er Jahre genutzt wird.

In einer *Entschließung der Konferenz der Datenschutzbeauftragten* des Bundes und der Länder vom 26./27.10.93 (abgedruckt unter 16.2.3) wird auf diese neuen, wenig bekannten Gefahren für die Datensicherheit beim Gebrauch von Funktelefonen hingewiesen. Hinzu kommt: Problematische sogenannte "Bewegungsprofile" lassen sich gewinnen, wenn der jeweilige Aufenthaltsort des Teilnehmers systematisch gespeichert und ausgewertet wird. Von Herstellern und Betreibern mobiler Telekommunikationstechniken fordere ich wirksame *Gegenmaßnahmen* und eine bessere

Information der Benutzer über den erreichten Datenschutz und dessen weiterhin bestehende Gefährdungen.

Sonstige Risiken
Mit dem Gebrauch von Funktelefonen und entsprechenden Funktelefonnetzen entstehen überdies auch noch *andere* Gefahren, die von den Anbietern und Herstellern teilweise nicht genügend deutlich gemacht werden.
Elektronische, insbesondere digitale Steuerungstechnik wird zunehmend im Alltag eingesetzt (elektronische Technik im Auto, im Flugzeug, aber auch in Hörgeräten, Herzschrittmachern, inplantierten Insulinpumpen, elektronischen Diagnose- und Therapiegeräten). Die elektromagnetische Abstrahlung von Funktelefonen in der Nähe kann unter Umständen zu unerwarteten Fehlfunktionen bei dieser Technik führen, in Ausnahmefällen mit fatalen Folgen (Lebensgefährdung).

Die Auswirkungen der elektromagnetischen *Funkstrahlung* beim Mobiltelefon (insbesondere bei sogenannten Handys, bei deren Gebrauch die Sendeantenne des Handgerätes direkt an den Kopf gehalten wird) auf den menschlichen Körper sind gegenwärtig noch *nicht ausreichend erforscht.* Durch die kombinierte elektromagnetische Strahlung aus vielen Quellen (Rundfunk, Fernsehen, Hochspannungsmasten, Funktelefonen) entsteht möglicherweise eine neue Art von Gesundheitsgefährdungen, die als *Elektrosmog* bezeichnet wird. Obwohl der Elektrosmog wahrscheinlich ungefährlicher ist als die von Autos und Industrie ausgehenden Luftschadstoffe und der Zigarettenrauch, sollte man den eigenen Körper vorsichtshalber soweit wie möglich von Abstrahlungsquellen, die sich *in der Nähe* befinden, fernhalten. Besonders empfindlich ist das *Auge* des Menschen.

Vorsicht ist geboten
Will man nicht auf die Vorteile und Annehmlichkeiten moderner elektronischer Medien und der Elektronik verzichten, was heute ja praktisch unmöglich ist, so bleibt nur noch übrig, sich nach der alten Regel "nicht so viel wie möglich, sondern nur so viel wie nötig" elektromagnetischer Strahlung auszusetzen.
Wer also auf sein bequemes Handy nicht verzichten möchte, sollte dieses Gerät bei Sendebetrieb nur dann an den Kopf (und die Antenne möglichst weit weg vom Auge) halten, wenn das für das Telefongespräch *erforderlich* ist, also z. B. nicht in Gesprächspausen oder beim Wählen.

Es gehört übrigens zu den Unsitten des Computergebrauchs, Bildschirme, die elektromagnetisch abstrahlen, laufen zu lassen, obwohl gar nicht an den Bildschirmen gearbeitet wird. Im Interesse einer Verringerung des elektromagnetischen Smogs wäre das Abschalten bei Nichtgebrauch angebracht.

Der Gebrauch einer Funktechnik, die in Ausnahmefällen möglicherweise bei einem Träger elektronischer Technik, (z. B. Herzschrittmachern, elektronische Insulinpumpe) fatale Folgen haben kann, erfordert sogar eine neue Art des Umgangs miteinander, ähnlich wie beim Rauchen. Es sollte zu einem rücksichtsvollen Umgang miteinander gehören, beispielsweise vor dem Gebrauch dieser möglicherweise gefahrenauslösenden Technik die Anwesenden zu fragen, ob *keine Einwände* gegen den Gebrauch bestehen. Eine Verordnung über die Vermeidung von Elektrosmog wäre angebracht.