Sächsischer Landtag
2. Wahlperiode

DRUCKSACHE 2/0930

Schutz des Persönlichkeitsrechts im öffentlichen Bereich

3. Tätigkeitsbericht

des

Sächsischen Datenschutzbeauftragten

Dem Sächsischen Landtag

vorgelegt zum 31. März 1995

gemäß § 27 des Sächsischen Datenschutzgesetzes

Eingegangen am: 7. April 1995

Ausgegeben am: 9. Mai 1995

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
Holländische Str. 2 Postfach 120905
01067 Dresden 01008 Dresden
Telefon: 0351/4935401
Fax : 0351/4935490

Vervielfältigung erwünscht.
Herstellung: OTTO Verlag und Druckerei OHG, 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.

AEAO	Anwendungserlaß zur Abgabenordnung
AgrStatG	Gesetz über Agrarstatistiken (Agrarstatistikgesetz) in der Fassung der Bekanntmachung vom 23. September 1992 (BGBl. I S. 1632)
AO	Abgabenordnung
AtG	Gesetz über die friedliche Verwendung der Kernenergie und den Schutz gegen ihre Gefahren (Atomgesetz) in der Fassung der Bekanntmachung vom 15. Juli 1985 (BGBl. I S. 1565), zuletzt geändert durch Art. 4 des Gesetzes zur Sicherung des Einsatzes von Steinkohle in der Verstromung und zur Änderung des Atomgesetzes und des Stromeinspeisungsgesetzes vom 19. Juli 1994 (BGBl. I S. 1618)
BAT(-O)	Erster Tarifvertrag zur Anpassung des Tarifrechts - Manteltarifliche Vorschriften (BAT-O) vom 10. Dezember 1990 (SächsABl. 1991 Nr. 10 S. 1)
BDSG	Gesetz zur Fortentwicklung der Datenverarbeitung und des Datenschutzes (Bundesdatenschutzgesetz)
BerRehaG	Gesetz über den Ausgleich beruflicher Benachteiligungen für Opfer politischer Verfolgung im Beitrittsgebiet (Berufliches Rehabilitierungsgesetz) vom 23. Juni 1994 (BGBl. I S.1311, 1314)
BewG	Bewertungsgesetz
BGB	Bürgerliches Gesetzbuch
BGySO	Verordnung des Sächsischen Staatsministeriums für Kultus über berufliche Gymnasien im Freistaat Sachsen (Schulordnung berufliche Gymnasien) vom 24. November 1993 (GVBl. S. 1185)
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), zuletzt geändert durch Art. 3 Abs. 2 des Gesetzes zur Neuordnung des Erfassungs- und Musterungsverfahrens vom 12. Juli 1994 (BGBl. I S. 1497)

BSHG	Bundessozialhilfegesetz in der Fassung der Bekanntmachung vom 10. Januar 1991 (BGBl. I S. 94, ber. S. 808), zuletzt geändert durch das Gesetz zur sozialen Absicherung der Pflegebedürftigkeit (Pflege-Versicherungsgesetz - PflegeVG) vom 26. Mai 1994 (BGBl. I S. 1014)
BSO	Verordnung des Sächsischen Staatsministeriums für Kultus über die Berufsschule im Freistaat Sachsen (Schulordnung Berufsschule) vom 11. März 1994 (GVBl. S. 477)
BStatG	Gesetz über die Statistik für Bundeszwecke (Bundesstatistikgesetz) vom 22. Januar 1987 (BGBl. I S. 462, 565), zuletzt geändert durch Art. 6 Abs. 36 des Gesetzes vom 27. Dezember 1993 (BGBl. I S. 2378)
BVerfSchG	Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz vom 20. Dezember 1990 (BGBl. I S. 2954), zuletzt geändert durch § 38 Abs. 2 des Sicherheitsüberprüfungsgesetzes vom 20. April 1994 (BGBl. I S. 867)
BVFG	Gesetz über die Angelegenheiten der Vertriebenen und Flüchtlinge (Bundesvertriebenengesetz) in der Fassung der Bekanntmachung vom 2. Juni 1993 (BGBl. I S. 829)
BZRG	Gesetz über das Zentralregister und das Erziehungsregister (Bundeszentralregistergesetz)
DA	Dienstanweisung für die Standesbeamten und ihre Aufsichtsbehörden vom 23. November 1987 (BAnz. Nr. 227 a), zuletzt geändert durch Änderungsverwaltungsvorschrift vom 31. März 1994 (BAnz. S. 3881)
EALG	Gesetz über die Entschädigung nach dem Gesetz zur Regelung offener Vermögensfragen und über staatliche Ausgleichsleistungen für Enteignungen auf besatzungsrechtlicher oder besatzungshoheitlicher Grundlage (Entschädigungs- und Ausgleichsleistungsgesetz) vom 27. September 1994 (BGBl. I S. 2624)
EGAB	Erstes Gesetz zur Abfallwirtschaft und zum Bodenschutz im Freistaat Sachsen vom 12. August 1991 (GVBl. S. 306)
Eigentumsübertragungsgesetz	Gesetz über die Übertragung des Eigentums und die Verpachtung volkseigener landwirtschaftlich genutzter Grundstücke an Genossenschaften, Genossenschaftsmitglieder und andere Bürger vom 22. Juli 1990 (DDR-GBl. I S. 899)
EStG	Einkommensteuergesetz
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)
FAGO	Geschäftsordnung für die Finanzämter
FGG	Gesetz über die Angelegenheiten der freiwilligen Gerichtsbarkeit

GeschoSReg	Geschäftsordnung der Sächsischen Staatsregierung vom 27. Juli 1992 (SächsABl. S. 1116), geändert gemäß Bekanntmachung vom 12. November 1993 (SächsABl. S. 1266)
GG	Grundgesetz für die Bundesrepublik Deutschland (Grundgesetz)
GO	Geschäftsordnung des Landtages des Freistaates Sachsen in der jeweils geltenden Fassung
GVG	Gerichtsverfassungsgesetz
KDO	Anordnung über den kirchlichen Datenschutz vom 14. Dezember 1993 (Kirchliches Amtsblatt für das Bistum Dresden-Meißen, Nr. 26, 15. Dezember 1993, S. 316) inhaltsgleich: Anordnung über den kirchlichen Datenschutz vom 30. Dezember 1993 (Amtsblatt der Apostolischen Administratur Görlitz, Nr. 2, 10. Januar 1994, S. 1)
KDO-DVO	Verordnung zur Durchführung der Anordnung über den kirchlichen Datenschutz vom 1. Juli 1994 (Kirchliches Amtsblatt für das Bistum Dresden-Meißen, Nr. 12, 5. Juli 1994, S. 164)
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)
KRG	Gesetz über Krebsregister (Krebsregistergesetz) vom 4. November 1994 (BGBl. I S. 3351)
KSchG	Kündigungsschutzgesetz
LMBG	Gesetz über den Verkehr mit Lebensmitteln, Tabakerzeugnissen, kosmetischen Mitteln und sonstigen Bedarfsgegenständen (Lebensmittel- und Bedarfsgegenständegesetz) in der Fassung der Bekanntmachung vom 8. Juli 1993 (BGBl. I S. 1169), zuletzt geändert durch Art. 2 des Gesetzes zur Reform des Weinrechts vom 8. Juli 1994 (BGBl. I S. 1467) und § 54 Medizinproduktegesetzes vom 2. August 1994 (BGBl. I S. 1963)
LPachtVG	Gesetz über die Anzeige und Beanstandung von Landpachtverträgen (Landpachtverkehrsgesetz) vom 8. November 1985 (BGBl. I S. 2075), zuletzt geändert durch Art. 31 des Agrarsozialreformgesetzes vom 29. Juli 1994 (BGBl. I S. 1890)

LuftVG	Luftverkehrsgesetz vom 1. August 1922 (RGBl. I S. 681) in der Fassung der Bekanntmachung 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)
LWO	Verordnung des Sächsischen Staatsministeriums des Innern über die Durchführung der Wahlen zum Sächsischen Landtag (Landeswahlordnung) vom 11. Februar 1992 (GVBl. S. 369)
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)
MRK	Konvention zum Schutze der Menschenrechte und Grundfreiheiten vom 4. November 1950 (BGBl. 1952 II S. 685)
MRRG	Melderechtsrahmengesetz in der Fassung der Bekanntmachung vom 24. Juni 1994 (BGBl. I S. 1430)
MVVO	Erste Verordnung des Sächsischen Staatsministeriums des Innern zur Durchführung des Sächsischen Meldegesetzes (Meldevordruckverordnung) vom 6. September 1993 (GVBl. S. 863)
OWiG	Gesetz über Ordnungswidrigkeiten (Ordnungswidrigkeitengesetz)
Pflegebedürftigkeits-richtlinien	Richtlinien der Spitzenverbände der Pflegekassen über die Abgrenzung der Merkmale der Pflegebedürftigkeit und der Pflegestufen sowie zum Verfahren der Feststellung der Pflegebedürftigkeit (PflRi) einschließlich Gutachten-Vordruck vom 7. November 1994 (nicht verkündet)
PStG	Personenstandsgesetz
RAFachBezG	Gesetz über Fachanwaltsbezeichnungen nach der Bundesrechtsanwaltsordnung und zur Änderung der Bundesrechtsanwaltsordnung vom 27. Februar 1992 (BGBl. I S. 369)
RegVBG	Gesetz zur Vereinfachung und Beschleunigung registerrechtlicher und anderer Verfahren vom 20. Dezember 1993 (BGBl. I S. 2182)
RVO	Reichsversicherungsordnung
SächsAGLMBG	Gesetz zur Ausführung des Lebensmittel- und Bedarfsgegenständegesetzes im Freistaat Sachsen vom 31. März 1994 (GVBl. S. 682)
SächsAGTierSG	Sächsisches Ausführungsgesetz zum Tierseuchengesetz (Landestierseuchengesetz) vom 22. Januar 1992 (GVBl. S. 29)

SächsArchG	Archivgesetz für den Freistaat Sachsen vom 17. Mai 1993 (GVBl. S. 449)
SächsBestG	Sächsisches Gesetz über das Friedhofs-, Leichen- und Bestattungswesen (Sächsisches Bestattungsgesetz) vom 8. Juli 1994 (GVBl. S. 1321)
SächsBeurtVO	Verordnung der Sächsischen Staatsregierung über die dienstliche Beurteilung der Beamten vom 11. Januar 1994 (GVBl. S. 90)
SächsBG	Beamtengesetz für den Freistaat Sachsen in der Fassung der Bekanntmachung vom 16. Juni 1994 (GVBl. S. 1153)
SächsDSG	Gesetz zum Schutz der informationellen Selbstbestimmung im Freistaat Sachsen (Sächsisches Datenschutzgesetz) vom 11. Dezember 1991 (GVBl. S. 401)
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)
SächsHKaG	Gesetz über Berufsausübung, Berufsvertretungen und Berufsgerichtsbarkeit der Ärzte, Zahnärzte, Tierärzte und Apotheker im Freistaat Sachsen (Sächsisches Heilberufekammergesetz) vom 24. Mai 1994 (GVBl. S. 935)
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)
SächsKVZ	Verordnung des Sächsischen Staatsministeriums der Finanzen über die Festsetzung der Verwaltungsgebühren und Schreibauslagen (Sächsisches Kostenverzeichnis) vom 14. Februar 1994 (GVBl. S. 493)
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 § 15 des Gesetzes über die Errichtung der Sächsischen Anstalt für kommunale Datenverarbeitung (SAKDG) vom 15. Juli 1994 (GVBl. S. 1432)
SächsPolG	Polizeigesetz des Freistaates Sachsen in der Fassung der Bekanntmachung vom 15. August 1994 (GVBl. S. 1541)

SächsPresseG	Sächsisches Gesetz über die Presse vom 3. April 1992 (GVBl. S. 125)
SächsSchulG	Schulgesetz für den Freistaat Sachsen vom 3. Juli 1991 (GVBl. S. 213), zuletzt geändert durch Gesetz zur Änderung des Schulgesetzes für den Freistaat Sachsen vom 15. Juli 1994 (GVBl. S. 1434)
SächsStatG	Sächsisches Statistikgesetz vom 17. Mai 1993 (GVBl. S. 453)
SächsStudDatVO	Verordnung des Sächsischen Staatsministeriums für Wissenschaft und Kunst zur Verarbeitung personenbezogener Daten der Studienbewerber, Studenten und Prüfungskandidaten für statistische und Verwaltungszwecke der Hochschulen (Sächsische Studentendatenverordnung) vom 9. Mai 1994 (GVBl. S. 916)
SächsVerf	Verfassung des Freistaates Sachsen vom 27. Mai 1992 (GVBl. S. 243)
SächsVSG	Gesetz über den Verfassungsschutz im Freistaat Sachsen (Sächsisches Verfassungsschutzgesetz) vom 16. Oktober 1992 (GVBl. S. 459)
SächsVwKG	Verwaltungskostengesetz des Freistaates Sachsen vom 15. April 1992 (GVBl. S. 164)
SächsVwVfG	Vorläufiges Verwaltungsverfahrensgesetz für den Freistaat Sachsen vom 21. Januar 1993 (GVBl. S. 74)
SächsWaldG	Waldgesetz für den Freistaat Sachsen vom 10. April 1992 (GVBl. S. 137)
SGB I	Sozialgesetzbuch - Allgemeiner Teil - vom 11. Dezember 1975 (BGBl. I S. 3015), zuletzt geändert durch Art. 2 des Agrarsozialreformgesetzes 1995 vom 29. Juli 1994 (BGBl. I S. 1890)
SGB IV	Sozialgesetzbuch - Gemeinsame Vorschriften für die Sozialversicherung - vom 23. Dezember 1976 (BGBl. I S. 3845), zuletzt geändert durch Art. 3 des Agrarsozialreformgesetzes 1995 vom 29. Juli 1994 (BGBl. I S. 1890)
SGB V	Sozialgesetzbuch - Gesetzliche Krankenversicherung - vom 20. Dezember 1988 (BGBl. I S. 2477), zuletzt geändert durch Art. 4 des Agrarsozialreformgesetzes 1995 vom 29. Juli 1994 (BGBl. I S. 1890)
SGB VI	Sozialgesetzbuch - Gesetzliche Rentenversicherung - vom 18. Dezember 1989 (BGBl. I S. 2261, ber. BGBl. 1990 I S. 1337), zuletzt geändert durch Art. 5 des Agrarsozialreformgesetzes 1995 vom 29. Juli 1994 (BGBl. I S. 1890)

SGB VIII	Sozialgesetzbuch - Kinder- und Jugendhilfe - vom 26. Juni 1990 (BGBl. I S. 1163) in der Fassung der Bekanntmachung vom 3. Mai 1993 (BGBl. I S. 637), zuletzt geändert durch Art. 5 des Zweiten Gesetzes zur Änderung des Sozialgesetzbuches vom 13. Juni 1994 (BGBl. I S. 1229)
SGB X	Sozialgesetzbuch - Verwaltungsverfahren - vom 18. August 1980 und 4. November 1982, zuletzt geändert durch Art. 6 des Zweiten Gesetzes zur Änderung des Sozialgesetzbuches vom 13. Juni 1994 (BGBl. I S. 1229)
SGB XI	Sozialgesetzbuch - Soziale Pflegeversicherung - vom 26. Mai 1994 (BGBl. I S. 1014), geändert durch Art. 6 des Agrarsozialreform-gesetzes 1995 vom 29. Juli 1994 (BGBl. I S. 1890)
SHG	Gesetz über die Hochschulen im Freistaat Sachsen (Sächsisches Hochschulgesetz) vom 4. August 1993 (GVBl. S. 693)
SOGS	Verordnung des Sächsischen Staatsministeriums für Kultus über Grundschulen im Freistaat Sachsen (Schulordnung Grundschulen) vom 2. Mai 1994 (GVBl. S. 1117)
SOGY	Verordnung des Sächsischen Staatsministeriums für Kultus über allgemeinbildende Gymnasien im Freistaat Sachsen (Schulordnung Gymnasien) vom 15. Dezember 1993 (GVBl. 1994 S. 220)
SOMI	Verordnung des Sächsischen Staatsministeriums für Kultus über Mittelschulen im Freistaat Sachsen (Schulordnung Mittelschulen) vom 10. September 1993 (GVBl. S. 879)
StGB	Strafgesetzbuch
StPO	Strafprozeßordnung
StrRehaG	Gesetz über die Rehabilitierung und Entschädigung von Opfern rechtsstaatswidriger Strafverfolgungsmaßnahmen im Beitrittsgebiet (Strafrechtliches Rehabilitierungsgesetz) vom 29. Oktober 1992 (BGBl. I S. 814, zuletzt geändert durch Art. 6 des Zweiten SED-Unrechtsbereinigungsgesetzes vom 23. Juni 1994 BGBl. I S. 1311)
StUG	Gesetz über die Unterlagen des Staatssicherheitsdienstes der ehemaligen Deutschen Demokratischen Republik (Stasi-Unterlagen-Gesetz) vom 20. Dezember 1991 (BGBl. I S. 2272), zuletzt geändert durch Art. 12 des Gesetzes vom 14. September 1994 (BGBl. I S. 2325)
StVG	Straßenverkehrsgesetz
StVZO	Straßenverkehrs-Zulassungs-Ordnung
SÜG	Gesetz über die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen des Bundes (Sicherheitsüberprüfungsgesetz) vom 20. April 1994 (BGBl. I S. 867)

TierSG	Tierseuchengesetz in der Fassung der Bekanntmachung vom 29. Januar 1993 (BGBl. I S. 116), zuletzt geändert durch Art. 7 § 5 des Gesundheitseinrichtungen-Neuordnungs-Gesetzes vom 24. Juni 1994 (BGBl. I S. 1416)
TreuhG	Gesetz zur Privatisierung und Reorganisation des volkseigenen Vermögens (Treuhandgesetz) vom 17. Juni 1990 (DDR-GBl. I S. 300), zuletzt geändert durch das Gesetz zur abschließenden Erfüllung der verbleibenden Aufgaben der Treuhandanstalt vom 9. August 1994 (BGBl. I S. 2062)
UIG	Umweltinformationsgesetz vom 8. Juli 1994 (BGBl. I S. 1490)
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)
VVVGVO	Verordnung des Sächsischen Staatsministeriums der Justiz zur Durchführung des Gesetzes über Volksantrag, Volksbegehren und Volksentscheid vom 18. Juli 1994 (GVBl. S. 1357)
VwRehaG	Gesetz über die Aufhebung rechtsstaatswidriger Verwaltungs-entscheidungen im Beitrittsgebiet und die daran anknüpfenden Folgeansprüche (Verwaltungsrechtliches Rehabilitierungs-gesetz) vom 23. Juni 1994 (BGBl. I S.1311)
VwVfG	Verwaltungsverfahrensgesetz
VZG 1983	Gesetz über eine Volks-, Berufs-, Wohnungs- und Arbeitsstätten-zählung (Volkszählungsgesetz 1983) vom 25. März 1982 (BGBl. I S. 369)
Wohnungs-belegungsgesetz	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
WoStatG	Gesetz über gebäude- und wohnungsstatistische Erhebungen (Wohnungsstatistikgesetz) vom 18. März 1993 (BGBl. I S. 337)
WPflG	Wehrpflichtgesetz in der Fassung der Bekanntmachung vom 14. Juli 1994 (BGBl. I S. 1505)

Sonstiges

AfL/ÄfL	Amt/Ämter für Landwirtschaft
AfNS	Amt für Nationale Sicherheit
AOK	Allgemeine Ortskrankenkasse
BfD	Der Bundesbeauftragte für den Datenschutz

BGBl.	Bundesgesetzblatt
BKK	Betriebskrankenkasse
BMJ	Bundesministerium der Justiz
BStU	Der Bundesbeauftragte für die Unterlagen des Staatssicherheitsdienstes der ehemaligen Deutschen Demokratischen Republik
BVerfGE	Amtliche Sammlung der Entscheidungen des Bundesverfassungsgerichts
BVerwGE	Amtliche Sammlung der Entscheidungen des Bundesverwaltungsgerichts
BVS	Bundesanstalt für vereinigungsbedingte Sonderaufgaben (bis 31. Dezember 1994: THA)
DSMeld	Datensatz für das Meldewesen
DVBl	Deutsches Verwaltungsblatt
DVO	Durchführungsverordnung
EG	Europäische Gemeinschaften
EU	Europäische Union
EWG	Europäische Wirtschaftsgemeinschaft
Gauck-Behörde	Der Bundesbeauftragte für die Unterlagen des Staatssicherheitsdienstes der ehemaligen Deutschen Demokratischen Republik
GVBl.	Sächsisches Gesetz- und Verordnungsblatt
IKK	Innungskrankenkasse
IM	Inoffizieller Mitarbeiter (des MfS/AfNS)
ISD	Internationaler Suchdienst Arolsen
JVA	Justizvollzugsanstalt
KBA	Kraftfahrtbundesamt in Flensburg
LUA	Landesuntersuchungsanstalt für das Gesundheits- und Veterinärwesen
LÜVA	Lebensmittelüberwachungs- und Verterinäramt
MfS	Ministerium für Staatssicherheit
NJW	Neue Juristische Wochenschrift
NVwZ	Neue Zeitschrift für Verwaltungsrecht
SächsABl.	Sächsisches Amtsblatt
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
SSG	Sächsischer Städte- und Gemeindetag e. V.
SLT	Sächsischer Landkreistag e. V.
THA	Treuhandanstalt

1 Datenschutz im Freistaat Sachsen

Abgeordnete, Mitarbeiter im öffentlichen Dienst und andere interessierte Leser können in diesem Tätigkeitsbericht einen Überblick über die Schwerpunkte meiner Arbeit gewinnen. Datenschutz muß mit Augenmaß betrieben werden; er muß dem Schutz der Privatheit ebenso genügen wie dem Anspruch des Gemeinwesens auf die im einzelnen erforderlichen Informationen.

Auch in diesem Jahr danke ich allen Mitarbeitern meiner Dienststelle, ohne die dieser Bericht natürlich nicht zustande käme. Sie haben mit Mut und Sachverstand ihre Dienstpflichten erfüllt.

Der manchmal kontroverse, manchmal auch einvernehmliche Diskurs um die richtige Entscheidung zwischen dem Schutz der Privatsphäre und dem Anspruch der Allgemeinheit an jeden Einzelnen wird die öffentliche Verwaltung auch weiterhin heilsam beunruhigen.

1.1 Datenverarbeitung und Zentralismus

Der Sächsische Städte- und Gemeindetag e. V. (SSG e. V.) hat ein Gutachten eines renommierten Softwareherstellers eingeholt und daraufhin seinen Mitgliedsgemeinden den Rat erteilt, ihre Datenverarbeitung auf eine kommunale Datenzentrale zu übertragen, die im Rechenzentrum der Stadt Leipzig eingerichtet werden soll.

Als Inhaber von Lizenzen der Datenzentrale Baden-Württemberg war der SSG e. V. als Ratgeber nicht frei von eigenen Interessen und daher befangen, zumal er dezentrale Alternativen durch den Gutachter nicht prüfen ließ: Der Auftrag an den Gutachter ging dahin herauszufinden, welches der sechs sächsischen Großrechenzentren die zentral angelegten baden-württembergischen Verfahren bearbeiten solle. Dem Rat eines so befangenen Gremiums vermag ich keine hinreichende Qualität abzugewinnen.

Es kann doch nicht wahr sein, daß der Sächsische Verfassungsgeber die Stellung der Gemeinden und ihre Pflicht zur Eigenständigkeit und Eigenverantwortung betont und stärkt und sodann deren Berater dem Zentralismus das Wort redet.

Ein weiteres: Im SMI träumen einige von einem landeseinheitlichen Datennetz der Verwaltung. Als Ideal gilt ein ungehinderter Datenaustausch zwischen allen öffentlichen Stellen. Die Frage nach einem Bedarf für solche Kommunikation scheint den Planern zweitrangig zu sein, sie wurde bislang jedenfalls nicht beantwortet. Die neue "Arbeitsgemeinschaft Landesnetz", an der meine Dienststelle teilnimmt, hat kürzlich den Blick von der Machbarkeit zur Erforderlichkeit gelenkt. Es mag sein, daß Dienste wie die Juris-Datenbank oder der Zugriff auf aktuelle Vorschriftensammlungen sinnvoll sind, einen ausreichenden Bedarf für eine Vernetzung bilden sie nicht.

Es ist ein datenschutzrechtliches Grundbedürfnis, insbesondere die automatisierte Datenverarbeitung überschaubar zu gestalten. Der Richter am Bundesverfassungsgericht Hermann Heußner (Freiheitssicherung durch Datenschutz, Frankfurt, 1987) führt als Ausgangsüberlegung der Verfassungslage aus:

> "Es gibt keine Einheit der Staatsgewalt im Sinne einer Informationseinheit der gesamten öffentlichen Verwaltung. Es ist auch innerhalb einer Körperschaft des öffentlichen Rechts nach den verschiedenen Funktionen und Aufgaben zu unterscheiden und die Informationsübermittlung danach abzugrenzen ... Mit dem Recht auf informationelle Selbstbestimmung ist es deshalb unvereinbar, wenn der Bürger nicht mehr wissen kann, wer was wann und bei welcher Gelegenheit über ihn weiß. Ein für den Bürger völlig undurchschaubarer Datenverkehr würde nicht nur die individuellen Entfaltungschancen, sondern auch das Gemeinwohl beeinträchtigen, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist."

Unüberschaubare Datensammlungen, Verknüpfungsmöglichkeiten und unkontrollierte Datenverkehrsmöglichkeiten widersprechen den elementaren Forderungen des Volkszählungsurteils. Diese Forderungen können umso leichter erfüllt werden, je ortsnäher und individueller die Daten verarbeitet werden. Die dezentrale Datenverarbeitung in den Gemeinden - folgt man der durchgängigen Rechtsprechung des Bundesverfassungsgerichts - ist eine Grundlage für kluge, ortsnahe Entscheidungen und damit ein Garant für die grundrechtlich verbürgte Überschaubarkeit der Datenverarbeitung.

Ich fordere daher die sächsischen Gemeinden auf, sich zu leistungsfähigen Einheiten, wie vielerorts bereits geschehen, zusammenzuschließen, um eine autonome Datenverarbeitung zu organisieren. Beratung und Betreuung übernehmen auch die privaten und öffentlichen Anbieter am Markt, in erster Linie aber die Sächsische Anstalt für Kommunale Datenverarbeitung, die durch Standards, Empfehlungen und Zertifikate einen Beitrag zur zukunftsorientierten und sparsamen kommunalen Datenverarbeitung leisten soll und wird.

Ich hoffe, daß die - für das Anliegen der Selbstverwaltung besonders aufgeschlossene - Stadt Leipzig ihre Aufgabe als eine vorübergehende betrachtet und daß auch ihre Fachleute im Rechenzentrum die Gemeinden mit in Zukunft mehr und mehr wachsender Verwaltungskraft darin bestärken, in der automatisierten Datenverarbeitung jeweils eigene Wege zu gehen.

Nur so entsteht ein neues und hochmodernes Betätigungsfeld für den für Sachsen sprichwörtlichen Erfindungsreichtum und für maßgeschneiderte Datenverarbeitungstechnik im örtlichen Bereich, nur so wird die sächsische Verwaltung von den sich ansiedelnden Unternehmen der Informations- und Kommunikationstechnik als kompetenter Partner akzeptiert.

Betonköpfe in West und Ost, die dem Zentralismus verhaftet sind, sollten darüber nachdenken, warum die DDR gescheitert ist: Es war weniger das Banausentum der Funktionäre, es war nicht so sehr das von Anfang an mißglückte Menschenbild des theoretischen Kommunismus, sondern der Grund für das Elend war der - allerdings aus beidem geborene - bürokratische Zentralismus: Zentralisten glauben an höhere Einsichten der Verwaltung mehr als an die personale Kraft des Einzelnen, sie hoffen auf die Vernunft eines anonymen, aber nichtsdestoweniger elitären Kollektivs mehr als auf störende Erfindungen eigenständiger Köpfe, und sie lieben die Ruhe des Massenbewußtseins mehr als die durch die Freiheit freigesetzten geistigen Kräfte. Materielles wird von den Zentralisten ins Mystische verklärt. Ihre metaphysischen Bedürfnisse nach Machbarkeit und Führung enden im Kult der rechtlosen Vernunft und der rücksichtslosen Technik.

Nun sollten die Zentralisten wissen, daß sie gescheitert sind.

Jeder, der etwas von der modernen technischen Entwicklung versteht, weiß, daß die Entwicklung der technischen Systeme hin zur Dezentralisierung fortschreitet. Große Netze mögen in Bezug auf kommerzielle Dienste und weltweit abrufbare, jedermann frei zugängliche und deshalb auf Dauer uninteressante Daten auch recht dienlich sein, in der öffentlichen Verwaltung sind sie jedoch meist überflüssig. Denn in vielen Bereichen der Verwaltung geht es um die Institutionalisierung von Herrschaftsrechten an aufgeteilten und monopolisierten Informationen. Jedem leuchtet ein, daß ein Informationsnetz der Polizei abgeschottet sein muß gegenüber Informationsnetzen der Statistik, der Sozialverwaltung, des Verfassungsschutzes oder des Landesamtes für Finanzen. Tatsächlich: Im SMI favorisierte das sich für zuständig haltende Fachreferat die Zusammenlegung des kommunalen Großrechenzentrums mit dem staatlichen Rechenzentrum des Statistischen Landesamtes in Kamenz. Ich halte es meiner Dienststelle, aber auch dem Zweckverband Westsachsen zugute, daß wir eine derartige - geradezu absurde - Lösung durch Einwirkung auf den Entscheidungsprozeß verhindern konnten.

1.2 Datenautobahn

Der Topos vom "Information-super-highway" beherrscht die Szene; er wurde durch den amerikanischen Vizepräsidenten Al Gore geprägt; mit dem deutschen Begriff "Datenautobahn" ist er unglücklich übersetzt. Ein Amerikaner kennt zwar den deutschen Begriff der "Autobahn" als Lehnwort und verbindet ihn mit Raserei und ungehemmter Bewegungsfreiheit; beim "Highway" denkt der Technikfreak aber nicht unbedingt an eine Autobahn, sondern ebenso an ein Glasfaserkabel oder einen Richtfunkstrahl. "Geisterfahrer" oder "Surfen im Netz"? Der Bilder gibt es viele (und falsche!).

Der deutsche EU-Kommissar Martin Bangemann hat die Entwicklung, die Anwendung und den weltweiten Vertrieb europäischer Datenverarbeitungsprodukte der neuen Hochtechnologie zur zentralen Aufgabe (und Hoffnung) künftiger Wirtschaftspolitik erklärt. Globale und europäische Informationskonzeptionen, online-Verbindungen und

Querschaltungen können nicht nur den Markt beherrschen, sondern das gesellschaftliche und politische Leben verändern.

Die diesjährige CeBit in Hannover hat gezeigt, daß dieser rasanten technischen Entwicklung - möglicherweise deshalb, weil man nicht zu den Bedenkenträgern gerechnet werden möchte - keine kritische Medienöffentlichkeit gegenübersteht. Die Freude auf neue Märkte und Arbeitsplätze, das kindliche Interesse an technischen Spielzeugen, aber auch die Faszination weltweiter Verbindung (Internet) führt zu einer fast euphorischen Haltung der Verantwortlichen.

Der Grundrechtsschutz bleibt da leicht auf der Strecke: Eine fundierte Technikfolgenphilosophie ist noch nicht entwickelt. Rechtsregeln für die Fahrt auf der Datenautobahn fehlen ebenso wie intelligente Verkehrsleitsysteme und Sanitätsdienste.

Ich rede hier nicht überzogenen Regelungsansprüchen das Wort: Die Forderung nach bereichsspezifischen Rechtsregeln im Umgang mit personenbezogenen Daten hat sicher ihre Grenzen; der Rechtsstaat darf nicht zum Rechtsregelstaat werden, der starr und immer ein wenig gestrig die wache Kompetenz der Verwaltung, auf neue Herausforderungen unverzüglich reagieren zu können, durch ein unüberschaubares - und deshalb menschenfeindliches - Regelwerk beschneidet.

Dennoch müssen die Ströme von Informationen über Menschen rechtlich beherrscht werden. Hier zwei Beispiele, wie man es nicht machen sollte:

a) Die Telekommunikation, die blitzschnell unbegrenzt komfortable Leistungen unter hoher allgemeiner Akzeptanz zur Verfügung stellt und weltweite Interaktion ermöglicht, soll - zwanzig Jahre zu spät - durch eine ISDN-Richtlinie der EU in ein rechtliches Korsett geschnürt werden. Nach recht hoffnungsvoller Einstimmung haben sich die Verhandlungen festgefahren: Die wirtschaftlichen Interessen der Einzelstaaten sind unüberwindlich. Nur über wenige Punkte wird eine Einigung auf der EU-Ebene möglich sein: Zweckbindungsregeln, der Schutz vor Kommunikationsprofilen, das Postgeheimnis werden zumindest teilweise auf der Strecke bleiben. Beratungsstellen können nicht mehr anonym angerufen werden, das spurenlose Miteinander-Reden gehört der Vergangenheit an. Natürlich bleibt das Herrschaftswissen darüber interessant, wer wie lang mit wem (und wahrscheinlich auch mit welchem Inhalt) kommuniziert hat. So wird sich auf Dauer jeder überlegen müssen, ob er am ISDN-System teilnehmen möchte, ob er diesen Service nutzt oder ihm aus Angst um seine Privatsphäre aus dem Weg geht. Letztlich wird - jedenfalls auf dem Gebiet der privaten Telekommunikation - der Markt entscheiden, ob nicht doch datenschutz-freundliche Systeme höhere Akzeptanz genießen und daher das Rennen machen. Schon jetzt überlegt die Telekom, besonders geschützte Verbindungen anzubieten, die der Verschlüsselung und Abhörsicherheit höheren Rang einräumen, und sie entwickelt prepaid-Systeme, bei denen keinerlei Abrechnungsdaten entstehen oder gespeichert werden.

b) Das längst eingerichtete, aber erst 1994 auf eine gesetzliche Grundlage gestellte Ausländerzentralregister (siehe 5.10.4 im 2. Tätigkeitsbericht) hat die bisherige Verwaltungspraxis zum Gesetzesmaßstab gemacht. Alles, was Ausländerbehörden, Polizeidienststellen und Nachrichtendienste bereits ohne Rechtsgrundlage eingerichtet hatten, wurde vom Gesetzgeber sanktioniert. Insbesondere die seit langem hier ansässigen Ausländer werden dadurch diskriminiert.

Es gibt aber auch Beispiele dafür, daß frühzeitig und parallel mit der technischen Entwicklung der Schutz eingearbeitet wird, der eine rechtliche Beherrschung der Informationen und Datensammlungen ermöglichen soll: Das Bundesverkehrsministerium hat bei der Suche nach einer Konzeption zur Gebührenerhebung auf Bundesautobahnen die Datenschutzproblematik von Anfang an gesehen und mitbedacht. Ich weiß noch nicht, ob die derzeitige Zurückhaltung des Ministeriums tatsächlich vermuten läßt, daß von den Plänen zur Mauterhebung Abstand genommen werden wird oder ob es sich bei dieser Zurückhaltung nur um einen Versuch zeitweiliger Beruhigung der Öffentlichkeit handelt. Mit meinen Kollegen in Bund und Ländern (vgl. unten 16.2.8) verlange ich, daß anonymes Fahren möglich sein muß, daß Spuren der Mautentrichtung nicht vorgehalten werden dürfen, Daten über korrekte Benutzer nicht gespeichert werden dürfen, daß Beschlagnahmeverbote für sämtliche Daten bestehen müssen und für alle Daten eine Zweckänderung ausgeschlossen ist.

Auch in diesem Zusammenhang taucht - allerdings meist abstrakt - die wohlfeile These auf, der "anständige Bürger" brauche keinen Datenschutz, weil er nichts zu verbergen habe. "Wozu Grundrechte? Ich liebe den Staat und vertraue ihm!" Wer dies behauptet, widerspricht aller Lebenserfahrung, denn jeder will nur solche Daten über seine persönlichen und geschäftlichen Verhältnisse verbreiten, die ihm vorteilhaft erscheinen. Niemand ist bereit, in jedem denkbaren Einzelfall z. B. seine wirtschaftliche Bedrängnis, seinen Konsum, sein heimliches Suchtverhalten (es gibt ja viele Süchte), seine Gesprächskontakte oder seine finanzielle Situation offenzulegen. Täte er dies, brächte er sich zumindest in die Gefahr, sich ständig nur rechtfertigen zu müssen, weil aus seiner Sicht mit bruchstückhaften Daten ein falscher Eindruck entstanden ist. Öffentliche Datensammlungen über charakterliche Spielarten, exzentrische Verhaltensweisen, gesundheitliche Verhältnisse, Kommunikationsdaten und Bewegungsbilder dürfen weder entstehen noch gar miteinander verknüpft werden. Würden sie darüber hinaus der Obrigkeit frei zugänglich sein, so wäre es mit unserer Freiheit und unserer natürlichen Individualität am Ende.

Zurück zur "Datenautobahn": Bei aller Faszination, die von der Entwicklung ausgeht, müssen wir daran festhalten, daß die Rechtsordnung nicht alles, was technisch machbar ist, gestatten darf. Dabei kommt dem Bereich der Privatautonomie sicherlich ein größerer Regelfreiraum zu als dem grundrechtlich begrenzten Handeln öffentlicher Institutionen. Ich will nicht unbedingt erreichen, daß jeder Umgang des Staates mit Daten seiner Bürger derart verrechtlicht werden muß, wie dies im Melderecht oder im Sozialgesetzbuch geschehen ist. Dennoch muß sichergestellt werden, daß das Grundrecht auf

informationelle Selbstbestimmung gewahrt bleibt. Hier wartet neue Arbeit auf den Gesetzgeber.

1.3 Die Rolle des Datenschutzbeauftragten

Bleibt man beim Bild der Datenautobahn, so ist offen, welche Rolle der Datenschutzbeauftragte spielen soll: Ist er die Autobahnmeisterei oder sorgt er nur für das Begleitgrün, schafft er Behelfsparkplätze und Behelfsausfahrten oder ist er - ganz allgemein - eine Datenpolizei, wie dies der ehemalige schleswig-holsteinische Innenminister und frühere Bundesdatenschutzbeauftragte Bull in dem Sinne andeutet, daß die Polizei in erster Linie Freund und Helfer der Verkehrsteilnehmer ist und erst ganz zuletzt hilft, den Rasern die Lizenz zu entziehen.

Ich sehe ein wenig die Gefahr, daß insbesondere die betrieblichen und behördlichen Datenschutzbeauftragten zu Alibiinstanzen einer allzu flotten Informationsgesellschaft werden; sie werden vorgezeigt und hofiert, wenn es darum geht, sich rechtsstaatlich zu geben oder gar staatliche Stellen zu schützen; sie werden aber umgangen und kurzgehalten, wenn ihre Kritik zu erwarten ist.

In Sachsen läuft die Zusammenarbeit mit den Behörden grundsätzlich zufriedenstellend. Versuche unzulässiger Einflußnahme auf den Datenschutzbeauftragten finden ebensowenig statt wie seine bewußte Umgehung. Allerdings hätte ich mir einige Male gewünscht, zu Veranstaltungen eingeladen oder rechtzeitig gefragt zu werden. Es muß in einigen Ressorts noch mehr zum Alltag gehören, den Datenschutzbeauftragten immer dann zu beteiligen, wenn technische, organisatorische und juristische Probleme im Zusammenhang mit personenbezogenen Daten zu lösen sind. In den vielen Fällen, in denen ich mitwirken konnte, habe ich mich nach Kräften bemüht, konstruktive Vorschläge zu machen.

Die im 2. Tätigkeitsbericht (1.1. bis 1.5) angedeuteten Probleme sind für mich folgenlos gelöst: Die gegen mich erhobenen Vorwürfe haben sich nach sorgfältiger Prüfung durch die zuständigen Behörden als haltlos herausgestellt. Die Unabhängigkeit meiner Amtsführung wurde nicht ernsthaft in Frage gestellt.

1.4 Systemnähe

Die Staatsregierung hat im Dezember 1994 - warum so spät, lasse ich hier dahingestellt - eine Verwaltungsvorschrift zur Eignung von Beamten veröffentlicht, die zwar im einzelnen regelt, aus welchen Gründen jemand nicht geeignet ist, sächsischer Beamter zu sein (Stasi-Verstrickung und ehemals allzu große Nähe zum Repressionssystem der DDR). Offengeblieben ist jedoch die Frage, unter welchen Voraussetzungen Angestellte aus derartigen Gründen im öffentlichen Dienst untragbar sind.

Immer wieder treffe ich auf Gesprächspartner, die meinen, die Berufung in das Beamtenverhältnis sei eine Art "höhere Weihe", sie sei Zeichen besonderen Vertrauens oder Lohn für besonders treue Dienste. Dieser Denkansatz ist gründlich falsch: Art. 33 Abs. 4 des Grundgesetzes und Art. 91 Abs. 1 der Sächsischen Verfassung schreiben vor, daß die Ausübung hoheitsrechtlicher Befugnisse als ständige Aufgabe in der Regel Beamten zu übertragen ist. § 2 Abs. 2 des Beamtenrechtsrahmengesetzes bestimmt, daß Beamten nur hoheitsrechtliche Aufgaben übertragen werden dürfen. Mithin geht die Rechtsordnung davon aus, daß die wahrgenommene Aufgabe darüber entscheidet, ob ein Dienstposten von einem Beamten besetzt werden muß oder nicht.

Ich habe nicht darüber zu entscheiden, ob man den Kreis der "hoheitsrechtlichen Befugnisse" besonders eng zieht (aus vielerlei Gründen bin ich in der Tat dieser Auffassung), vielmehr geht es mir darum zu verhindern, daß mit den Formen des Beamtenrechts in Sachsen Mißbrauch getrieben wird. Dabei ist folgendes zu bedenken: Anders als alle anderen Datenschutzgesetze in Deutschland schreibt das Sächsische Datenschutzgesetz (in § 9) vor, daß die Verarbeitung personenbezogener Daten nur von solchen Stellen wahrgenommen werden darf, die die erforderlichen *"personellen Voraussetzungen"* erfüllen. Zur Ausfüllung dieses unbestimmten Rechtsbegriffs ist die gesamte Rechtsordnung, insbesondere Art. 119 der Sächsischen Verfassung heranzuziehen. Ich vertrete die Auffassung, daß immer dann, wenn es um die Verarbeitung personenbezogener Daten geht, der Einsatz nur solcher Personen in Betracht kommt, die unser besonderes Vertrauen rechtfertigen. Dies ist weder bei Personen der Fall, die nachhaltig, klaren Verstandes und konspirativ für das MfS gearbeitet haben, noch bei solchen Personen, die sich aktiv und maßgeblich in das Repressionssystem der DDR haben einbinden lassen. Ich habe übrigens die persönliche Erfahrung gemacht, daß belastete Personen auch weniger tüchtig sind. Jedoch bedarf es schon wegen der Komplexität der Vorgänge, z. B. bei besonders tragischen Verwicklungen, aber auch ganz grundsätzlich wegen zwingender rechtsstaatlicher Garantien einer Einzelfallprüfung in einem fairen Verfahren. Dies ändert jedoch nichts an dem Grundsatz, daß ich es nicht hinzunehmen vermag, daß beispielsweise in einem Landratsamt Bedienstete in Führungspositionen "im Rahmen der Personalkontinuität" den Menschen in der gleichen Funktion wie früher gegenübertreten. Ich kann verstehen, daß die Bürger in diesen Fällen kein Vertrauen in einen sorgfältigen Umgang mit ihren Daten entwickeln können.

1.5 Professoren-TÜV?

Studenten werden über die Leistungen ihrer Professoren ausgefragt. Die ersten Ergebnisse einer sächsischen Universität liegen mir vor. Ich erwarte, daß in diesem Jahr die Diskussion um die sog. "Evaluierung" der Leistungen in Forschung und Lehre an den sächsischen Hochschulen an Bedeutung zunimmt:

Wenn ein Gesetz eine staatliche Aufgabe beschreibt, enthält es dadurch zumindest ansatzweise hinreichende Kriterien dafür, welche Daten zur Erreichung dieses festgesetzten Zieles "erforderlich" sind. Anders ist es jedoch mit § 135 Abs. 3 SHG, der den Umgang

mit Daten des wissenschaftlichen und künstlerischen Personals u. a. zur Beurteilung der Lehr- und Forschungstätigkeit durch die Hochschulen regelt: Weil Lehr- und Forschungstätigkeit nach Art. 5 Abs. 3 GG frei von staatlichen oder anderen Einwirkungen ist, lassen sich gerade keine (oder nur sehr wenige) Kriterien dafür finden, welche Daten erhoben und verarbeitet werden dürfen. Welche Mittel der Wissenschaftler einsetzt und welche Wege er geht, um wahre Erkenntnisse zu gewinnen und sie zu verbreiten, wird vom Grundgesetz sowohl der sich selbst ergänzenden wissenschaftlichen Gemeinschaft der Hochschule als auch dem zu ihr gehörenden Einzelnen überlassen. Dies ist ein erfolgreiches und zugleich menschliches Rezept der Wissenschaft, von dem sich nur absolute Systeme zu ihrem Schaden abwenden. Das Grundrecht der Wissenschaftsfreiheit steht nicht unter dem Vorbehalt gesetzlicher Einschränkungen, sondern orientiert sich nur an der Suche nach Wahrheit, unter Wahrung der Treue zur Verfassung. Aufgabe des Staates und der Hochschulen ist es, die Rahmenbedingungen für eine freie Forschung und Lehre herzustellen und zu sichern, nicht aber, den Betrieb und den Einzelnen auf Erfolg zu kontrollieren. Nach welchen Maßstäben wollten sie das auch tun? Die Freiheit nach Art. 5 Abs. 3 GG bedeutet nahezu eine Unbegrenztheit, eine Nicht-Zielgenauigkeit, eine Zweck-Losigkeit der Wissenschaft. Rechtstechnisch heißt das: Weil die Zwecke des Hochschulgesetzes, was die Methode der Wahrheitsfindung und -vermittlung betrifft, gerade nicht definiert sind, kann auch die Frage der Erforderlichkeit eingreifender Maßnahmen nicht anhand einer gesetzlichen Vorgabe begrenzt oder beurteilt werden. Folglich enthält das Gesetz keine Kriterien dafür, welche Daten des wissenschaftlichen Personals gesammelt werden dürfen und welche Formen der Datenverarbeitung erforderlich sind, um den Inhalt und die Methode von Forschung und Lehre zu bewerten. Gerade die Freiheit ist das geeignete Mittel, um einen Wissenschaftsbetrieb als öffentlichen Zweck zu organisieren.

Wenn es noch eines Beweises dafür bedürfte, könnte man ohne Zuhilfenahme der Verfassung auf § 5 Abs. 3 SHG verweisen. Dort heißt es: "*Die Freiheit der Lehre umfaßt im Rahmen der Lehraufgaben insbesondere die Abhaltung von Lehrveranstaltungen und deren inhaltliche und methodische Gestaltung sowie das Recht auf Äußerung von wissenschaftlichen und künstlerischen Lehrmeinungen*". Wohlgemerkt: All dies frei von staatlicher Aufsicht oder sonstiger, auch inneruniversitärer amtlicher Einwirkung.

Die Vorschrift lautet weiter: "*Beschlüsse von Hochschulorganen zur Lehre sind insoweit zulässig, als sie sich auf die Organisation des Lehrbetriebes und auf die Aufstellung und Einhaltung von Studien- und Prüfungsordnungen beziehen; sie dürfen die Freiheit im Sinne von Satz 1 nicht beeinträchtigen.*"

Erlaubt ist demgemäß - zu Recht - lediglich die Festlegung von Mindeststandards der Lehrbetriebs-Organisation und die Kontrolle der Einhaltung von Studienordnungen und Prüfungsordnungen mit Hilfe der dazu in der Tat erforderlichen Daten.

Hingegen ist es ein Eingriff in Art. 5 Abs. 3 GG, wenn man die Methodik des "Rüberbringens" wissenschaftlicher Inhalte (Lehre) einer administrativen Kontrolle unterwirft.

Gestattet ist nach alledem nur die Festlegung eines - mit Sicherheit nicht in die Freiheit der Wissenschaft eingreifenden - Mindeststandards, z. B. gewisse Pflichtstunden, gewisse sprachliche Verständlichkeiten, Sprechstunden für Studenten, u. ä. Nur die damit verbundene -geringfügige - Datenverarbeitung findet im SHG eine verfassungsrechtlich gesicherte Grundlage; nur insoweit ist eine Rechtsverordnung zulässig und geboten.

Angesichts seines freiheitswidrigen - weil zu weiten - Ansatzes ist § 135 Abs. 3 SHG deshalb verfassungsrechtlich zumindest höchst problematisch. Konkret durchgeführt wird dieser Ansatz der Beschränkung der Wissenschaftsfreiheit im Gesetz nicht. Es stellt nur ein *Instrumentarium* für solche Eingriffe bereit, ohne den Zweck von dessen Verwendung inhaltlich zu bestimmen.
Das hat naturgemäß einen weiteren Verfassungsverstoß zur Folge: Der Verordnungsermächtigung in § 135 Abs. 3 Satz 2 SHG fehlt die nach Art. 80 Abs. 1 Satz 2 GG erforderliche Bestimmtheit von Zweck, Inhalt und Ausmaß! Anschaulicher: Es fehlt in der Vorschrift jeder Rahmen für die Qualität, die Validität sowie die Eingriffstiefe der Daten, die erhoben werden sollen, um die Leistung der Forscher und (wissenschaftlichen) Lehrer zu bewerten. § 135 Abs. 3 SHG enthält aber eben nur Regelungen dazu, daß die Zweckbindung der Daten gesichert, ihre Kenntnis für den Betroffenen garantiert und die Vernichtung geregelt werden.

Der Verfassungsgrundsatz des *Vorbehaltes des Gesetzes* (Wesentlichkeits-Doktrin des Bundesverfassungsgerichts) verbietet es, dem Verordnungs- oder gar Satzungsgeber - und ein solcher ist die Universität bekanntlich aufgrund und im Rahmen ihrer Autonomie - insoweit freie Hand zu geben. Noch weniger ginge es an, die universitäre oder staatliche Wissenschaftsverwaltung im Einzelfall frei (oder gebunden an jedenfalls verfassungswidrige Regeln) bestimmen zu lassen, welche Folgerungen sie aus bestimmten Daten zieht. Es ist zu vermuten, daß genau das den Verantwortlichen vorschwebt.

Das Wissenschaftsministerium wird einwenden, daß in § 135 Abs. 3 SHG die Datenverarbeitung deswegen so unbestimmt geregelt sei, weil man die Datenerhebung und sonstige Datenverarbeitung im übrigen den einzelnen Fakultäten oder Universitäten zur selbständigen Entscheidung habe überlassen wollen, um eben die Freiheit von Lehre und Forschung nicht über Gebühr zu beeinträchtigen (vgl. § 108 Abs. 3 SHG). Dieses Argument mag im Verhältnis zwischen Staat und Fakultät berechtigt sein; es enthebt den Gesetzgeber aber nicht der Pflicht, gesetzlich festzulegen (und es enthebt die Universität nicht der Pflicht, durch Satzung festzulegen), welche Daten vom einzelnen Lehrer und Forscher selbst oder über ihn, also ihn betreffend, bei Dritten (Studenten) erhoben werden dürfen. Denn die Wissenschaftsfreiheit ist nicht allein Grundrecht der Universität (insoweit würde die jetzt gewählte Konstruktion in der Tat ausreichen), sondern sie ist Grundrecht der einzelnen Person, mithin des einzelnen Forschers und wissenschaftlichen Lehrers, so wie er auch das Grundrecht auf informationelle Selbstbestimmung persönlich genießt. Fakultäten oder Fachbereiche (in der DDR: Sektionen) haben kein Recht, allein über Umfang und Inhalt des Lehrangebots zu entscheiden, - so das Bundesverfassungsgericht (BVerfGE 67, 207 ff.). Ich ergänze, daß Inhalt und Form in der universitären Lehre nicht getrennt werden können.

Man könnte mir ferner entgegnen, es sei nicht von vornherein ein Eingriff in die Lehre, wenn Studenten nach ihrem Urteil über die Lehrveranstaltung eines Dozenten befragt würden. Das scheint nur auf den ersten Blick richtig. Denn jeder Umgang mit Daten durch öffentliche Stellen bedarf einer gesetzlichen Grundlage, die der Verfassung genügt. Jede autorisierte und nicht gänzlich unbeachtliche offizielle Datenverarbeitung über einen betroffenen Lehrenden muß einen Sinn (Zweck) haben. Sie hätte ihn nur dann, wenn sie geeignet wäre, in die Qualität von Lehre und Forschung "einzugreifen". Eine amtliche Datensammlung ist nicht erforderlich, um den Hochschullehrer zur freiwilligen Selbstkorrektur anzuregen; um die dazu nötigen Informationen kann er sich selbst kümmern, was ja auch häufig geschieht.

Der dritte - und intellektuell schwächste - Einwand lautet, dann könnten die Professoren ja machen, was sie wollten, und das auf Kosten des Steuerzahlers. Ja, so ist es. Die Verfassung will es so, und sie hat damit großen Erfolg: Um das Niveau der Universitäten werden wir von denen beneidet, die ihren Lehrbetrieb staatlich verordnen, die Lehrveranstaltungen überwachen und Gelder nur für Konformisten bereitstellen. DDR-Nostalgie ist hier wirklich nicht am Platz.

Zu beachten sind diese datenschutzrechtlichen und wissenschaftsrechtlichen Vorgaben auch im Hinblick auf die Vorformen des amtlichen Professoren-TÜV, nämlich die von Studenten privat organisierten Umfragen. Aus den genannten verfassungsrechtlichen Gründen dürfen universitäre oder staatliche Stellen solche Datensammlungen nicht zur Kenntnis nehmen und schon gar nicht, in welcher Form auch immer, auswerten. Auch für *solche* Datenverarbeitung fehlt jede Rechtsgrundlage.
Zwar kann die rein private Sammlung solcher Daten durch Studenten von Seiten der Universität wohl nicht unterbunden werden. Aber die Hochschule hat es zu unterlassen, studentischen Vereinigungen universitäre Einrichtungen (z. B. ein Schwarzes Brett oder eine Wand) zur Verfügung zu stellen, um diese Daten zu veröffentlichen. Denn das wäre die Beteiligung der Hochschule an einem Vorgang der Datenverarbeitung (Speicherung, Nutzung durch veröffentlichungsartige Bekanntgabe), und für diese fehlt es der Universität an der nötigen rechtlichen Erlaubnis (Ermächtigungsgrundlage).

Das Grundrecht des Art. 5 Abs. 3 GG wird einer Ermächtigung zu einer solchen Datenverarbeitung immer entgegenstehen: Eine derartige öffentliche Datenpräsentation, mit ggf. bloßstellender Wirkung für bestimmte Dozenten, wäre eine Form der mittelbaren Kontrolle von Forschung bzw. wissenschaftlicher Lehre durch die öffentliche Gewalt. Statt des freien - öffentlichen - wissenschaftlichen, auch hochschuldidaktischen, Diskurses über Lehrinhalte sowie Methoden der Lehre oder gar der Forschung fände ein *administrativ* veranstalteter, zumindest mitveranstalteter Diskurs statt, der in eine Darlegungsnot und einen Rechtfertigungsdruck führte, der von ganz anderer Art wäre als die Begründungslast, die jeder trägt, der an der freien wissenschaftlichen Diskussion teilnimmt.
Gerade ein solcher - zwar mittelbarer, aber womöglich um so wirksamerer - Druck auf die freie Lehre muß eben von Verfassungs wegen unterbleiben. Im Gegenteil haben wohl

Universität und staatliche Wissenschaftsverwaltung eher die Aufgabe, die Freiheit von Wissenschaft, Forschung und wissenschaftlicher Lehre zur Entfaltung zu bringen und zu diesem Zweck den Universitätslehrer gegen außerwissenschaftliche gesellschaftliche Einflüsse, die diesem subjektiv lästig zu sein haben und ihn objektiv behindern, abzuschirmen.
Die Frage nach der persönlichen Unvoreingenommenheit der Studenten und ihrem sonstigen Beurteilungsvermögen und damit der Validität der bei ihnen erhobenen Daten im Hinblick auf die Leistungen einzelner Universitätslehrer will ich gar nicht aufwerfen. Auch diese Frage stellt sich jedoch unter dem datenschutzrechtlichen Gesichtspunkt der Geeignetheit der Datenerhebung.
Ein weiteres: Jede Datenerhebung bei Dritten greift per se besonders tief in das Grundrecht auf informationelle Selbstbestimmung ein. Da bleibt, von seltenen gesetzlich genau geregelten und notwendigen Konstellationen (z. B. Polizei, Verfassungsschutz) abgesehen, ein Odium von Schnüffelei. Scherbengerichte haben in der Beurteilung von Gelehrten bekanntlich keine gute Tradition; die Beweisregeln der Inquisition scheinen mir geordneter gewesen zu sein als die heutzutage beliebten Befragungsverfahren vor der Verleihung der "Silbernen Zitrone" für den unbeliebtesten 'Proff'.
Die von mir oben geäußerte Vermutung übrigens, den Verantwortlichen schwebe vor, die Wissenschaftsverwaltung im Einzelfall bestimmen zu lassen, welche Folgerungen sie aus bestimmten über die Forschungs- bzw. Lehrtätigkeit erhobenen *inhaltlichen* Daten zieht, ist alles andere als eine grundlose Befürchtung. Hat doch Sachsens Wissenschaftsminister Meyer in einem autorisierten Interview in der Sächsischen Zeitung vom 22. Dezember 1994 auf die Frage, welche Konsequenzen ein schlecht beurteilter Professor zu erwarten habe, ausgeführt: "*Wenn es beispielsweise um die Verteilung der nicht gerade reichlich vorhandenen Gelder geht, um die Genehmigung freier Forschungssemester ohne Lehrpflicht oder um längere Dienstreisen, dann dürfen schlechte Noten für Professoren nicht unberücksichtigt bleiben.*"
Eine Rechtsgrundlage für derartige Eingriffe in die Wissenschaftsfreiheit durch Datensammlungen fehlt und läßt sich nach geltendem Verfassungsrecht auch nicht schaffen.

1.6 Gesundheitspolitik mit der Chipkarte

Die gesetzlichen Krankenkassen entdecken den Markt: Ab Januar 1996 hat jeder Pflichtversicherte die Auswahl, ob er der AOK, der BKK, der IKK oder einer Ersatzkasse (Barmer, DAK) beitritt. Alle rüsten zum Kampf um die Gunst der Patienten und um das Wohlwollen der Politiker. Die Marketingabteilung des Bundesverbandes der AOK hat der guten alten Krankenkasse nicht nur das neue Flair "Ihre Gesundheitskasse" verpaßt, sondern kümmert sich - gesetzlich zur Prävention verpflichtet - darum, wie die Kunden bei der Stange gehalten werden: Beratungs- und Auskunftsstellen (Stichworte "Gesundheitsförderung, Krankheitsverhütung") pflegen den Kontakt zum "bewußten Patienten".

Der AOK-Bezirksverband Leipzig will mit 600 000 Mitgliedern und 1 500 Vertragsärzten starten: Auf der "VitalCard", einer Prozessorchipkarte, speichern die behandelnden Ärzte

- individuell als Eingeber erkennbar - die wesentlichen Identifikations-, Präventions-, Indikations-, Diagnose-, Leistungs- und Therapiedaten des Patienten; er kann die Daten und ihren Verlauf bei Ärzten, in den Beratungsstellen der AOK und auf persönlichen Lesegeräten abrufen und hat sie so jederzeit zur Verfügung.

Die AOK betont derzeit, ihr sei nur an der Kenntnis der Präventionsdaten (Rückenschule, Ernährungs- und Suchtdisziplin, sportliche Aktivitäten etc.) gelegen. Allein die Kombination von Lesegerät und individueller Beratung läßt mehr vermuten.

Als weitere Vorteile nennt die AOK Verminderung des Leistungsmißbrauchs und von Doppelleistungen, gezielte ärztliche Beratung, rasche und richtige Notfallmedizin, vereinfachten Datenaustausch unter den behandelnden Ärzten und eine Stärkung des "mündigen Patienten", der aber, von der Ausnahme eigener ärztlicher Vorbildung abgesehen, mit den Daten wenig anfangen kann.

Auf die Idee von der Mündigkeit des Bürgers, des Patienten, lassen sich aufgeklärte Politiker und Werbestrategen besonders gern ein; wenn das noch mit "High-Tech" verbunden ist, dann gibt es kein Halten mehr: Projekte wie die Apotheker-Card, die Smart Card, die Systeme zur Erhebung von Autobahngebühren, ja sogar die weltfremde Idee von einer Asyl-Card ("ohne Karte keine Leistung") beweisen es.

Die AOK unterstreicht die Freiwilligkeit der Beteiligung. Das spricht aber gerade gegen die Eignung zum Kampf gegen Leistungsmißbrauch und Doppelleistungen; der Patient ohne Karte, mehr noch derjenige, der einzelne Leistungen nicht eintragen läßt, verschleiert sein Bild, er mißbraucht geschickter. Oder ist es doch so, daß man ohne Karte, ohne die Einwilligung zu jeder Eintragung, nun doch zum Patienten zweiter Klasse oder zum Verdächtigen des Leistungsmißbrauchs wird? Ist ein Arzt, der nicht lückenlos einträgt, ein Gebührenschneider? Welche praktischen Nachteile erleidet ein Arzt, der es generell oder im Einzelfall ablehnt, dem Patienten Diagnose- und Therapiedaten an die Hand zu geben und damit auch seine eigene Leistung dem Urteil unbekannter Kartenleser zu unterwerfen? Vom Lesen zum Speichern ist es nur ein kleiner Schritt.

Nur die informierte Einwilligung kann von Belang sein, sie setzt die genaue Belehrung des einzelnen und sein Verstehen der Kartenverwendung voraus. Hier wird der "mündige Bürger" zur Zauberformel: Der Patient, häufig alt, einsam, auch hilflos den modernen Zeiten und den freundlichen Helfern von der Gesundheitskasse anheimgegeben, soll entscheiden. Nur zu natürlich, daß diese Entscheidung situativ gefärbt ist.
Grundsätzlich darf die Versicherung nur fallbezogene Leistungsdaten zu Abrechnungs- und Statistikzwecken, jedoch keine personenbezogenen Diagnosedaten zur Kenntnis nehmen. Ist also - nach langem politischem Tauziehen - der Datenstrom abschließend geregelt, so ist kein Raum für "freiwillige" institutionalisierte Datenübermittlungen. Die AOK darf - anders als private Anbieter, denen Privatautonomie zusteht - nicht mit der Beliebigkeit, die die Mutter der Freiwilligkeit ist, den Kreis ihres gesetzlich fest umrissenen Auftrags erweitern.

Der Datenchip soll die "Kommunikation von Arzt zu Arzt erleichtern". Nur: Kommunikation findet nicht statt, vielmehr lediglich ein einseitiger Transport von Begriffen und Schlagworten. Diese Verkürzung führt dazu, daß der Sendearzt, der den Empfänger nicht kennt, sich auf möglichst Unverfängliches beschränkt, während die Gefahr besteht, daß der Empfängerarzt von der Validität, Aktualität und Klarheit der Daten ausgeht und fälschlich auf eigenständige Feststellungen verzichtet. Statt der notwendigen Qualitätsverbesserung der Daten wird der angeblich mündige, in Wahrheit mit Halbwissen versorgte Patient erzeugt und suggeriert, die ärztliche Kunst entspräche dem Niveau eines Beratungsgesprächs in der AOK.

Die VitalCard - wir sehen, der Name verrät vieles - gibt dem Patienten seine Krankheitsdaten (nein, es sind keine Gesundheitsdaten) in die Hand, obgleich unsere Rechtsordnung diese Daten seit altersher in ärztliche Obhut legt, wo sie gut geschützt sind. Der Versicherte unterliegt im täglichen Leben großem sozialem Druck zur Offenlegung dieser Daten. Ausländerbehörde, Sozialamt und Polizei sind an den Daten über Geschlechtskrankheiten, Suchtverhalten und Nervenleiden interessiert, aber auch Freundin, Ehefrau, Arbeitgeber: Ihrem liebenswürdigen Druck standzuhalten oder einzelne Felder für den Lesezugriff zu sperren fällt schwer; das Lesegerät kostet 170,- DM. Und selbst wenn gesetzliche Abfrage- und Leseverbote ergingen, der sublime Druck im sozialen Umfeld wächst um so mehr, denn das Lesen ist doch "Vertrauenssache".

Zur Notfallmedizin: Von der Schwierigkeit, überall Lesegeräte zur Hand zu haben, will ich nicht sprechen, auch nicht von Auslandsreisen und von der Obliegenheitsverletzung im Versicherungsfall, wenn die Karte nicht zur Hand ist. Jedenfalls ist unerfindlich, warum die wenigen Daten (Blutgruppe, Allergien, Impfdaten, Dauermedikation, Körperersatzstücke) der komplizierten Chiptechnik bedürfen. Hier hilft viel besser der (mittlerweile EU-genormte) Notfallpaß.

Und schließlich ist noch die Weiterentwicklung zu bedenken und damit die Machtfrage zu stellen: Die Erfahrung lehrt, daß vorhandene Datensammlungen leicht anderen Zwecken dienstbar gemacht werden. Es liegt nicht fern, die Begehrlichkeit der Versicherer zu befriedigen: Im Interesse der Kostendämpfung werden die Patienten dann bestimmten Risiko- und Verhaltensgruppen zugeordnet; Bonuspunkte winken. Ärzte können nach Abrechnungslauterkeit, Verordnungsverhalten, Diagnosefestigkeit und Erfolg beurteilt werden. Patienten wollen gesund bleiben oder wieder werden, Ärzte helfen (angeblich nur) für's liebe Geld, das die Versicherer solidarisch bezahlen. Wenn nun Patienten und Beratungsstellen mit der Chipkarte - und dies muß im Hinterkopf die Absicht der Versicherer sein - die Ärzte auf Sparsamkeit kontrollieren sollen, so kann die Grundlage aller ärztlichen Kunst, nämlich das persönliche Vertrauensverhältnis (man denke an das Hausarztprinzip), nicht mehr entwickelt werden. Dies führt zwangsläufig zur Verflüchtigung des ärztlichen Berufsethos. Die Chipkarte bewirkt Mißtrauen, Mißverständnisse und den intelligenten, das heißt eigensüchtigen Umgang mit der Karte durch jeden Beteiligten, auf Kosten der beiden anderen.

Kostendämpfung geht im Prinzip nur so: Sozial gerechte Kostenbeteiligung, überhaupt auf das Notwendige begrenzte Solidarität tarieren das System.

Die Subsidiarität ist intelligenter als der Chip.

Chipkarten dürfen im Gesundheitswesen immer dann eingesetzt werden, wenn der Patient nicht zum "Datenträger" wird. Er geht ja nicht in erster Linie zum Arzt, weil er seine Daten kennen will, sondern weil er krank ist und der Arzt ihm helfen soll. Die Daten des Patienten, die der Arzt erhebt, gehören dem Arzt! Der Patient hat allerdings grundsätzlich das Recht, die ihn betreffenden Daten kennenzulernen. Würden die Daten jedoch dem Patienten generell und institutionalisiert übergeben, so würde nicht der Arzt, sondern der Patient "Herr der Daten". Sie könnten von ihm abgefordert, bei ihm beschlagnahmt werden. Anstelle des uralten und sozial akzeptierten Arztgeheimnisses hätten wir das rechtlich ungeschützte und damit offene Patientendatum.

Ferner sind Chipkarten unbedenklich, wenn die Versicherungsunternehmen keinen Zugriff erhalten. § 295 SGB V sichert nach langem Tauziehen im Gesetzgebungsverfahren den Grundsatz, daß dem Versicherer Abrechnungsdaten nicht patientenbezogen zugänglich sind.

Es bleiben nach meiner Meinung daher für patientenbezogene Chipkarten u. a. folgende Bereiche:

- Chipkarten für Diabetiker, Dialysepatienten oder andere Personen, die bei der verantwortlichen und informierten Selbstkontrolle auf die Kenntnis aktueller Daten und ihrer Verläufe angewiesen sind.
- Abrechnungschipkarten zum Datentransfer zwischen Ärzten und privaten oder öffentlichen Abrechnungsstellen
- Chipkarten im Datenverkehr zwischen Hausarzt und Spezialisten
- Chipkarten im Datenverkehr von Krankenhausinformationssystemen
- Chipkarten im Datenverkehr zwischen Arzt und Labor, zwischen Zahnarzt und Techniker.

Die Diskussion ist insgesamt technisch (ist die Chipkarte nur eine Vorstufe zur Vernetzung?) und rechtlich noch offen. Die Datenschutzbeauftragten werden dazu recht bald weitere Vorstellungen entwickeln.
Ich appelliere an Ärzte und Patienten im Bezirk der AOK Leipzig, sich an dem "Großversuch" der AOK, der in Wahrheit ein Werbegag ist und die vorgenannten Probleme nicht bedacht hat, *nicht* zu beteiligen.

1.7 Die Pflegeversicherung als Wachsamkeitslücke?

Ein anderer Fall, in dem man es zu Lasten des Persönlichkeitsschutzes, also der Menschenwürde, unterläßt, die staatlich verordnete Solidargemeinschaft auf das Maß des

Erforderlichen zu beschränken, ist die Einführung der Pflegeversicherung, die - wenn man sich dafür entschieden hat, unvermeidlich - zur Verarbeitung sehr intimer Daten führt (dazu näher unten 10.2.2): Ich halte die Datenerhebung und den außerärztlichen Umgang mit den Daten der Pflegebedürftigen in der Pflegeversicherung für schlimm.

Es gibt bei uns hauptamtlichen Datenschützern kleine Wachsamkeitslücken (jemand, der genug Abstand und Überblick hat, sollte sie einmal untersuchen!). Die Pflegeversicherung scheint sich des Umstandes zu erfreuen, gerade in einer solchen Wachsamkeitslücke plaziert zu sein. Man hat, dies muß ich selbstkritisch anmerken, von uns Datenschützern im Laufe der langwierigen Auseinandersetzungen um die Pflegeversicherung nicht viel gehört. Datenschutz(recht) darf sich nicht zu schade sein, zur Früherkennung der Hypertrophie, d. h. der Überbeanspruchung des Sozialstaats beizutragen.

2 Parlament; Rechnungshof

Datenschutzkontrolle bei den Rechnungsprüfungsbehörden

Anläßlich der Beratungen zum Entwurf einer bundesweit geltenden Steuerdaten-Abruf-Verordung war unter den Datenschutzbeauftragten des Bundes und der Länder zu klären, ob Rechnungsprüfungsbehörden bei ihrer Prüftätigkeit der Kontrolle der Datenschutzbeauftragten unterliegen.

In Sachsen ist die Rechtslage folgendermaßen zu beurteilen:

Als oberste Landesbehörde fällt der Sächsische Rechnungshof in den Anwendungsbereich des Sächsischen Datenschutzgesetzes nach § 2 Abs. 1 SächsDSG. Dabei wird der Rechnungshof nicht von meiner grundsätzlichen Kontrollzuständigkeit ausgenommen: Nach § 24 Abs. 1 SächsDSG erfolgt eine Einschränkung lediglich für die Gerichte. Diese unterliegen meiner Kontrolle nur, soweit sie in Justizverwaltungsangelegenheiten tätig werden (vgl. § 24 Abs. 2 SächsDSG, siehe auch 1. Tätigkeitsbericht, 8.1).
Zu beachten ist jedoch, daß nach Art. 100 Abs. 2 der Sächsischen Verfassung die Mitglieder des Rechnungshofes die gleiche Unabhängigkeit wie die Richter besitzen. Daraus folgt, daß ihre unabhängige Prüftätigkeit nicht meiner Kontrolle unterliegt. Soweit der Rechnungshof aber im Rahmen seiner Verwaltungstätigkeit personenbezogene Daten verarbeitet (z. B. Personaldatenverarbeitung), unterliegt er allerdings meiner Kontrolle.

Die besondere Regelung zur Kontrollbefugnis läßt jedoch die Verpflichtung des Rechnungshofes unberührt, bei seinen sämtlichen personenbezogenen Datenverarbeitungsvorgängen die datenschutzrechtlichen Vorschriften zu beachten. Ich habe die Überzeugung, daß dies geschieht.

3 Europäische Union / Europäische Gemeinschaften

3.1 EU-Richtlinie zum Datenschutz

Die Beratungen des Ministerrats der EU in seiner Arbeitsgruppe für Wirtschaftsfragen sind mit der Feststellung eines Gemeinsamen Standpunkts vom 15. Februar 1995 abgeschlossen worden. Als eine künftige gemeinsame Richtlinie des Europäischen Parlaments und des Rates ist der erarbeitete Text dem Europäischen Parlament vorgelegt worden.

Mit dem Gemeinsamen Standpunkt zeichnet sich ab, daß das deutsche Datenschutzrecht nicht grundlegend umgestaltet werden muß. So wird im nicht-öffentlichen Bereich die Selbstkontrolle durch betriebliche Datenschutzbeauftragte nach den §§ 36 f. BDSG auch nach Erlaß der Richtlinie Bestand haben dürfen. Damit kann zugleich eine Dateien-Meldepflicht entfallen. Nach meiner Auffassung ersetzt Selbstkontrolle jedoch nicht die staatliche Aufsicht.

Bei den Beratungen war zentrales Problem, ob die Mitgliedsstaaten in ihrem Datenschutzrecht ein höheres Schutzniveau schaffen dürfen, als es die Richtlinie vorsieht. Das einzelstaatliche Recht kann "allgemeine Bedingungen für die Rechtmäßigkeit der Verarbeitung" festlegen, wobei in der Tendenz eine "Verbesserung" des gegenwärtigen Schutzes anzustreben ist. Im Rahmen ihres nationalen "Spielraums" wird den Mitgliedsstaaten jedoch die "Beachtung des Gemeinschaftsrechts" auferlegt - ein klares Indiz dafür, daß die Richtlinie - nur für internationalen Datentransfer - die obere Grenze des Schutzniveaus vorgibt; so jedenfalls wird sie von den deutschen Datenschutzbeauftragten interpretiert.

Wird die Richtlinie durch das Europäische Parlament angenommen, erlassen die Mitgliedsstaaten innerhalb von drei Jahren die erforderlichen Rechts- und Verwaltungsvorschriften. Für den Fall, daß sich die Verabschiedung wegen des Beitritts weiterer Länder hinauszögern sollte, werden allerdings weitere - zeitintensive - Abstimmungsberatungen unvermeidlich sein.

Die Beratungen zur ISDN-Richtlinie des Europäischen Parlaments und des Rates wurden - getrennt von der EG-Datenschutzrichtlinie - fortgesetzt. Inzwischen liegt ein geänderter Vorschlag der EG-Kommission vom 14. Juni 1994 vor. Es ist zu wünschen, daß bei den weiteren Beratungen die ISDN-Richtlinie auf die EG-Datenschutzrichtlinie abgestimmt wird.

3.2 Entwurf einer EG-Statistik-Verordnung

Die EU-Kommission hat im Jahre 1994 den Entwurf einer EG-Statistik-Verordnung vorgelegt (BR-DS 283/94 vom 31. März 1994). Das Regelwerk soll, gewissermaßen als

Gegenstück zum Bundesstatistikgesetz, die allgemeinen, für sämtliche EU-Statistiken geltenden Vorschriften enthalten.

Gegen den Entwurf sind schwerwiegende datenschutzrechtliche Einwände zu erheben. Ich war an den Bemühungen der Datenschutzbeauftragten des Bundes und der Länder beteiligt, diese Einwände im einzelnen auszuarbeiten. Ergebnis war die aus Abschnitt 16.2.17 ersichtliche Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom August 1994, auf die wegen der Einzelheiten hier verwiesen wird. Erfreulicherweise stehen die deutschen Datenschützer nicht allein: Auch der Bundesrat hat, und zwar schon mit Beschluß vom 8. Juli 1994 (zu BR-DS 283/94) mit Nachdruck eine große Zahl detaillierter Verbesserungswünsche zugunsten des Datenschutzes geltend gemacht. Von der Bundesregierung muß erwartet werden, daß sie nach Kräften zu verhindern sucht, daß das EU-Statistik-Wesen zu einer offenen Flanke des Datenschutzes in der EU wird.

Auch auf die strikte Einhaltung der für das Statistische Amt der EU (EUROSTAT oder SAEG genannt) geschaffenen Regeln der VO (EURATOM, EWG) Nr. 1588/90 des Rates der EG vom 11. Juni 1990 über die Übermittlung von unter die Geheimhaltungspflicht fallenden Informationen an das Statistische Amt der EU - kurz EUROSTAT-VO genannt - sollte von deutscher Seite aus geachtet werden.

4 Medien

Anforderungen an den Persönlichkeitsschutz im Medienbereich

Redaktionen der Presse, des Rundfunks, Films und Fernsehens nutzen immer mehr modernste Informations- und Kommunikationstechnik, z. B. optische Speicher, Multimediatechniken und neue Datennetze. Die neuen Möglichkeiten des elektronischen Publizierens in Netzen, interaktive Dienstleistungen des Fernsehens, der Zugriff auf elektronisch gespeicherte Pressearchive und deren Auswertungsmöglichkeiten gefährden den Einzelnen bei der Ausübung seines Rechts auf informationelle Selbstbestimmung. Diesen qualitativ neuen Gefährdungen muß der Datenschutz auf rechtlicher und technisch-organisatorischer Ebene angemessen begegnen. Auch darf z. B. der Bericht über eine Gerichtsverhandlung mit den modernen Techniken der Berichterstattung durch Hörfunk und Fernsehen nicht zu einem massenmedialen "modernen Pranger" der Angeklagten, der Opfer oder Zeugen werden.

Auf damit zusammenhängende neue Probleme macht die 49. Konferenz der Datenschutzbeauftragten des Bundes und der Länder mit ihrer Entschließung "Anforderungen an den Persönlichkeitsschutz im Medienbereich" (siehe 16.2.9) aufmerksam.

Entsprechend meinem Vorschlag werden diese Anforderungen dem bundesweit einflußreichen Deutschen Presserat zur Kenntnis gegeben.

5 Inneres

5.1 Personalwesen

5.1.1 Anwendbarkeit der Verwaltungsvorschrift des SMI über die Führung und Verwaltung von Personalakten für Beamte auch auf Arbeiter und Angestellte? Verbindlichkeit der Verwaltungsvorschrift auch für den Kommunalbereich?

Verwaltungsvorschriften sind keine Rechtsvorschriften, sie sind zwar behördenintern verbindlich, regeln aber nicht die Rechtsverhältnisse der Betroffenen.
Die Verwaltungsvorschrift des SMI ist aufgrund von § 160 SächsBG erlassen worden und gilt - rein rechtlich - nur für Beamte. Immer wieder werde ich von öffentlichen Stellen gefragt, ob und wieweit diese Verwaltungsvorschrift auch für die Personalaktenführung der Arbeiter und Angestellten gilt und ob sie für den Kommunalbereich verbindlich ist.

In meiner Stellungnahme zu dem Entwurf der Verwaltungsvorschrift (siehe auch 2. Tätigkeitsbericht, 5.1.1) hatte ich angeregt, den Anwendungsbereich der Verwaltungsvorschrift unter Beteiligung des SMF auf alle Beschäftigten des öffentlichen Dienstes auszudehnen und die - wenn auch wenigen - Punkte herauszustellen, die einen differenzierten Umgang mit den Personalakten erfordern. Leider hat das SMI diesen Vorschlag nicht aufgegriffen.

Nach meinem Dafürhalten kann für den Umgang mit den Personalakten der Arbeiter und Angestellten im öffentlichen Dienst die analoge Anwendung der Verwaltungsvorschrift allenfalls empfohlen werden. Dabei sollte stets bedacht werden, daß die Anwendung beamtenrechtlicher Regelungen bei Arbeitnehmern zu Problemen führen kann, und zwar aus folgenden Gründen:

Da die Tarifverträge (bis auf das Akteneinsichtsrecht) und die allgemeinen Vorschriften des Arbeitsrechts keine Regelungen für den Umgang mit den Personalakten von Arbeitern und Angestellten im öffentlichen Dienst enthalten, ist das Sächsische Datenschutzgesetz als Auffanggesetz anzuwenden (§ 2 Abs. 4 SächsDSG). Insbesondere § 31 SächsDSG, der die Personaldatenverarbeitung für Bewerber und Beschäftigte im öffentlichen Dienst regelt, führt in einigen Punkten zu einem anderen Ergebnis als die Anwendung des Sächsischen Beamtengesetzes (z. B. bei der Weitergabe von Personalaktendaten an Dritte, Akteneinsichtsrecht nach Beendigung des Arbeitsverhältnisses). Auch die Aufbewahrungsfrist für Personalakten ist bei Beamten an die grundsätzlich anders gestaltete Beamtenversorgung geknüpft und kann nicht ohne weiteres auf die Personalakten der übrigen Beschäftigten übertragen werden.

Ich habe die Problematik dem für den Tarifbereich zuständigen SMF vorgetragen und den Handlungsbedarf verdeutlicht. Das SMF hat daraufhin für den *eigenen* Geschäftsbereich eine Verwaltungsvorschrift erlassen, in der die Personalaktenführung einheitlich für die Arbeiter, Angestellten und Beamten (nicht unbedingt zufriedenstellend) geregelt wird.

Weiter kann im Hinblick auf das verfassungsrechtlich garantierte Selbstverwaltungsrecht der Gemeinden, der Landkreise und der anderen Gemeindeverbände (Art. 28 Abs. 2 GG, Art. 82 Abs. 2 SächsVerf) nicht per se angenommen werden, daß die Verwaltungsvorschrift für die Personalaktenführung auch in diesem Bereich gilt. Die Anwendung der Verwaltungsvorschrift steht den Kommunen daher frei. Jedenfalls müssen die Gemeinden jedoch die Rechtsvorschriften (Verfassung, formelle Gesetze, Rechtsverordnungen, allgemeinverbindlich erklärte Tarifverträge, eigene Satzungen) einhalten.

Ich werde die Angelegenheit weiterverfolgen.

5.1.2 Rechtsverordnung der Staatsregierung über den Arbeitsschutz für jugendliche Beamte

Das SMI hat mir Gelegenheit zur Stellungnahme zu dem Verordnungsentwurf gegeben, in dem neben Regelungen zur Arbeitszeit, zum Unterrichtsbesuch, zu Ruhepausen, zum Schichtdienst und zur täglichen Freizeit auch Vorschriften über ärztliche Untersuchungen (Inhalt und Durchführung, Kosten, Mitteilung an die Ernennungsbehörde, Information der Personensorgeberechtigten) vorgesehen sind. Schwerpunkt meiner Stellungnahme waren die ärztlichen Untersuchungen. Unter anderem habe ich angeregt, die Ergebnisse der ärztlichen Untersuchung nicht nur der Beschäftigungsbehörde und den Personensorgeberechtigten zuzuleiten, sondern auch dem jugendlichen Beamten selbst. Denn zum Recht auf informationelle Selbstbestimmung gehört auch, daß der Betroffene *unmittelbar* und nicht über den Umweg seiner Eltern Kenntnis von Daten erhält, die ihn ganz persönlich und sein Dienstverhältnis betreffen. Hinzu kommt, daß die Mitteilung Bestandteil der Personalakte sein muß, die dem uneingeschränkten Einsichtsrecht des Beamten unterliegt (§ 120 Abs. 1 SächsBG).

Im Hinblick auf *freiwillige Nachuntersuchungen* habe ich gefordert klarzustellen, daß mit Ausnahme der Fälle des § 6 Abs. 2 Satz 2 SächsGDG (Abwehr einer Gefahr für Leben und Gesundheit Dritter) die Ergebnisse nur *mit Einwilligung* des Betroffenen an die Beschäftigungsbehörde und die Personensorgeberechtigten weitergegeben werden dürfen. Ein Betroffener, der bereits Beamter ist, ist sicher auch fähig, die Tragweite seiner Einwilligung abzuschätzen.

Das SMI hat signalisiert, daß meine Vorschläge umgesetzt werden. Die Verordnung wird voraussichtlich im ersten Quartal 1995 in Kraft treten.

5.1.3 Verwaltungsvorschrift des SMI zur Begründung und Beendigung des Beamtenverhältnisses; Frage nach anhängigen Strafverfahren

Die Verwaltungsvorschrift sieht die Frage nach laufenden Ermittlungsverfahren und noch nicht abgeschlossenen Straf- oder Disziplinarverfahren vor. Dies habe ich kritisiert:

Häufig weiß man nicht, daß ein Ermittlungsverfahren anhängig ist. Aber selbst wenn man es weiß, verbietet die Unschuldsvermutung, nach der jeder Mensch bis zum gesetzlichen

Nachweis seiner Schuld als unschuldig gilt (Art. 20 Abs. 3 sowie Art. 2 Abs. 1 GG und Art. 6 Abs. 2 Europäische Menschenrechtskonvention), eine derartige Frage. Denn wenn sie bejaht würde, dürfte die Antwort unter rechtsstaatlichen Gesichtspunkten keinen Einfluß auf die Einstellungsentscheidung haben, weil der gleiche Zugang zu einem öffentlichen Amt gemäß Art. 33 Abs. 2 GG, Art. 91 Abs. 2 SächsVerf als Grundrecht nur durch *rechtsstaatlich gesicherte* Feststellungen eingeschränkt werden darf.

Das SMI widersprach dieser Rechtsauffassung mit der - leider oberflächlichen - Begründung, eine Einstellungsentscheidung beruhe im Hinblick auf die vom Bewerber künftig zu erfüllenden Amtspflichten auch auf einer günstigen Prognose über die charakterliche Eignung. Die umfassende Prüfung dieser Eignung müsse die Gesamtpersönlichkeit berücksichtigen und daher auch die Frage nach anhängigen Ermittlungs- oder Strafverfahren zulassen. Soweit ein Bewerber eine diesbezügliche Frage bejahe, müsse damit nicht zwangsläufig eine Ablehnung verbunden sein, denn nicht jedes *negative* Kriterium reiche aus, die Eignung in Frage zu stellen. Vielmehr bleibe es dem pflichtgemäßen Ermessen des Dienstherrn überlassen, welches Gewicht er einem eingeleiteten Ermittlungs- bzw. anhängigen Straf- oder Disziplinarverfahren bei seiner Auswahlentscheidung zumesse.

Das SMI verkennt dabei jedoch, daß die Unschuldsvermutung auf Art. 2 Abs. 1 GG basiert und damit nach dem Rechtsstaatprinzip *Verfassungsrang* hat, und zwar mit allen Konsequenzen für die Verwaltung als vollziehende Gewalt, die an die Grundrechte als unmittelbar geltendes Recht gebunden ist (Art. 1 Abs. 3 GG, Art. 36 SächsVerf). Ein offenes Verfahren hat daher bei der Prognose über die charakterliche Eignung eines Bewerbers außer Betracht zu bleiben, weil es *kein* Eignungskriterium ist, *erst recht kein negatives*. Für eine Ermessensentscheidung bleibt kein Raum, weil keine Erkenntnisse über einen gesicherten Sachverhalt vorliegen. Diesen Grundsatz sollte jeder Jurist kennen! Und wie will man denn das Gewicht der vorläufigen Ermittlungen prüfen, wenn man die Akten nicht kennt? Zur Anforderung der Akte besteht aber keine gesetzliche Grundlage. Die Praxis sieht doch so aus, daß der Bewerber keine Chance hat, wenn er die Frage bejaht, die Vorwürfe schildert und sie zu widerlegen versucht. Solche Bewerbungen werden "zuunterst" gelegt ...

In Anbetracht dessen, daß etwa zwei Drittel der staatsanwaltlichen Ermittlungsverfahren eingestellt werden und es vor Gericht immer wieder Freisprüche gibt, kann ich nicht nachvollziehen, wie ein noch offenes Verfahren eine Prognose zum Charakter eines Menschen ermöglichen soll. Eine ernsthafte Auseinandersetzung mit dieser Frage vermisse ich in der Antwort des SMI. Ich halte deshalb an meiner Forderung fest, die Frage nach laufenden Ermittlungs- sowie anhängigen Straf- oder Disziplinarverfahren zu unterlassen, und fordere das SMI auf, sich zu neuen und verfassungsrechtlich orientierten Überlegungen aufzuraffen.

5.1.4 Datenschutz im Vorfeld von Konkurrentenklagen

Bei anstehenden Beförderungen bewerben sich häufig mehrere Beamte um die Stelle. Hat sich die Behörde für die Beförderung eines Beamten entschieden, können die Mitbewerber versuchen, die möglicherweise gegen Art. 33 Abs. 2 GG (gleicher Zugang zum öffentlichen Amt) verstoßende bevorstehende Ernennung des Beamten gerichtlich zu verhindern (sogenannte "Konkurrentenklage"), um selbst zum Zuge zu kommen. Eine bereits *erfolgte* Beförderung läßt sich aus beamtenrechtlichen Gründen nicht mehr rückgängig machen.

Eine personalaktenführende Stelle fragte, ob sie den "unterlegenen" Bewerbern *vor* Erheben einer Konkurrentenklage Einsicht in die Personalakte des bevorzugten Mitbewerbers (oder zumindest Auskunft hieraus) geben darf. Die Frage habe ich wie folgt beantwortet:

Ein Akteneinsichtsrecht nach § 29 VwVfG besteht nicht. Die Vorschrift gewährt zwar den an einem Verwaltungsverfahren Beteiligten ein Einsichtsrecht in die das Verfahren betreffenden Akten, sie wird aber durch den spezielleren § 121 SächsBG verdrängt (vgl. § 1 Abs. 1 VwVfG). Nach § 121 Abs. 2, 2. Fall SächsBG dürfen Auskünfte aus der Personalakte an Dritte (keine Aktenvorlage!) ohne Einwilligung des Beamten nur gegeben werden, wenn dies der Schutz berechtigter, höherrangiger Interessen des Dritten zwingend *erfordert*.

Dies ist bei Anträgen auf Auskunft aus der Personalakte des bevorzugten Beamten im Vorfeld einer Konkurrentenklage nicht der Fall:

Die Mitbewerber *benötigen* die Auskunft aus der Personalakte nicht, um die bevorstehende Ernennung des ausgewählten Bewerbers gerichtlich überprüfen lassen zu können. Hierzu brauchen sie lediglich den Namen des bevorzugten Beamten zu kennen (vgl. BVerfG NJW 1990, 501). Auch aus dem Grundrecht auf einen *effektiv* zu gewährleistenden Rechtsschutz (vgl. Art. 19 Abs. 4 GG) läßt sich kein Auskunftsanspruch der Mitbewerber herleiten. Aus diesem Grundrecht folgt lediglich die Pflicht der Behörde, schriftlich (anhand der aus Art. 33 Abs. 2 GG ersichtlichen Kriterien) festzulegen, warum sie einen Bewerber bevorzugt hat, damit *im Gerichtsverfahren* eine sachgerechte Überprüfung der Entscheidung möglich ist. Die Übermittlung von Personalaktendaten ist daher auch unter Berücksichtigung des Grundrechts auf einen effektiv zu gewährleistenden Rechtsschutz im Vorfeld einer Konkurrentenklage nicht erforderlich und daher unzulässig.

5.1.5 Unzulässige Datenerhebung im Förderschulbereich

Im Förderschulbereich wurden im Hinblick auf angeblich anstehende Bedarfskündigungen Datenerhebungen zur Sozialauswahl durchgeführt, und zwar im *Februar/März 1994*. Sie wurden mit einem zum damaligen Zeitpunkt vorliegenden *Referentenentwurf* für ein Gesetz zur Änderung des Schulgesetzes gerechtfertigt. Die Argumentation war nicht nachzuvollziehen, weil der Entwurf vorsah, daß das im Dienst des Freistaates Sachsen stehende medizinisch-therapeutische Personal (Betreuungspersonal) kraft Ge-

setzes zum *1. August 1995 (!)* in den Dienst der kommunalen oder freien Schulträger übergehen sollte - also *ohne Kündigung*.

Auch wenn sich abzeichnete, daß die künftigen Träger mit der Übernahme des gesamten Betreuungspersonals finanziell überfordert sein würden und deshalb nur ein reduzierter Personalbestand übergeben werden sollte, fehlte eine Grundlage für Bedarfskündigungen. Es war unklar, ob überhaupt durch den Freistaat Sachsen, und wenn ja, bis wann und in welchem Umfang zu kündigen sein würde. Ich habe deshalb die weitere Aufbewahrung der erhobenen Daten als unzulässige Vorratsdatenspeicherung gewertet. Wie zutreffend meine Einschätzung der Rechtslage war, zeigt, daß - allerdings erst im Dezember 1994 - eine interministerielle Arbeitsgruppe "Personalschlüssel" für die unterschiedlichen Arten der Förderschulen (Verhältnis Förderschüler zu Betreuungspersonal) zur Ermittlung des Personalüberhangs vorgelegt hat. Auf dieser Grundlage soll nunmehr der Personalabbau beginnen. Ich werde weiterverfolgen, in welcher Form dies geschieht.

Außerdem habe ich beanstandet, daß die *fach*aufsichtsführenden Schulräte, und damit Personen außerhalb der personalverwaltenden Oberschulämter, die Daten erhoben haben. Die zu diesem Zweck den Schulräten ausgehändigten Formblätter, die inhaltlich wie Fragebogen aufgebaut waren und die wesentlichen Personalaktendaten der Betroffenen enthielten, hätten die Betroffenen ebensogut selbst ausfüllen und den Oberschulämtern zurücksenden können. Dies wäre nicht nur eine datenschutzgerechte, sondern auch eine verwaltungsökonomische Variante gewesen.

Auch wenn das SMK meiner datenschutzrechtlichen Beurteilung widersprach, hat es dennoch die Vernichtung der Unterlagen veranlaßt.

5.1.6 Unsicherheit bei der Anwendung des § 121 SächsBG (Auskünfte aus Personalakten an Dritte)

Wiederholt haben mich Anfragen zur Auslegung von § 121 SächsBG erreicht. Zweifelhaft war, ob dort die Auskunft aus Personalakten und die Einsicht in Personalakten *abschließend* geregelt ist oder ob andere Spezialgesetze des Landes oder des Bundes bei fehlender Einwilligung des Beamten ein *vorrangiges* Einsichts- bzw. Auskunftsrecht begründen (z. B. Sächsisches Verfassungsschutzgesetz bzw. Bundesverfassungsschutzgesetz, Sächsisches Petitionsausschußgesetz, Sächsisches Untersuchungsausschußgesetz).

Nach Nr. 5.2 Abs. 1 letzter Satz der *Verwaltungsvorschrift des SMI über die Führung und Verwaltung von Personalakten* vom 4. November 1993 bleiben die Erteilung von Auskünften oder die Vorlage von Personalakten aufgrund anderer gesetzlicher Vorschriften unberührt. Ich teile diese Auffassung des SMI, halte aber im Hinblick auf die vom Bundesverfassungsgericht im Volkszählungsurteil vom 15. Dezember 1983 (BVerfGE 65, S. 1, NJW 1984, S. 419) aufgestellten Grundsätze, wonach personenbezogene Daten nur durch oder aufgrund *normenklarer Gesetze* verarbeitet werden dürfen, eine entsprechende Klarstellung in § 121 SächsBG für erforderlich.

Es bleibt abzuwarten, ob das SMI für eine Modifizierung des § 121 SächsBG sorgt.

5.1.7 Behandlung von Personalakten aus DDR-Zeiten (Kaderakten)

Häufig haben sich öffentliche Stellen bei mir nach der Behandlung der aus DDR-Zeiten vorhandenen Personalakten (Kaderakten) für übernommene Beschäftigte erkundigt. Ihnen war unklar, ob und gegebenenfalls wieweit sie unter Berücksichtigung datenschutz-, archiv- und personalaktenrechtlicher Vorschriften in die neu angelegten Personalakten zu integrieren sind. Dabei habe ich von ganz unterschiedlichen Handhabungen in den öffentlichen Stellen erfahren: Einige nahmen vollständige Kaderakten - verschlossen oder auch unverschlossen - zur Personalakte. Andere haben der Personalakte nur die mit dem derzeitigen Dienst- oder Arbeitsverhältnis in Zusammenhang stehenden Unterlagen aus der Kaderakte beigefügt (z. B. Zeugnisse, Qualifikations- und Beschäftigungsnachweise). Auch wurden Kaderakten unter Hinweis auf § 35 Abs. 2 SächsDSG als Altdaten unter Verschluß gehalten und Akteneinsicht nur nach vorheriger Zustimmung des SMI gewährt.

Dies war für mich Anlaß, dem SMI die Gesamtproblematik darzustellen, die insbesondere darin besteht, Datenschutz-, Archiv- und Personalaktenrecht in Einklang zu bringen. Mein Ziel war es, die Rechtslage zu klären und für Sachsen eine einheitliche Behandlung der Kaderakten zu erreichen.

Mit dem SMI kam ich zu dem Ergebnis, daß das Personalaktenrecht im Verhältnis zu den datenschutz- und archivrechtlichen Bestimmungen lex specialis ist. Danach muß von einer einheitlichen, also durchgehend geführten Personalakte ausgegangen werden, die das Beschäftigungsverhältnis sowohl vor als auch nach der Wiedervereinigung umfaßt. Denn laut Einigungsvertrag endete ein Beschäftigungsverhältnis damit nicht automatisch. Die Personalunterlagen dienen dazu, den gesamten beruflichen Werdegang eines Mitarbeiters aufzuzeichnen, was sich insbesondere in dem Grundsatz "Vollständigkeit und Richtigkeit der Personalakten" widerspiegelt.

Der Inhalt der Kaderakte hat weiterhin inhaltliche und rechtliche Bezüge zum Beschäftigungsverhältnis. Wesentlich sind jedenfalls alle Unterlagen, aus denen Stasi-Belastung oder Systemnähe abgeleitet werden können. Nach wie vor halte ich - aus Gründen der Wahrheit und Vollständigkeit der Personalakte - daran fest, daß die "Bereinigungsaktion" unter Modrow (auch nach der damaligen Rechtslage) Unrecht war. Folglich ist jeder Bedienstete verpflichtet, die damals entnommenen Aktenteile beizubringen. Ich weiß, daß diese Pflicht nicht durchgesetzt werden kann; dies ändert nichts daran, daß sie besteht.

§ 35 SächsDSG (Altdaten-Regelung) ist nicht einschlägig, da diese Bestimmung nur die sichere Aufbewahrung alter, für die rechtmäßige Aufgabenerfüllung der Verwaltung nicht mehr benötigter Unterlagen sicherstellen will.

Allerdings sollten Kaderakten wie die Alt-Personalakten eines früheren Arbeitgebers bzw. Dienstherrn für sich geheftet bleiben und als *verschlossen* geführte Teilakte behandelt werden.

5.1.8 Datenschutzrechtliche Kontrolle der Personalverwaltung für die Lehrer im Oberschulamt

Bei einer Kontrolle der Personalverwaltung der Lehrer in einem Oberschulamt habe ich folgendes festgestellt:

Der *interne Datenschutzbeauftragte* war lediglich mündlich bestellt worden, seine Befugnisse waren unklar. Außerdem war er weder im Geschäftsverteilungsplan noch im Telefonverzeichnis erwähnt. Damit er seine Funktion effektiv ausfüllen kann, habe ich gefordert, seine Befugnisse schriftlich festzulegen.

Das *Dateienverzeichnis* war unvollständig und daher ergänzungsbedürftig.

Wegen des umfangreichen Bestands von ca. 18 000 Personalakten habe ich ein *technisch-organisatorisches Datensicherheitskonzept* für unerläßlich gehalten. Die wenigen vorgesehenen Maßnahmen zur Gewährleistung der Datensicherheit waren unzureichend.

Die *Vernichtung von Schriftstücken* mit personenbezogenen Daten (z. B. überarbeitete Entwürfe) war nicht geregelt. Meist wurden sie gesammelt und sporadisch zum Reißwolf gegeben. Ich habe deshalb eine verbindliche Regelung gefordert (keine Entsorgung über den Papierkorb, Aufbewahrung bis zur Vernichtung entsprechend den für Personalakten geltenden Sicherheitsmaßnahmen).

Bei der *Personalaktenführung* wendet das Oberschulamt - obwohl kaum Beamte beschäftigt werden - die *Verwaltungsvorschrift des Sächsischen Staatsministeriums des Innern über die Führung und Verwaltung von Personalakten* an. Diese basiert auf beamtenrechtlichen Vorschriften. Ich habe auf die Problematik bei der Anwendung im Angestelltenbereich hingewiesen, da dies zum Beispiel bei Datenübermittlungen an Dritte zu rechtsfehlerhaften Ergebnissen führen kann.

Obwohl die *Aufbewahrung der Personalakten* in der zentralen Registratur in offenen Hängeregalen erfolgt, habe ich die Datensicherheit wegen der sonstigen getroffenen Maßnahmen (festgelegte Zugriffsberechtigungen; Sicherheitsschlösser, die mit dem Universalschlüssel nicht zu öffnen sind; kontrollierte Schlüsselverwaltung; Reinigung innerhalb der Dienstzeiten; Akteneinsicht durch Beschäftigte unter Aufsicht; Unterbringung der Registratur im ersten Obergeschoß) als *insgesamt* gewährleistet angesehen.

Soweit für einen übernommenen Beschäftigten Personalunterlagen aus DDR-Zeiten (*Kaderakten*) vorhanden waren, wurden sie zur Grundakte genommen (siehe 5.1.7).

Die Grundakten enthielten kein Verzeichnis über vorhandene *Teil- und Nebenakten*, obwohl in den Schulämtern und Schulen Nebenakten, im Landesamt für Finanzen die Bezügeakten und in einer separaten Stelle des Oberschulamts Teilakten zu Personalüberprüfungen und Kündigungen geführt werden. Die fehlenden Verzeichnisse gefährden das Recht der Beschäftigten auf Einsicht in die vollständige Personalakte. Außerdem ist nicht gewährleistet, daß das Oberschulamt den Überblick über alle Teil- und Nebenakten behält. Ich habe deshalb gefordert, die Verzeichnisse anzulegen.

Der *Versand der Personalakten* erfolgte in DIN A4-Umschlägen mit der Post. Ich habe gebeten, künftig folgenden Mindeststandard zur Gewährleistung der Datensicherheit einzuhalten:

1. Für den Aktentransport sind verschließbare Transporttaschen zu verwenden (Alternative: versiegelte Umschläge).
2. Der Transport per Boten ist - sofern möglich - dem Postweg vorzuziehen.
3. Bei Postversand sind die Personalakten als Wertpaket zu versenden.
4. Die Aktenübergabe hat gegen Empfangsbescheinigung zu erfolgen.
5. Aktenrückgaben sind zu überwachen.

Zur Unterstützung der Personalverwaltung führte das Oberschulamt eine *Lehrerpersonaldatei* mit den Grunddaten der Beschäftigten. Die Gesamtdatei war den Zuständigkeiten der Personalbearbeiter entsprechend in Einzeldateien für die jeweiligen Einzelplatz-PCs aufgeteilt. Die PC-Lösung sollte eine Zwischenlösung bis zum Einsatz der vom SMK konzipierten *Lehrpersonaldatenbank* sein. Die Datensicherheit der PCs war nur ungenügend gewährleistet. Von einer förmlichen Beanstandung der Sicherheitsmängel habe ich nur deshalb abgesehen, weil die PC-Lösung kurzfristig durch das verbesserte Verfahren "Lehrpersonaldatenbank" abgelöst werden sollte.

Vorgänge über *abgelehnte Bewerber* wurden seit 1990 aufbewahrt. Da selbst bei vorläufigen Ablehnungen spätestens nach einem Jahr von einer endgültigen Nichteinstellung ausgegangen werden kann, habe ich die Löschung von Bewerbungsvorgänge gefordert, die älter als ein Jahr sind, und angeregt, spätestens nach fünf Jahren die Daten auch in zugehörigen Bewerberkarteien oder Bewerberdateien zu löschen.

Das Verfahren zur *Personalüberprüfung* sowie das Bewußtsein der Mitarbeiter über die datenschutzgerechte Behandlung dieser Vorgänge vermittelten insgesamt einen positiven Eindruck. Gerügt habe ich jedoch, daß die laut "Gauck"-Auskunft belasteten Beschäftigten über das jeweilige Staatliche Schulamt in einem unverschlossenen Schreiben zur Anhörung eingeladen wurden. Einladungen zu Personalgesprächen (auch in Angelegenheiten außerhalb der Personalüberprüfung) sind direkt an die Privatanschrift des Beschäftigten zu richten.

Das SMK hat inzwischen die notwendigen Schritte eingeleitet, um die festgestellten Mängel meinen Vorschlägen entsprechend abzustellen.

5.1.9 Datenerhebung bei Fortbildungsveranstaltungen des SMI

Bei Fortbildungsveranstaltungen des SMI werden die Teilnehmer aufgefordert, das Seminar und die Leistung des Referenten zu beurteilen. Dabei haben die Teilnehmer ihren Namen und ihre Dienststelle in den Bewertungsbogen einzutragen. Ich habe das SMI aufgefordert, das Verfahren in folgenden Punkten zu ändern:

- Die Erhebung der Namen und der Dienststellen der Seminarteilnehmer für Zwecke der Seminarbeurteilung ist nicht erforderlich (§ 11 Abs. 1 SächsDSG). Das SMI wird künftig auf diese Angaben verzichten.

- Aus Sicht des Referenten erhebt das SMI über ihn personenbezogene Daten bei Dritten - nämlich den Seminarteilnehmern -, indem es diese den Seminarinhalt und die Vortragsweise beurteilen läßt. Dies ist bisher ohne die nach § 11 Abs. 4 Nr. 2 SächsDSG erforderliche Einwilligung geschehen. Hierzu will sich das SMI erst äußern, wenn es die Verfahrensweise in den anderen Bundesländern geklärt hat. Was das soll, weiß ich nicht.
- Zur Frage nach der Aufbewahrungsdauer der Bewertungsbogen hat das SMI mitgeteilt, sie würden im Hinblick auf Prüfungen des Rechnungshofs *fünf* Jahre aufbewahrt. Nach meiner Auffassung sind Seminarbeurteilungen keine Belege zu Buchungen und fallen damit nicht unter die Aufbewahrungsbestimmungen zu § 71 der SäHO. Die Bewertungsbogen sollten nach deren Auswertung, spätestens jedoch nach einem Jahr, vernichtet werden (§ 19 Abs. 1 Nr. 2 SächsDSG).

5.1.10 Automatisierte Verarbeitung von Arbeitszeitdaten durch private Auftragnehmer

Eine öffentliche Stelle bat mich um Stellungnahme zu der Frage, ob es zulässig sei, mit der automatisierten Verarbeitung von Arbeitszeitdaten ein privates Rechenzentrum zu beauftragen (§ 7 SächsDSG). Dazu habe ich wie folgt Stellung genommen:

Sowohl das SächsBG als auch das SächsDSG schließen die Verarbeitung von Beschäftigtendaten durch private Auftragnehmer nicht per se aus.

Da jedoch im Zuge einer automatisierten Verarbeitung von Arbeitszeitdaten stets auch Personaldaten (Voll- oder Teilzeitbeschäftigung, Urlaubs- und Krankheitszeiten) verarbeitet werden, sollten diese möglichst nicht an private Auftragnehmer weitergegeben werden. Soweit dies (z. B. aus Kostengründen) unerläßlich ist, sollten die übertragenen Verarbeitungsschritte auf ein Mindestmaß reduziert werden. Ich habe geraten, Terminal und Drucker in den Räumen der öffentlichen Stelle zu installieren, damit dort Dateneingabe, Auswertung und Ausdruck erfolgen können.

5.1.11 Fehlende Aufgabenabgrenzung bei der Personalverwaltung für die Lehrer

Für meine Kontrolltätigkeit habe ich das SMK gebeten, mir darzulegen, wie die personalverwaltenden Aufgaben zwischen Oberschulämtern, Staatlichen Schulämtern und Schulen abgegrenzt sind. Ohne Kenntnis der Aufgabenverteilung kann ich nicht beurteilen, ob die Akteninhalte von Grund-, Teil- und Nebenakten den Vorgaben entsprechen und der Datenaustausch zwischen den beteiligten Stellen datenschutzgerecht erfolgt. Offenbar ist dieser wichtige Bereich fünf Jahre nach der sogenannten "Wende" immer noch nicht geregelt, denn anstelle einer Auskunft habe ich nur den Hinweis auf eine noch zu erarbeitende Verwaltungsvorschrift erhalten.

Außerdem habe ich angeregt, die derzeitige Organisation der Personalverwaltung zu überdenken und sie nur *einer* Stelle - Oberschulamt *oder* Schulamt - zu übertragen. Dies würde den Kreis der mit Personalangelegenheiten befaßten Personen verringern, den Umfang der auszutauschenden Daten reduzieren und überflüssigen Aufwand ersparen.

Nach dem Ministerwechsel habe ich den Eindruck gewonnen, daß die bestehenden Probleme nunmehr vorrangig gelöst werden sollen.

5.1.12 Anwendbarkeit des Sächsischen Datenschutzgesetzes auf die Beschäftigten bei Sparkassen

Ich erhielt Kenntnis von der Geschäftsanweisung einer Stadtsparkasse, nach der ihre Mitarbeiter gehalten sind, bei anderen Geldinstituten keine Kredite aufzunehmen oder Bürgschaftsverpflichtungen einzugehen, keine Konten zu unterhalten und Geld- oder Wertpapiergeschäfte nur bei der eigenen Sparkasse abzuwickeln. Ausnahmen davon seien genehmigungspflichtig, und zwar auch dann, wenn die betreffenden Rechtsgeschäfte vor Erlaß der Geschäftsanweisung getätigt wurden. Ich wurde um Prüfung gebeten, ob darin ein Verstoß gegen § 31 Abs. 1 SächsDSG liege, wonach Daten von Beschäftigten nur zur Eingehung, Durchführung oder Beendigung des Arbeitsverhältnisses verarbeitet werden dürften.

Trotz meiner - sicher verständlichen - Empörung kam ich zu der Auffassung, daß auch auf das Personal der Sparkassen im Freistaat Sachsen die Vorschriften des BDSG (mit Ausnahme des zweiten Abschnitts) Anwendung finden und meine Zuständigkeit damit nicht gegeben ist. Dabei bin ich von folgenden Überlegungen ausgegangen:

Gemäß § 2 Abs. 3 SächsDSG finden die Vorschriften des BDSG auf *öffentlich-rechtliche Unternehmen mit eigener Rechtspersönlichkeit* Anwendung, *soweit* sie am *Wettbewerb* teilnehmen (§ 2 Abs. 3 SächsDSG). § 1 Abs. 1 SächsSparkG stattet die Sparkassen als *rechtsfähige Anstalten des öffentlichen Rechts* mit einer eigenen Rechtspersönlichkeit aus; § 2 Abs. 1 SächsSparkG macht es ihnen als Wirtschafts*unternehmen* zur Aufgabe, den *Wettbewerb* im Kreditgewerbe zu stärken.

Damit sind Sparkassen öffentlich-rechtliche Unternehmen mit eigener Rechtspersönlichkeit, die am Wettbewerb teilnehmen.

Durch die Einschränkung "*soweit"* entsteht die Frage, ob jedoch das SächsDSG im Personalbereich Anwendung findet. Denn aus der Verwendung von "soweit" könnte gefolgert werden, daß Sparkassen bei der Verarbeitung von Beschäftigtendaten *insoweit nicht am Wettbewerb* teilnehmen. Würde die Anwendbarkeit des SächsDSG im Personalbereich bejaht, müßte dies konsequenterweise auch für alle übrigen internen Bereiche gelten, die zwar die Funktionsfähigkeit des Unternehmens gewährleisten, aber nicht *direkt* auf den Wettbewerb ausgerichtet sind. Damit würde die gesamte Verarbeitung personenbezogener Daten außerhalb des eigentlichen Bankgeschäfts, z. B. in den Bereichen Organisation und Verwaltung in den Anwendungsbereich des SächsDSG fallen, also die Verarbeitung der Daten von Lieferanten, Handwerkern, Software-, Werbe- und Baufirmen, fremdem Reinigungs-, Sicherheits- und Wartungspersonal, Architekten, Maklern usw.

Bereits die Fragestellung, ob ein rechtsfähiges Unternehmen mit seinem Personal am Wettbewerb teilnimmt, ist verfehlt. Denn es wird übersehen, daß die juristische Person (das Unternehmen) nur als solches am Wettbewerb teilnehmen kann, nämlich als ein

einheitliches Ganzes. Eine juristische Person kann nicht in einen "Innenbereich" (Personal, allgemeine Verwaltung, Organisation) ohne Wettbewerbscharakter und einen "Außenbereich" (Bankgeschäft) mit Wettbewerbscharakter aufgeteilt werden. Vielmehr verleiht der "Innenbereich" dem theoretischen Gebilde der juristischen Person erst seine Handlungsfähigkeit.

Die sich aus § 2 Abs. 3 SächsDSG ergebende Frage ist damit nicht, ob ein öffentlich-rechtliches Wettbewerbsunternehmen mit seinem Personalbereich am Wettbewerb teilnimmt, sondern, *ob* ein öffentlich-rechtliches Unternehmen mit seiner gesamten Rechtspersönlichkeit am Wettbewerb teilnimmt. Denn anders als private Wirtschaftsunternehmen können öffentlich-rechtliche Unternehmen auch außerhalb des Wettbewerbs in hoheitlichen Angelegenheiten oder als Inhaber einer Monopolstellung tätig werden. Unterwirft § 2 Abs. 1 SächsDSG zunächst *jede* "sonstige der Aufsicht des Freistaates Sachsen unterstehende juristische Person des öffentlichen Rechts" dem Geltungsbereich des SächsDSG, so nimmt § 2 Abs. 3 SächsDSG davon wieder diejenigen aus, die am Wettbewerb teilnehmen, und unterstellt sie den Vorschriften des BDSG. Die Konjunktion "soweit" schränkt also § 2 Abs. 1 SächsDSG ein und knüpft nicht unterschiedliche Rechtsfolgen an einzelne Handlungen ein und derselben juristischen Person, je nachdem ob die jeweilige Handlung Wettbewerbscharakter hat oder nicht.

Der Regierungspräsident führt die Datenschutzaufsicht über die Sparkassen. Er muß beurteilen, ob - was naheliegt - die Geschäftsanweisung unrechtmäßig ist.

5.1.13 Frage nach der Religionszugehörigkeit bei Lehrern und Lehramtsbewerbern

Lehrer und Lehramtsbewerber haben im Personalbogen ihre Religionszugehörigkeit anzugeben. Weder das SMK noch das SMI haben bisher zu der Frage Stellung genommen, für welche Zwecke dieses Datum benötigt wird. Auch ein dazu befragtes Oberschulamt (personalverwaltende Stelle für den Lehrerbereich) konnte nicht angeben, welche Schlußfolgerungen aus einer bestimmten Religionszugehörigkeit gezogen werden. Ich muß also von der Nichterforderlichkeit dieses Datums ausgehen und werde die Angelegenheit weiterverfolgen.

5.1.14 Kein Austausch von Bewerberdaten im Geschäftsbereich des SMI

Anläßlich eines Vorstellungsgesprächs bei einer Behörde im nachgeordneten Geschäftsbereich des SMI erfuhr ein Petent, daß man dort bereits über seine weiteren Bewerbungen - ebenfalls im Geschäftsbereich des SMI - Bescheid wußte. Der Petent bat mich der Frage nachzugehen, ob Bewerberdaten im Geschäftsbereich des SMI zentral erfaßt würden, um Mehrfachbewerbungen sowie bereits abgelehnte Bewerber oder Bewerber mit Einstellungszusagen erkennen zu können.

Sowohl das SMI als auch die Regierungspräsidien haben mir ausdrücklich versichert, es würden zentral *keine* Bewerberdaten erfaßt. Es war nicht nachvollziehbar, woher das SMI über die Mehrfachbewerbung Kenntnis hatte. Dies habe ich dem Petenten mitgeteilt.

5.1.15 Kritik an der Verordnung über die dienstliche Beurteilung der Beamten (SächsBeurtVO) und der Beurteilungsrichtlinie des SMI

Ich habe gegenüber dem SMI sowohl die SächsBeurtVO als auch die Beurteilungsrichtlinie vom 11. Februar 1994, an denen ich nicht beteiligt worden bin, aus folgenden Gründen kritisiert:

Gemäß § 5 Abs. 4 SächsBeurtVO sind in der Befähigungsbeurteilung die *allgemeinen Fähigkeiten* eines Beamten anhand von Befähigungsmerkmalen zu bewerten. Eine nähere Konkretisierung der zu bewertenden Befähigungsmerkmale enthält die Rechtsverordnung nicht, obwohl § 115 Abs. 1 SächsBG eine entsprechende Ermächtigungsgrundlage bietet (Bestimmung der Beurteilungs*grundsätze*). Außerdem läßt die Verordnung offen, *wie* die Befähigungsbeurteilung im Rahmen der dienstlichen Beurteilung zu berücksichtigen ist, z. B. für die weitere dienstliche Verwendung oder berufliche Entwicklung des Beamten.

Ausgehend vom Zweck der Beurteilung - einen Beamten entsprechend seinen Fähigkeiten einzusetzen, um eine effektive Verwaltung zu gewährleisten - muß nicht nur die Leistungsbeurteilung, sondern auch die Befähigungsbeurteilung einen Bezug zur dienstlichen Tätigkeit aufweisen. Deshalb dürfen *allgemeine* Charaktereigenschaften nicht in einem Umfang bewertet werden, der einem Persönlichkeitsprofil gleichkommt.
Weder die vorliegende Beurteilungsverordnung noch die dazu vom SMI erlassene (und von anderen Staatsministerien übernommene) Verwaltungsvorschrift berücksichtigen diesen datenschutzrechtlichen Aspekt. Das zeigt der Katalog von etwa 30 (!) "Befähigungsmerkmalen", die der Beurteiler um weitere Merkmale ergänzen kann.

Da dieser Katalog keine Systematik erkennen läßt, Leistungsmerkmale den Befähigungsmerkmalen zuordnet (z. B. schriftliche und mündliche Ausdrucksfähigkeit, vgl. dazu Beurteilungsrichtlinie des SMF), die Bewertung gleicher und ähnlicher Merkmale sowohl in der Leistungs- als auch in der Befähigungsbeurteilung vorsieht (z. B. Eigenständigkeit/Selbständigkeit der Durchführung; Führungsverhalten/Mitarbeiterführung; Arbeitsplanung/Organisationsfähigkeit) und reine Persönlichkeitsmerkmale bewertet (Einfallsreichtum, Lernfähigkeit, geistige Beweglichkeit, Kontaktfähigkeit), beeinträchtigen die vorgesehenen Befähigungsmerkmale in ihrer Gesamtheit das Persönlichkeitsrecht des Beamten.

Ich halte deshalb eine Änderung der Beurteilungsverordnung und eine Überarbeitung der Merkmalskataloge für die Leistungs- und Befähigungsbeurteilung für erforderlich.

5.1.16 Kündigung wegen angeblicher Verletzung des Datengeheimnisses

Einer Beschäftigten wurde wegen (angeblicher) Verletzung des Datengeheimnisses (§ 6 SächsDSG) gekündigt, weil sie die *negative* Einschätzung eines Fachvorgesetzten zur vorgesehenen Verbeamtung an die betroffene Mitarbeiterin weitergeleitet hatte. Dem vorgetragenen Sachverhalt zufolge hatte die Gekündigte dabei wie in einem anderen Fall gehandelt, in dem sie der für die Verbeamtung Vorgesehenen die - allerdings *positive* - Einschätzung auf Weisung des Fachvorgesetzen zugeleitet hatte.

Im Rahmen des Kündigungsschutzprozesses hat mich die ÖTV um Stellungnahme gebeten, ob gegen das Sächsische Datenschutzgesetz verstoßen worden sei. Ich habe dazu folgende Auffassung vertreten:

Wesen und Zweck des Datenschutzes ist es, *den einzelnen davor zu schützen*, daß er durch Behörden oder sonstige öffentliche Stellen in *seinem Persönlichkeitsrecht, insbesondere seinem Recht auf informationelle Selbstbestimmung*, beeinträchtigt wird (Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG; Art. 33 SächsVerf, § 1 SächsDSG). Diesem Anliegen werden insbesondere die §§ 17 ff. SächsDSG (Schutzrechte) gerecht. Hervorzuheben ist hier das weitgehende Recht des Betroffenen auf Auskunft über die zu seiner Person gespeicherten Daten (§ 17 SächsDSG), das ein Indiz dafür ist, daß das Datengeheimnis gegenüber Dritten, nicht aber gegenüber der Betroffenen selbst gilt. Die verfassungskonforme Auslegung des § 6 SächsDSG läßt nur den Schluß zu, daß ein Verstoß schon deshalb nicht vorliegt, weil durch die Weitergabe der Einschätzung an die Betroffene selbst deren Recht auf informationelle Selbstbestimmung in keiner Weise beeinträchtigt wurde. Datenschutzrechtlich liegt somit kein *unbefugtes* Verarbeiten, insbesondere keine Datenübermittlung und sonstige Nutzung i. S. v. § 3 Abs. 2 Nr. 5 und 6 und Abs. 4 SächsDSG (der Betroffene ist nicht "Dritter"), vor.

Eine andere Auffassung würde den Schutzgedanken des Datenschutzgesetzes auf den Kopf stellen.

5.1.17 Einsichtnahme in Personalakten nach Beendigung des Beschäftigungsverhältnisses

Ein Petent, der bereits im Jahre 1990 ausgeschieden und in ein anderes Bundesland verzogen war, bat seine ehemalige Beschäftigungsbehörde, ihm eine Kopie seiner Personalakte zu übersenden. Dies wurde abgelehnt, weil nach Nr. 4.3 der Verwaltungsvorschrift des SMI über die Führung und Verwaltung von Personalakten eine Personalakte nicht vollständig fotokopiert werden darf. Zudem verwies man auf das in den *Barmer Briefen* - allerdings unvollständig - wiedergegebene Grundsatzurteil des Bundesarbeitsgerichts vom 11. Mai 1994 (5 AZR 66/93). Dieses besagt zum einen, daß durch § 83 BetrVG und § 13 BAT dem Arbeitnehmer ein Einsichtsrecht in seine Personalakten nur bis zur Beendigung des Arbeitsverhältnisses gewährt wird (in den *Barmer Briefen* wiedergegebener Teil des Urteils) und zum anderen, daß aus nachwirkender Fürsorgepflicht auch noch nach dem Ausscheiden ein Einsichtsanspruch bestehen kann (in den *Barmer Briefen nicht* wiedergegebener Teil des Urteils).

Ich habe der Behörde das vollständige Urteil übersandt und gebeten, dem Antrag des Betroffenen aus folgenden Gründen zu entsprechen:

Selbst wenn eine nachwirkende Fürsorgepflicht vier Jahre nach dem Ausscheiden des Betroffenen verneint werden sollte, besteht für ihn gemäß § 17 SächsDSG ein Einsichtsrecht in die Personalakte. Insoweit löst diese Vorschrift nach Beendigung des Arbeitsverhältnisses das Einsichtsrecht nach § 13 BAT ab. Denn § 17 Abs. 3 SächsDSG sieht vor, daß die speichernde (öffentliche) Stelle Einsicht in Akten zu gewähren hat, die zur Person des Betroffenen geführt werden.

Die Form der Einsichtnahme bestimmt die speichernde Stelle gemäß § 17 Abs. 4 SächsDSG nach *pflichtgemäßem Ermessen*. Dies kann z. B. durch Anfertigung von Kopien geschehen. Wegen der erheblichen räumlichen Entfernung zwischen dem Wohnort des Petenten und der Behörde (ca. 700 km) wäre es unverhältnismäßig und damit ermessensfehlerhaft, den Betroffenen auf eine persönliche Akteneinsichtnahme zu verweisen. Die Übersendung von Kopien wäre bürgerfreundlich und im Interesse des Grundrechts auf informationelle Selbstbestimmung für den Betroffenen eine angemessene Alternative. Daß die Anfertigung von Kopien aus Personalakten grundsätzlich zulässig ist, stellen sowohl die Protokollnotiz zu § 13 Abs. 1 BAT-O als auch § 120 Abs. 3 SächsBG klar. Zwar teile ich die Auffassung der Behörde, daß die Aushändigung von Kopien kompletter Personalakten unüblich ist - *unüblich* bedeutet jedoch nicht per se *unzulässig*.

Außerdem habe ich darauf aufmerksam gemacht, daß in das Recht auf informationelle Selbstbestimmung nur *durch Gesetz* oder *aufgrund eines Gesetzes* eingegriffen werden darf (Art. 33 SächsVerf, § 4 Abs. 1 SächsDSG), nicht aber aufgrund einer *Verwaltungsvorschrift*, die im übrigen nur für Beamte gilt.

Inzwischen hat die Behörde dem Petenten die vollständig kopierte Personalakte übersandt.

5.1.18 Beihilfegewährung für Kommunalbeamte

Ich habe beim Kommunalen Versorgungsverband Sachsen (KVS) eine Änderung der Antragsvordrucke zur Beihilfegewährung erreichen können (siehe 2. Tätigkeitsbericht, 5.1.9). So sind künftig nur noch dann Angaben über den Ehegatten zu machen, wenn für ihn Aufwendungen geltend gemacht werden. Auf die Frage nach dem Grund für eine Beurlaubung ohne Bezüge wird ebenso verzichtet wie auf die Angabe, warum ein Kind für die Beihilfegewährung entfallen ist. Außerdem sind die Art der Behandlung sowie der behandelnde Arzt nicht mehr anzugeben.

Angaben zur Art der Aufwendungen werden jedoch weiterhin gefordert, was immer noch Rückschlüsse auf bestimmte Erkrankungen zuläßt. Das Argument, der KVS müsse doppelt eingereichte Belege erkennen, überzeugt mich nicht. Denn bereits anhand des Datums und des Rechnungsbetrages dürfte dies möglich sein. Zudem werden die Belege vor ihrer Rücksendung als "für Beihilfezwecke verwendet" gekennzeichnet. Ich habe den KVS aufgefordert, die Beihilfeanträge in diesem Punkt an die vom Landesamt für Finanzen verwendeten Vordrucke anzupassen.

Erfreulich war, daß durch meine Initiative die Beihilfeanträge inzwischen ohne Einhaltung der Personalstelle direkt beim KVS eingereicht werden können.

5.1.19 Sozialauswahl für bedarfsbedingte Kündigungen von Erziehern und Hortnern

Einer Großstadt stellt sich das Problem, von den rd. 1800 Erziehern und Hortnern ca. 400 wegen mangelnden Bedarfs entlassen zu müssen. Im Hinblick auf die personelle Auswahl der zu Kündigenden sollte mit dem Personalrat eine Dienstvereinbarung gem. § 81 Abs. 3 Nr. 8 SächsPersVG abgeschlossen werden. Diese wurde mir im Entwurf zur datenschutzrechtlichen Beurteilung vorgelegt. Folgendes Verfahren war beabsichtigt:

- Die in dem automatisierten Personalinformationssystem gespeicherten Grunddaten *Beschäftigungszeit, Lebensalter, Schwerbehinderung/Gleichstellung, unterhaltsberechtigte Kinder, Familienstand* werden für alle 1800 Beschäftigten nach einem Punkteschema (= "Sozialpunkte") ausgewertet.
- Die 400 Beschäftigten mit den wenigsten Sozialpunkten und alle Beschäftigten, die die durchschnittliche Punktzahl um bis zu 1,5 Punkten überschreiten, werden über die vorgesehene Kündigung informiert und aufgefordert, weitere, insbesondere soziale Gründe anzugeben, die einer Kündigung entgegenstehen könnten.
- Die Antworten werden schematisch auf ihre soziale Relevanz hin überprüft, um die Anwendung einheitlicher Maßstäbe bei der Auswertung zu gewährleisten, wobei Spielraum für nicht katalogisierte Gründe bleibt. Als Alternative war vorgesehen, mögliche Sozialgründe über einen Fragenkatalog zu ermitteln.

Ich habe wie folgt Stellung genommen:

Im Hinblick auf die in § 1 Abs. 3 KSchG vorgeschriebene Sozialauswahl im Vorfeld anstehender Kündigungen ist es zulässig, Beschäftigtendaten im Rahmen der §§ 12 Abs. 1 und 11 Abs. 1 und 2 SächsDSG zu verarbeiten, wobei ich bei der Frage der Erforderlichkeit strenge Maßstäbe anlege.

Datenschutzrechtlich bestehen keine Bedenken, wenn für Zwecke der *Vorauswahl* die bereits in einem Personalinformationssystem gespeicherten Grunddaten der Beschäftigten *Beschäftigungszeit, Lebensalter, Schwerbehinderung/Gleichstellung, unterhaltsberechtigte Kinder* und *Familienstand* automatisiert nach einem Punkteschema ausgewertet werden. Bei 1800 in Betracht kommenden Personen dürfte dies erforderlich sein.

Nach § 1 Abs. 3 KSchG und der dazu ergangenen Rechtsprechung sind bei der Sozialauswahl jedoch die individuellen Besonderheiten des Einzelfalles ausschlaggebend. Der Arbeitgeber hat also diejenigen Arbeitnehmer zu ermitteln, die eine Kündigung - relativ gesehen - am wenigsten hart trifft. Dies setzt voraus, daß sich der Arbeitgeber auch Kenntnis von Sachverhalten aus der privaten Lebenssphäre seiner Arbeitnehmer verschaffen muß, die eine Kündigung als sozial ungerechtfertigt erscheinen lassen. Dem Kündigungsschutzgesetz ist nicht zu entnehmen, was konkret unter *sozialen Gesichtspunkten* zu verstehen ist. Insoweit verwendet das Gesetz einen unbestimmten Rechtsbegriff, der dem Arbeitgeber einen Beurteilungsspielraum läßt. Da das Gesetz

zudem kein Verfahren zur Sozialauswahl vorschreibt, muß das Verfahren aus datenschutzrechtlicher Sicht so gestaltet werden, daß keine Vorratsdatenerhebung erfolgt und sich das Verfahren stufenweise entwickelt: Je mehr der Einzelne in die Sozialauswahl hineingerät, um so mehr Daten kann er "ins Spiel bringen".

Diesem Erfordernis entspricht weitgehend das im Entwurf der Dienstvereinbarung vorgesehene Modell, wonach die für eine Kündigung in Betracht kommenden Arbeitnehmer die gegen eine Kündigung sprechenden sozialen Gründe in freier Form vorbringen können. Dieses Verfahren hat gegenüber einer Datenerhebung durch einen *starren* Fragenkatalog den Vorteil, daß die Betroffenen selbst bestimmen, welche Gründe sie nennen wollen und in welchem Umfang sie ihre soziale Situation darstellen. Denn gerade bei einer Sozialauswahl würden durch einen vorgegebenen Fragenkatalog stets eine Reihe für den konkreten Einzelfall nicht erforderlicher Daten erhoben werden; in atypischen Fällen würden die dort interessanten Daten gar nicht zur Geltung gelangen.

Gleichwohl sollte aus dem Informationsschreiben hervorgehen und durch Beispiele veranschaulicht werden, was unter sozialen Gesichtspunkten zu verstehen ist. Ich habe angeregt, einige katalogmäßig zu prüfende Merkmale bereits vor Abfrage der einzelfallrelevanten sozialen Gründe mitzuteilen, damit jeder weiß, worauf es ankommt, und damit der Kreis der für eine Kündigung in Betracht kommenden Personen abgrenzbar ist.

Außerdem habe ich auf folgendes hingewiesen:
- Von der Befragung sind Personen auszunehmen, deren ordentliche Kündigung gesetzlich ausgeschlossen ist (z. B. Schwangere, sofern der Dienststelle die Schwangerschaft bekannt ist, Mitglieder der Personalvertretung).
- Da das Kündigungsschutzgesetz den Arbeitnehmer nicht ausdrücklich zur Auskunft *verpflichtet*, die Erteilung von Auskünften über soziale Gesichtspunkte jedoch Voraussetzung für die Fortsetzung des Arbeitsverhältnisses, also für die Gewährung eines Rechtsvorteils ist, sind die Beschäftigten in dem Informationsschreiben gemäß § 11 Abs. 2 SächsDSG entsprechend zu unterrichten und über die Folgen einer Verweigerung von Angaben aufzuklären.

Ich gehe davon aus, daß die Stadt in vorstehendem Sinne verfährt.

5.1.20 Keine Bekanntgabe von Daten aus der Arbeitszeiterfassung im Umlaufverfahren an alle Mitarbeiter trotz Einwilligung

Ich wurde gefragt, ob es datenschutzrechtlich zulässig sei, Übersichten mit Daten aus der Arbeitszeiterfassung allen Mitarbeitern der Abteilung einer Behörde im Umlaufverfahren bekanntzugeben, damit das Versenden der Monatsübersichten im verschlossenen Umschlag entfallen könne. Alle Mitarbeiter hätten sich "aktenkundig" nicht nur für das Verfahren ausgesprochen, sondern es aus verschiedenen Gründen sogar für wünschenswert gehalten.

Im Hinblick auf die Grenzen der Einwilligung habe ich mich dazu wie folgt geäußert:

Werden Daten aus der Arbeitszeiterfassung abteilungsweise zu Übersichten zusammengefaßt und allen Mitarbeitern der Abteilung im Umlaufverfahren zur Kenntnis gegeben, so ist dies eine Datenübermittlung im Sinne des § 3 Abs. 2 Nr. 5 Buchst. a SächsDSG, da den Mitarbeitern neben den eigenen stets auch die Arbeitszeit-Daten der Kollegen - also von Dritten - bekanntgegeben werden. Nach § 31 Abs. 2 SächsDSG ist eine solche Datenübermittlung an Private - abweichend von § 15 SächsDSG - nur auf gesetzlicher Grundlage oder mit Einwilligung des Betroffenen *zulässig*.

Da alle Mitarbeiter einer Abteilung aktenkundig gemacht haben, daß sie den Umlauf einer solchen Abteilungsliste nicht nur akzeptieren, sondern sogar wünschen, könnte man zu dem Schluß gelangen, daß die Datenübermittlung (jeweils der eigenen Daten an die anderen Mitarbeiter) mit Einwilligung der Betroffenen zulässig sei. Die Einwilligung in eine Datenübermittlung (oder sogar der ausdrückliche diesbezügliche Wunsch) bedeutet für eine öffentliche Stelle jedoch nicht per se die *Verpflichtung* zur Datenübermittlung. Oder anders ausgedrückt: Die Mitarbeiter können mit ihrer Einwilligung die Bekanntgabe ihrer Daten im Umlaufverfahren nicht erzwingen. Vielmehr hat die öffentliche Stelle über die Datenübermittlung nach pflichtgemäßem Ermessen zu entscheiden, wobei sie - gebunden an gesetzmäßiges Verwaltungshandeln - stets auch allgemeine Grundsätze wie Verhältnismäßigkeit, Fürsorgepflicht, Erforderlichkeit der Datenverarbeitung, Zweckbindung der Daten und Übermittlungsverbote zu beachten hat. Das bedeutet, daß trotz der Einwilligung aller Mitarbeiter eine Datenübermittlung an sie aus den genannten Gründen keineswegs erlaubt ist.

Der Weitergabe der Abteilungsliste an alle Mitarbeiter steht hier § 31 Abs. 5 SächsDSG entgegen, wonach alle zur Verhaltens- und Leistungskontrolle erhobenen Daten unter einen besonderen Schutz gestellt sind. Nach dieser Vorschrift dürfen die zur Verhaltenskontrolle erhobenen Arbeitszeit-Daten nur für Zwecke der Arbeitszeitkontrolle *genutzt*, d. h. nur von den zur Arbeitszeitkontrolle Befugten *ausgewertet* werden. Die Verwendung des Wortes "nutzen" anstelle des weiteren Begriffs "verarbeiten", der die Datenübermittlung umfassen würde, führt zu dem Schluß, daß der Gesetzgeber die Bekanntgabe von Daten aus der Leistungs- und Verhaltenskontrolle an Dritte ausschließen wollte. Folglich kommt die Bekanntgabe der Arbeitszeit-Daten im Umlaufverfahren trotz Einwilligung der Mitarbeiter *nicht* in Betracht.

Es ist auch zu bedenken, daß soziale Zwänge oder gruppendynamische Prozesse die eine oder andere "Freiwilligkeit" beeinflussen. Schließlich ist Streit für den Fall

vorprogrammiert, daß jemand seine Einwilligung - was jederzeit ohne Begründung möglich ist - widerruft. Die Verantwortung für die Einhaltung der Arbeitszeit liegt beim jeweiligen Vorgesetzten (Gruppen- oder Referatsleiter, Abteilungsleiter usw.). Die Belegschaft - auch der Personalrat - ist an dieser Kontrolle nicht beteiligt.

5.2 Landessystemkonzept

Seit mehreren Jahren steht ein Landessystemkonzept für den Freistaat Sachsen zur Diskussion, das die Staatsregierung unter Federführung des SMI erarbeiten sollte. In den Grundzügen müßte es folgendes umfassen:

a) Zielbeschreibung

Grundlagen:
1. Datenverarbeitung in Sachsen muß rechtmäßig gestaltet werden (bei Personenbezug: aufgabenbezogene spezialgesetzliche Regelungen; Sächsisches Datenschutzgesetz).
2. Datenverarbeitung in Sachsen muß prioritär dezentral gestaltet werden (siehe Organisationsvorgaben der Verfassung, Ressortprinzip, Selbstverwaltung von Kommunen, Kommunalverbänden, Universitäten, Kammern; siehe aber auch Prinzipien der Subsidiarität, der größtmöglichen Privatisierung und der Deregulierung). Manche haben es noch nicht erkannt: Zentralismus ist erfolglos.
3. Datenverarbeitung in Sachsen soll technisch zukunftsoffen und krisensicher gestaltet werden (keine langfristige Bindung an nur einen oder an nur wenige Partner; Schaffung eines innovativen Marktes). Wie sollen wir ein attraktiver Wirtschaftsstandort werden, wenn die Verwaltung im Host-Rechner die Erfüllung ihrer Träume sieht?
4. Datenverarbeitung in Sachsen soll kostengünstig gestaltet werden (z. B. bei Datenverarbeitung im Auftrag: Ausschreibungen! - Sie setzen Fachkenntnis beim Auftraggeber voraus; ich habe den Eindruck, daß manche Verwaltung möglichst viele warme Sessel erhalten will).

b) zeitliche Dimension

Die in a) vorgegebenen Prämissen müssen in folgendenSchritten umgesetzt werden:

- Analyse des Ist-Zustandes (an welchen Gemeinschaftseinrichtungen nehmen die Ressorts teil? Welche Landesbehörden tauschen Datenmassen in einem Umfang aus, der Datenfernverbindungen erforderlich macht?).
- Möglichkeiten zur Erreichung des Soll-Zustandes (wie vor).
- Prognose über Entwicklungsmöglichkeiten (einschließlich Technikfolgenabschätzung).

Dies muß für folgende Teilbereiche je einzeln und in ihrer Verknüpfung erfolgen:

c) Teilbereiche

Hardware
Software (unter anderem vorhandene Großverfahren)
Systemarchitekturen

Vernetzung
Kommunikation
Anschaffung (Standards, Rahmenverträge, Wirtschaftlichkeitsberechnungen)
Wartung
Datensicherheit und Datenschutz
Personal (Anstellung, Fortbildung)
Diese Aufzählung ist nicht abschließend.

d) Vorschläge

Erst daraus folgen dann organisatorische Maßnahmen (z. B. Schaffung einer ständigen Beratungsstelle, Netzbetreibung durch private Anbieter), rechtliche Maßnahmen (generelle Verwaltungsvorschrift zur Datenverarbeitung, Haushaltsgrundsätze bei der Beschaffung), personelle Maßnahmen (z. B. Art. 119 SächsVerf; Fortbildungsangebote) und technische Maßnahmen (Test zur Durchführbarkeit).

Leider sind bisher im SMI nur bruchstückhafte und halbherzige Ansätze erkennbar, die aber nicht im gebotenen Zusammenhang stehen, stellenweise nicht ausreichend tief angelegt waren und trotz interessanter Einzelergebnisse damit dem Anliegen eines Landessystemkonzepts, das insbesondere die rechtlichen Grundlagen berücksichtigt, nicht entsprechen.

In meinem letzten Tätigkeitsbericht erwähnte ich, daß unter Federführung des SMI mehrere Modellversuche zu ausgewählten Bereichen (Datenübermittlung zwischen Staatsregierung und Regierungspräsidien, Datenübermittlung zwischen den Ressorts) durchgeführt werden sollten. Nach einer längeren Anlaufphase existiert mittlerweile ein Modellnetz zwischen mehreren Ressorts und nachgeordneten Behörden, in dem die Nutzer auf mehrere Anwendungen zugreifen konnten (dpa-Pressedienst, JURIS, Statistisches Landesamt, Electronic-Mail-Dienst nach der ISO X-400-Norm). Nachdem ursprünglich der 31. März 1994 als Endtermin festgelegt war, stellte sich bald heraus, daß für brauchbare Ergebnisse ein längerer Zeitraum nötig sein würde, so daß mittlerweile das Modellnetz bis zum 30. Juni 1995 weiter betrieben wird. Eine erste Auswertung ergab, daß wohl die technische Machbarkeit eines solchen Netzes gezeigt wurde, die Ergebnisse des Modellversuches aber als tragfähige Entscheidungsgrundlage für ein Landesdatennetz in keiner Weise ausreichen.

Mittlerweile ist ebenfalls die Beratungsstelle für Informationstechnik (BIT) eingerichtet. Sie soll ressortübergreifend die Planung und den Einsatz der Informationstechnik koordinieren, Grundsatzfragen bearbeiten, neue Entwicklungen in der Informationstechnik berücksichtigen sowie Schulungen durchführen.
Im Dezember 1994 berichtete die BIT über im Arbeitskreis IT über ihre bisherige Arbeit. Folgende Ergebnisse wurden vorgestellt:
- Erfassung der Ist/Soll-Bedarfspläne der Ressorts und ihrer nachgeordneten Bereiche nach einheitlichen Richtlinien,
- Feststellung des IT-Koordinierungsbedarfes für ressortübergreifende IT-Vorhaben sowie für IT-Verfahren, die in mehreren Ressorts eingesetzt werden,
- Definition von Technischen Standards für den Einsatz der Informationstechnik anhand von Checklisten, die datenschutzrechtliche Forderungen berücksichtigen,

- Erarbeitung eines Leitfadens für die Durchführung von Wirtschaftlichkeitsbetrachtungen für IT-Vorhaben, der bei der Erarbeitung der Ist- und Soll-Bedarfspläne helfen soll,
- Beratung und Mitwirkung bei der Planung von IT-Vorhaben der Ressorts,
- Prüfung von (ressortübergreifenden) IT-Vorhaben auf Verträglichkeit mit den IT-Grundsätzen (Standards, Schnittstellen) der Landesverwaltung.

Zur Zeit erstellt die BIT einen Bericht an das Kabinett, in dem auch zukünftige Aufgaben, Organisationsform und Angliederung der Beratungsstelle behandelt werden. Ich empfinde die bisherige Arbeit der BIT als hilfreich und begrüße ein Fortbestehen dieser Beratungseinrichtung.

Seit September 1994 arbeitet eine Arbeitsgruppe “Landesnetz”, der vor allem die Ressorts mit großen DV-Anwendungen angehören, an der Frage des Landessystemkonzeptes. In einer ersten Sitzung wurde die einfachere und billigere Gestaltung der bestehenden, bisher von den Ressorts getrennt betrieben Datenverbindungen als vorrangige Aufgabe bestimmt. Ausgangspunkt sollte eine Bestandsanalyse sein, die neben den Datenverbindungen auch die Telekommunikation umfaßt. Die Ergebnisse machen deutlich, daß große Datenmengen nur ressortintern (mit den Schwerpunkten Finanzbereich und Polizei) fließen. Damit stellt sich verstärkt die Frage nach der Sinnhaftigkeit eines flächen- und behördendeckenden Landesnetzes neu. Zur Zeit wird unter Einbeziehung der vorhandenen Kapazitäten untersucht, welche finanziellen und technischen Auswirkungen verschiedene Netzmodelle haben. Ich habe deutlich gemacht, daß generell (egal bei welcher Variante und bei welchen Anwendungen, die in dieser Variante im Netz laufen) darauf geachtet werden muß, daß ein aufwärtskompatibler Grundschutz innerhalb des Netzes vorzusehen ist, auf den dann abhängig von den laufenden Anwendungen zusätzliche notwendige Maßnahmen des Datenschutzes und der Datensicherheit aufgesetzt werden müssen.

Auf seiner Sitzung im Februar 1995 hat sich der Haushalts- und Finanzausschuß des Sächsischen Landtages mit dem Bericht des Landesrechnungshofes befaßt; er teilt zum Punkt "Landessystemkonzept" die Meinung des Rechnungshofes, der das Fehlen eines solchen Konzeptes seit längerem bemängelt. Er hatte der Staatsregierung bis zum März Gelegenheit zur Stellungnahme gegeben und sich vorbehalten, gegebenfalls Maßnahmen wie die Sperrung bestimmter Haushaltstitel mit IT-Bezug vorzuschlagen. Nachdem die Staatsregierung im März berichtete, verzichtete er auf einschränkende Vorschläge.

5.3 Einwohnermeldewesen

5.3.1 Rechtliche Entwicklung - erforderliche Änderungen des Sächsischen Meldegesetzes

Mit dem Inkrafttreten des Sächsischen Meldegesetzes am 13. Mai 1993 wurde das sächsische Meldewesen (auch) aus datenschutzrechtlicher Sicht dem Gebot des Volkszählungsurteils vom 15. Dezember 1983 (BVerfGE 65, 1 ff., NJW 1984, 419 ff.) entsprechend weitgehend normenklar geregelt. Es hat seine erste Bewährungsprobe im wesentlichen bestanden.

Gleichwohl haben die Novellierung des Melderechtsrahmengesetzes (in der Fassung der Bekanntmachung vom 24. Juni 1994) sowie des Wehrpflichtgesetzes (in der Fassung der Bekanntmachung vom 14. Juli 1994) und die Erfahrungen der bisherigen Anwendungspraxis dazu geführt, eine Änderung bzw. Ergänzung des Sächsischen Meldegesetzes aus datenschutzrechtlicher Sicht in folgenden Punkten zu fordern:

5.3.1.1 Auswirkungen des geänderten WPflG auf die Mitwirkung der Meldebehörden bei der Wehrüberwachung (§ 5 Abs. 2 Nr. 5 SächsMG)

a) Die Sächsischen Meldebehörden speicherten bisher zum Zwecke der Datenübermittlung an die Wehrersatzbehörden (§ 2 2. BMeldDÜV) nach § 5 Abs. 2 Nr. 5 Buchst. a SächsMG die Tatsache, daß der Betroffene auch nach Vollendung des 32. Lebensjahres der Wehrüberwachung unterliegt.

   Der neue § 24 a WPflG bewirkt, daß die (bisher) vorgesehene Speicherung des Kennzeichens "Wehrüberwachung" bei den über 32jährigen männlichen Deutschen entfällt und die Daten dieses Personenkreises nicht mehr an die Wehrersatzbehörden übermittelt werden dürfen. Eine regelmäßige Datenübermittlung an die Wehrersatzbehörden erfolgt nunmehr nur noch bei männlichen Deutschen zwischen dem 17. und dem 32. Lebensjahr.

   Die ersatzlose Streichung des § 5 Abs. 2 Nr. 5 Buchst. a SächsMG ist daher erforderlich.

b) Aufgrund der bisherigen Fassung des § 41 WPflG speicherten die Meldebehörden nach § 5 Abs. 5 b SächsMG die Tatsache, daß männliche deutsche Sowjetzonenflüchtlinge (§ 3 Abs. 1 Satz 1 BVFG) und Vertriebene aus den deutschen Ostgebieten (§ 1 Abs. 2 Nr. 3 BVFG), für zwei Jahre von der Wehrerfassung befreit sind.

Wegen der Wiedervereinigung wird durch die Neufassung des § 41 WPflG nunmehr die zweijährige Befreiung von der Wehrerfassung auf die Vertriebenen aus den deutschen Ostgebieten beschränkt.
Die Anpassung des § 5 Abs. 2 Nr. 5 Buchst. b SächsMG an die Neufassung des § 41 WPflG ist erforderlich.

5.3.1.2 Auswirkungen des novellierten MRRG auf das SächsMG

a) *Löschung von Querverweisungen zwischen den Meldedatensätzen der Eltern und deren Kindern (und umgekehrt)*

Durch § 2 Abs. 1 Nr. 16 MRRG, wonach im Meldedatensatz auch Angaben der Kinder bis zur Vollendung des 27. Lebensjahres gespeichert werden dürfen, ist § 5 Abs. 1 Nr. 16 SächsMG (Speicherung der Kinderdaten nur bis zur Vollendung des 18. Lebensjahres) überholt. Bis zu einer Novellierung des SächsMG ist § 2 Abs. 1 Nr. 16 MRRG für den Freistaat insofern unmittelbar geltendes Recht.

Für die Praxis bedeutet dies, daß die Querverweisungen in den Datensätzen der Eltern und deren Kinder (und umgekehrt), statt wie bisher schon nach Eintritt der Volljährigkeit, nun erst nach Vollendung des 27. Lebensjahres zu löschen sind.

Die Angleichung von § 5 Abs. 1 Nr. 16 SächsMG an § 2 Abs. 1 Nr. 16 MRRG ist unumgänglich.

b) *Löschung von Melderegisterauskunftsdaten bei den politischen Parteien usw. (§ 22 Abs. 1 Satz 3 MRRG, § 33 Abs. 1 SächsMG)*

Nach § 33 Abs. 1 SächsMG darf die Meldebehörde Parteien, Wählergruppen und anderen Trägern von Wahlvorschlägen im Zusammenhang mit Wahlen zu parlamentarischen und kommunalen Vertretungskörperschaften in den sechs der Wahl vorangehenden Monaten Gruppenauskunft über Familiennamen, Vornamen, Doktorgrad und Wohnanschrift von Wahlberechtigten erteilen, für deren Zusammensetzung das Lebensalter der Betroffenen bestimmend ist. Diese Gruppenauskunft kann mit Auflagen versehen werden (vgl. auch 5.3.3.3).

Nach § 22 Abs. 1 Satz 3 des novellierten MRRG haben die Datenempfänger (politische Parteien usw.) die Wählerdaten spätestens einen Monat nach der Wahl zu löschen. Diese (bundesrechtliche) Löschungsverpflichtung bezieht sich jedoch nur auf Wählerdaten, die dem Datenempfänger im Zusammenhang mit der Europa- oder Bundestagswahl übermittelt worden sind. Eine entsprechende Regelung für die Landtags- und Kommunalwahlen fehlt in § 33 Abs. 1 SächsMG.

Die Ergänzung von § 33 Abs. 1 SächsMG um eine dem § 22 Abs. 1 Satz 3 MRRG entsprechende Löschungsverpflichtung halte ich für geboten.
Bis dahin sollten die Meldebehörden die Erteilung von Gruppenauskünften an politische Parteien usw. unbedingt mit einer entsprechenden Auflage zur Löschung der Daten versehen und sich die erfolgte Löschung bestätigen bzw. nachweisen lassen.

c) *Identifizierungspflicht von Hotel-/Pensionsgästen*

Nach § 16 Abs. 2 des novellierten MRRG haben sich ausschließlich Ausländer gegenüber dem Leiter der Beherbergungsstätte oder seinem Beauftragten durch die Vorlage eines gültigen Identitätsdokuments auszuweisen. Diese Verpflichtung beruht auf Art. 45 Abs. 1 Buchst. a des Übereinkommens zur Durchführung des

Übereinkommens von Schengen vom 14. Juli 1985 betreffend den schrittweisen Abbau der Grenzkontrollen. Hierbei handelt es sich um eine Ausgleichsmaßnahme zur Aufrechterhaltung der Sicherheit im Zusammenhang mit dem Abbau der Binnengrenzkontrollen.

Abweichend von § 16 Abs. 2 MRRG sehen §§ 18 Abs. 2, 19 Abs. 1 SächsMG auch eine Identifizierungspflicht für *Deutsche* vor. Hierdurch wird meines Erachtens in *unzulässiger* Weise und ausschließlich durch den Freistaat Sachsen die durch das Schengener Durchführungsübereinkommen vorgesehene Ausgleichsmaßnahme für den Wegfall der Binnengrenzkontrolle, die durch § 16 Abs. 2 MRRG *abschließend* in nationales Recht transformiert wurde, auf Inländer erweitert. § 18 Abs. 2 SächsMG ist insofern rahmenrechtswidrig.

Soweit §§ 18 Abs. 2, 19 Abs. 1 SächsMG eine Identifizierungspflicht außerhalb der Intention des Schengener Durchführungsübereinkommens vorsehen, wird darüber hinaus das Recht der betroffenen Deutschen auf informationelle Selbstbestimmung empfindlich beeinträchtigt, zumal es im deutschen Paß- und Personalausweisrecht keine Verpflichtung zur Mitführung der Personalpapiere gibt. Legt ein Betroffener aber bei seiner Anmeldung kein Ausweispapier vor, so hat dies der Leiter der Beherbergungsstätte auf dem Meldeschein zu vermerken (§ 19 Abs. 1 Satz 2 SächsMG). Bei einer Auswertung der Gästemeldescheine durch die Polizei (im Rahmen des § 19 Abs. 4 SächsMG) wird dieser deutsche Personenkreis (der nicht zur Mitführung seiner Personalpapiere verpflichtet ist) per se als "verdächtig" in die weitergehende polizeiliche Ermittlungsarbeit einbezogen. Solche Eingriffe in das Persönlichkeitsrecht können jedoch weder den Betroffenen selbst noch den Leitern der Beherbergungstätten (Ruf- und Geschäftsschädigung) zugemutet werden.

Eine Angleichung des § 18 Abs. 2 SächsMG an die Vorgaben des § 16 Abs. 2 MRRG ist daher dringend geboten.

d) *Auskunft aus Patientenverzeichnissen an die Meldebehörde und an die Polizeidienststellen (§§ 20 Abs. 4, 21 SächsMG)*

Nach § 20 Abs. 2 SächsMG sind Personen, die in einem Krankenhaus, Pflegeheim oder einer ähnlichen Einrichtung aufgenommen werden, unverzüglich in ein Verzeichnis einzutragen.

Die Meldebehörden und die Polizeidienststellen können verlangen, daß ihnen aus diesem Verzeichnis Auskunft erteilt wird, soweit dies nach ihrer Feststellung *zur Abwehr einer erheblichen Gefahr, zur Strafverfolgung oder zur Aufklärung des Schicksals von Vermißten und Unfallopfern im Einzelfall erforderlich ist (§ 20 Abs. 4 SächsMG)*.

§ 16 Abs. 3 Satz 3 des novellierten MRRG regelt die Auskunftserteilung aus diesen Verzeichnissen aber wie folgt:

"*Der zuständigen Behörde* ist hieraus Auskunft zu erteilen, wenn dies nach ihrer Feststellung zur Abwehr einer erheblichen *und gegenwärtigen* Gefahr, zur Verfolgung

von Straftaten oder zur Aufklärung des Schicksals von Vermißten und Unfallopfern im Einzelfall erforderlich ist."

Der Rahmengesetzgeber hat unter Berücksichtigung des für den betroffenen Personenkreis besonders zu berücksichtigenden Rechts auf informationelle Selbstbestimmung den Auskunftsanspruch der zuständigen Behörden nicht nur vom Vorliegen einer *erheblichen Gefahr* abhängig gemacht; vielmehr muß die Gefahr auch *gegenwärtig* sein, d. h. sie muß *unmittelbar bevorstehen*.

Dieser qualitative Unterschied zur (nur) erheblichen Gefahr muß daher rahmenrechtskonform in den §§ 20 Abs. 4, 21 SächsMG berücksichtigt werden.

Außerdem halte ich die sächsische Regelung, wonach auch den Meldebehörden Auskunft aus den Verzeichnissen zur Abwehr einer erheblichen Gefahr, zur Strafverfolgung oder zur Aufklärung des Schicksals von Vermißten und Unfallopfern im Einzelfall zu erteilen ist, für verunglückt. Für mich ist es nicht nachvollziehbar, daß die Meldebehörden, deren Aufgaben in § 1 SächsMG beschrieben sind, den Polizeidienststellen als Strafverfolgungsbehörden gleichgestellt sein sollen. Auch die Aufklärung der Schicksale von Vermißten und Unfallopfern bewegt sich ebenso außerhalb der melderechtlichen Aufgaben wie die Abwehr einer erheblichen (gegenwärtigen) Gefahr.
In §§ 20 Abs. 4, 21 SächsMG müssen die Meldebehörden deshalb gestrichen werden.

5.3.1.3 Praxisbedingte Änderungsvorschläge für das SächsMG

a) *Fehlende Sanktionen bei Verstößen gegen das Meldegeheimnis (§ 9 SächsMG) im SächsMG*

Nach § 9 Abs. 1 SächsMG darf das Meldeamtspersonal (einschließlich der Auftragnehmer bei Auftragsdatenverarbeitung) personenbezogene Daten nicht unbefugt verarbeiten oder sonst verwenden. Das SächsMG sieht aber keine Sanktionen bei Verstößen gegen das Meldegeheimnis vor.
Zwar verweist § 4 Abs. 2 SächsMG auf die Anwendbarkeit des SächsDSG und damit wohl auch auf die Bußgeld- und Strafvorschriften (§§ 32, 33 SächsDSG); um den gewissenhaften Umgang mit Meldedaten jedoch noch besser zu gewährleisten, sollten zur Klarstellung Verstöße gegen das Meldegeheimnis unmittelbar im SächsMG mit Sanktionen belegt werden (z. B. in § 35 SächsMG).

b) *Kostenerhebung für die Eintragung einer melderechtlichen Auskunftssperre bei Gefahr für Leben, Gesundheit, persönliche Freiheit oder ähnliche schutzwürdige Belange (§§ 32 Abs. 4, 34 SächsMG)*

Im 2. Tätigkeitsbericht habe ich in Nr. 5.3.3 meine Bemühungen deutlich gemacht, die Eintragung einer Auskunftssperre wegen Gefahr für Leben, Gesundheit, persönliche Freiheit oder ähnliche schutzwürdige Belange nicht von einer Verwaltungsgebühr abhängig zu machen. Gleichwohl wurde meiner Forderung auf Gebührenverzicht im

SächsKVZ *nicht* Rechnung getragen. Nr. 91, Tarifstelle 2.1 SächsKVZ sieht für die Eintragung der Auskunftssperre im Melderegister eine Gebühr von 30,- DM vor.

Nachhaltige Verhandlungen mit dem SMI und dem SMF, in denen ich immer wieder betonte, daß die Betroffenen von der Geltendmachung eines solchen wesentlichen Schutzrechts nicht durch eine Gebühr abgehalten werden dürfen, lassen immer noch nicht hoffen, daß die Kostenfreiheit zumindest dieser Auskunftssperre in § 23 Abs. 1 SächsMG festgeschrieben wird. Jedenfalls hat das SMI die Bereitschaft zu einer entsprechenden Gesetzesergänzung nur vage angedeutet.

Ich werde mich weiter nachhaltig für die Kostenfreiheit einsetzen, zumal Gebühren für die Eintragung melderechtlicher Auskunftssperren außer in Sachsen nur noch in drei weiteren Bundesländern erhoben werden. Dabei werde ich mich auch auf das Urteil des OVG Saarland vom 27. November 1990, 1 R 482/88-1 K 215/87 berufen, wonach die der Nr. 91, Tarifstele 2.1 SächsKV entsprechende saarländische Gebührenstelle im Gebührenverzeichnis für *ungültig* erklärt wurde.

c) *Zweckbindung und Auflagen bei Jubiläumsauskünften und Datenübermittlungen an Adreßbuchverlage (§ 33 Abs. 2 und 3 SächsMG)*

Während in § 33 Abs. 1 SächsMG ausdrücklich darauf verwiesen wird, daß Meldedatenübermittlungen an politische Parteien usw. dem Zweckbindungsgrundsatz unterliegen und von Auflagen abhängig gemacht werden können, fehlen solche Verweisungen bei den Jubiläumsdaten und bei den Datenübermittlungen an Adreßbuchverlage.

Eine Ergänzung des § 33 Abs. 2 und 3 SächsMG halte ich für erforderlich.

5.3.2 Meldedatenübermittlungen innerhalb des öffentlichen Bereichs

5.3.2.1 Stellungnahme zum Entwurf einer Sächsischen Meldedatenübermittlungsverordnung

Nach § 36 Nr. 4 SächsMG ist das SMI ermächtigt, regelmäßige Datenübermittlungen oder automatisierte Abrufverfahren durch Rechtsverordnung zuzulassen.

Den mir übersandten Entwurf einer Sächsischen Meldedatenübermittlungsverordnung habe ich schwerpunktmäßig wie folgt bewertet:

5.3.2.1.1 Unzureichender Schutz bei Auskunftssperren

Gemäß § 3 Abs. 1 des Entwurfs hat die Meldebehörde bei Auskunftssperren nach § 34 SächsMG den Empfängern einen "entsprechenden Hinweis" zu geben. Diese Vorschrift bietet nach meiner Auffassung keinen hinreichenden Schutz für die Betroffenen. Regelmäßige Datenübermittlungen sollten auf jeden Fall ausgeschlossen sein, wenn die Voraussetzungen des § 32 Abs. 4 SächsMG vorliegen (Gefahr für Leben, Gesundheit

etc.). Außerdem bestehen nicht unerhebliche Bedenken gegen regelmäßige Datenübermittlungen an öffentlich-rechtliche Religionsgesellschaften (aber auch an andere Stellen), wenn eine Auskunftssperre nach § 1758 Abs. 2 BGB (Adoptionspflege) gespeichert ist.
Ich habe angeregt, *konkrete Übermittlungssperren* in die Verordnung einzuarbeiten.

5.3.2.1.2 Unzulässigkeit regelmäßiger Datenübermittlung an die Finanzämter

Der Entwurf sieht vor, daß die Meldebehörden regelmäßig Daten "für Zwecke der Besteuerung sowie zur Sicherung des Steueraufkommens" an die Finanzämter übermitteln. Diese Vorschrift ist nach meiner Auffassung deswegen unzulässig, weil im Falle von regelmäßigen Datenübermittlungen bei den Finanzbehörden praktisch ein zweites - wenn auch verkürztes - Melderegister entstehen würde. Gemäß § 2 Abs. 1 SächsMG sind ausschließlich *die Gemeinden* Meldebehörden. Außerdem wäre die Übermittlung der in der Vorschrift genannten Daten *aller* Einwohner gemäß § 29 Abs. 1 SächsMG nicht erforderlich (und daher nicht von der Verordnungsermächtigung des § 36 Nr. 4 SächsMG gedeckt), weil nicht jeder im Melderegister gespeicherte Einwohner als Abgabepflichtiger in Bezug zum Finanzamt steht.

5.3.2.1.3 Online-Anbindungen der Polizeidienststellen und des Landesamtes für Verfassungsschutz an die Melderegister

Mit der Meldedatenübermittlungsverordnung sollen die Polizeidienststellen und das Landesamt für Verfassungsschutz die Befugnis erhalten, im automatisierten Verfahren personenbezogene Daten bei den Meldebehörden abzurufen. Ein automatisiertes Abrufverfahren ist nach § 8 Abs. 1 SächsDSG nur zulässig, wenn dies ein Gesetz *ausdrücklich* vorsieht. Gesetze im Sinne dieser Vorschrift sind ausschließlich *formelle* Bundes- und Landesgesetze; Rechtsverordnungen und Satzungen, die unter den materiellen Gesetzesbegriff fallen, kommen nicht in Betracht (vgl. meine Bekanntmachung vom 29. Juni 1994, unten 16.1.1).

Somit ist zunächst zu klären, welche bereichsspezifischen Gesetze als Grundlage eines automatisierten Abrufverfahrens (Online-Verfahren) in Betracht kommen:

a) Für die Polizei
   Das Sächsische Polizeigesetz enthält mit § 48 eine Vorschrift, die die Einrichtung automatisierter Abrufverfahren ausdrücklich erlaubt - allerdings mit der wesentlichen Einschränkung, daß lediglich Datenübermittlungen *zwischen Polizeidienststellen* Gegenstand des Verfahrens sein dürfen. Damit sind die polizeilichen Online-Befugnisse abschließend geregelt, es sei denn, das SächsMG enthielte eine an die Polizei gerichtete, im Sinne des § 8 Abs. 1 SächsDSG *ausdrückliche* Vorschrift zum automatisierten Abrufverfahren. Dies ist aber nicht der Fall: § 29 Abs. 5 SächsMG spricht nur unbestimmt von "Behörden oder sonstigen öffentlichen Stellen", die als Adressaten regelmäßiger Datenübermittlungen in Betracht kommen können; eine notwendige explizite Benennung der am automatisierten Abrufverfahren beteiligten Stellen, wie sie z. B. vorbildhaft in § 36 StVG normiert wird, fehlt jedoch.

Die Ermächtigung des SMI nach § 36 Nr. 4 SächsMG, durch Rechtsverordnung regelmäßige Datenübermittlungen und den automatisierten Abruf zuzulassen, kann daher nicht als tragfähige Grundlage des automatisierten Abrufverfahrens herangezogen werden, weil der das Verfahren konkretisierenden Rechtsverordnung die erforderliche Normqualität fehlt (lediglich formelle Gesetze sind ausreichend; vgl. oben). Daß § 36 Nr. 4 SächsMG nicht als befugnisbegründende Norm in Frage kommt, ergibt sich auch aus folgender Überlegung: Mit Hilfe der Verordnungsermächtigung hätte es die Exekutive in der Hand, Datenverarbeitungsbefugnisse öffentlicher Stellen zu erweitern, deren Grenzen der Gesetzgeber zuvor aufgrund des Ergebnisses der parlamentarischen Beratung bereichsspezifisch bewußt eng gefaßt hat.

b) Für den Verfassungsschutz

Gleiches gilt für die Beteiligung des Landesamtes für Verfassungsschutz an einem automatisierten Meldedaten-Abrufverfahren. Die Datenverarbeitung des Landesamtes kann nur auf der Grundlage des Bundesverfassungsschutzgesetzes und des Sächsischen Verfassungsschutzgesetzes erfolgen. Diese Gesetze beschreiben detailliert die Voraussetzungen, die erfüllt sein müssen, damit die vorwiegend ohne Wissen des Betroffenen durchgeführten und damit stets durch große Eingriffstiefe für das Persönlichkeitsrecht geprägten Datenverarbeitungsvorgänge als rechtmäßig gelten. Dagegen enthält das Sächsische Meldegesetz keine entsprechenden ausschließlich dem Verfassungsschutz gewidmeten Regelungen, die es als bereichsspezifisches Gesetz klassifizieren würden.

Im übrigen bräche die geplante Online-Regelung des § 9 des Entwurfs ein bislang nicht angetastetes Tabu:

Nach den Gesetzen für die Nachrichtendienste der Bundesrepublik Deutschland ist die Einrichtung automatisierter Abrufverfahren allgemein ausgeschlossen, da nach § 27 BVerfSchG, § 13 MADG, § 11 BNDG jeweils § 10 BDSG nicht anzuwenden ist. Im Entwurf des BVerfSchG (BT-Drs. 11/4306, S. 24 ff.) in der Fassung der Beschlüsse des Innenausschusses des Deutschen Bundestages (BT-Drs. 11/7235, S. 69), war noch eine bereichsspezifische Regelung zum automatisierten Abrufverfahren enthalten (§ 23), wonach allerdings

- eine unbefristete Einrichtung dieses Übermittlungsverfahrens ausgeschlossen war und
- die befristete Einrichtung "extremen Ausnahmesituationen ... einer Massierung terroristischer Anschläge" (Entwurfsbegründung, BT-Drs. 11/4306, S. 64) vorbehalten blieb, nämlich wenn "eine erhebliche Beeinträchtigung der freiheitlichen demokratischen Grundordnung droht oder eine konkrete Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes besteht" (Entwurf § 23 Satz 1).

Selbst eine solche restriktive Regelung ist dem Gesetzgeber zu weit gegangen (vgl. BT-Drs. 11/7504, Nr. 32). Eine spezialgesetzliche Regelung, die demgegenüber sogar noch unter wesentlich verminderten Voraussetzungen die Einrichtung des Abrufverfahrens zuließe, müßte mit ganz außergewöhnlichen Umständen begründet werden können.

Bereichsspezifische Besonderheiten für eine derart außergewöhnliche Regelung sind nicht ersichtlich. Auch im Vergleichsfall des Verkehrszentralregisters (ZEVIS) haben die Nachrichtendienste mit § 36 StVG wohlweislich keinen Online-Zugriff erhalten.

Ergebnis: Die Einführung automatisierter Abrufverfahren im Meldebereich kann im Hinblick auf § 8 Abs. 1 SächsDSG nicht durch eine Rechtsverordnung geregelt werden. Als Regelungsort kommt nur ein bereichsspezifisches *Gesetz* in Frage; dieses könnte auch das SächsMG sein.

Ungeachtet dieser grundsätzlichen Kritik begegnet der Entwurf weiteren gravierenden Bedenken:

Dem Wortlaut des § 8 zufolge sollen Polizeidienststellen bei den Meldebehörden abrufberechtigt sein. Eine regionale Begrenzung ist ersichtlich nicht vorgesehen. Vielmehr sollen sämtliche Polizeidienststellen den Zugriff auf die Daten sämtlicher Meldebehörden erhalten, damit "polizeiliche Aufgaben" erfüllt werden, ohne daß weitere online-bezogene Nutzungsvoraussetzungen erfüllt sein müssen. Regelungen zur Relevanzprüfung und Löschungsverpflichtung fehlen gänzlich.

Faktisch steht mit Hilfe der Vorschrift jeder Polizeidienststelle der Direktzugriff auf den sich stets aktualisierenden sächsischen Meldedaten(teil)bestand zur Verfügung. Dieser landesweite Direktzugriff verstößt angesichts der polizeilichen Aufgabenerfüllung, die stets einzelfallbezogen zu erfolgen hat, gegen das verfassungsmäßige Übermaßverbot. Stichprobenartige Kontrollen in den alten Bundesländern haben gezeigt, daß der Online-Zugriff auch nicht mit einem hohen Anfragebedarf zu Nachtzeiten und am Wochenende begründet werden kann. Abgesehen von den Großstädten wurden die Meldebehörden durch *örtliche* Polizeidienststellen nur selten in Anspruch genommen. Um so weniger dürften Polizeidienststellen einen Direktzugriff auf Melderegister entfernt liegender Orte benötigen. Sie können innerhalb weniger Minuten telefonisch eine Auskunft erhalten. Das Argument, wertvolle Zeit würde hierüber verloren gehen, kann nur dann überzeugen, wenn zum einen die große Zahl der Datenanfragen, zum anderen die Abwägung aller betroffenen Rechtsgüter (Aufgabe der beteiligten Stelle unter Berücksichtigung der schutzwürdigen Belange der Betroffenen) zu dem Ergebnis führt, die Einrichtung sei angemessen. Demgegenüber bewirken technische Hürden, daß auch nur wirklich erforderliche Daten abgefragt werden. Wenn die Mehrheit der Flächenländer, insbesondere diejenigen, die größer als Sachsen sind, ohne einen landesweiten Direktzugriff auf Meldedaten oder - wie Baden-Württemberg - überhaupt ohne Abrufverfahren auskommt, erscheint der für Sachsen geplante zentrale Zugriff um so weniger als verhältnismäßig.

Darüber hinaus steht der Referentenentwurf in Widerspruch zur gesetzgeberischen Strukturentscheidung, die Melderegister dezentral bei den Gemeinden einzurichten. Zwar sah bereits der 1978 von der Bundesregierung vorgelegte Entwurf eines Bundesmeldegesetzes Landesadreßregister für polizeiliche Zwecke vor. Aufgrund der Ergebnisse einer Sachverständigenanhörung im Bundestag hat der Gesetzgeber jedoch ausdrücklich auf die Einführung dieser Register verzichtet.

5.3.2.2 Online-Anschluß der Standesämter an das Melderegister

Der SSG fragte, unter welchen Voraussetzungen Standesämtern ein automatisierter Zugriff auf Melderegisterdaten gestattet werden kann.

Hierzu habe ich ausgeführt, daß die Meldebehörde nach § 29 Abs. 7 SächsMG anderen kommunalen Dienststellen *innerhalb der Gemeinde* Melderegisterdaten - auch im Onlineverfahren - übermitteln darf, soweit diese Daten zur (rechtmäßigen) Aufgabenerfüllung des Datenempfängers (hier Standesamt) *erforderlich* sind.

Aus datenschutzrechtlicher Sicht muß danach also gewährleistet sein, (z. B. durch Begrenzung des Datenumfanges in der Bildschirmmaske), daß dem Standesamt nur für das Personenstandswesen erforderliche Meldedaten übermittelt werden. Nicht erforderlich sind z. B.
- Paß- und Personalausweisdaten
- Paßversagungsdaten
- Wehrüberwachungsdaten
- lohnsteuerrelevante Daten
- Wahlausschlußdaten.

Die Zulässigkeit solcher automatisierter Abrufverfahren innerhalb der Gemeinde ist weiterhin von der Beachtung des § 8 Abs. 2 und 3 SächsDSG abhängig. Zu Einzelheiten hierzu verweise ich auf meine Bekanntmachung vom 29. Juni 1994, unten 16.1.1.

Standesämtern außerhalb der Gemeinde ist derzeit ein Online-Zugriff auf Melderegisterdaten (anderer Gemeinden) aus rechtlichen Gründen verwehrt (§§ 29 Abs. 5, 36 Nr. 4 SächsMG).

Der SSG hat seine Mitglieder im vorstehenden Sinne informiert.

5.3.2.3 Zugriffsrechte des Landratsamtes auf Melderegisterdaten

Ein Landratsamt forderte die kreisangehörigen Gemeinden auf, ihm zur Aufgabenerfüllung einen Direktzugriff auf die bei der Firma Alldata GmbH automatisiert geführten Melderegister zu gewähren. Einige Gemeinden kamen kritiklos dieser Aufforderung nach. Eine Stadt allerdings informierte mich.

Das Landratsamt übersah, daß der beabsichtigte automatisierte Zugriff auf die Meldedaten der kreisangehörigen Gemeinden unzulässig ist, weil weder Bundes- noch Landesrecht eine solche Vorgehensweise legitimieren (§ 29 Abs. 5 SächsMG). Eine Verordnung des SMI (§ 36 Nr. 4 SächsMG) über den automatisierten Abruf von Meldedaten durch Landratsämter ist meines Wissens nicht im Gespräch.

Meiner Forderung entsprechend hat das Landratsamt sowohl die kreisangehörigen Gemeinden als auch die Alldata von der Unzulässigkeit unterrichtet und bereits erteilte Einwilligungserklärungen an die Gemeinden zurückgegeben.

Dieser Fall ist wieder einmal Beispiel dafür, daß sich viele kreisangehörige Gemeinden (immer noch) per se auf die Rechtmäßigkeit von Forderungen des Landratsamtes verlassen, ohne selbst das verfassungsmäßige Gebot der Gesetzmäßigkeit der Verwaltung (Art. 20 Abs. 3 GG, Art. 3 Abs. 3 SächsVerf) im Rahmen ihres kommunalen Selbstverwaltungsrechts (Art. 28 Abs. 2 GG, Art. 82 Abs. 2 SächsVerf) zu beachten.

5.3.2.4 Regelmäßige Meldedatenübermittlungen an die Landratsämter (Abfallwirtschaftsämter)

Nach meinen Erkenntnissen wird der Berechnung von Müllgebühren im Freistaat vorwiegend der Personenmaßstab zugrundegelegt. Die Gebührenhöhe orientiert sich an der Anzahl der Personen in einem Haushalt zu einem bestimmten Stichtag. Die Abfallwirtschaftsämter fordern daher von den Meldebehörden die regelmäßige Übermittlung von Einwohnerdaten.

Diese Aufforderung erfolgt offensichtlich in Unkenntnis von §§ 29 Abs. 5, 36 Nr. 4 SächsMG, wonach die regelmäßige Meldedatenübermittlung durch Bundes- oder Landesrecht, zumindest aber durch Rechtsverordnung des SMI geregelt sein muß.

Da bisher eine solche gesetzliche Regelung in Sachsen fehlt, dürfen die Meldebehörden nicht zur (rechtswidrigen) Meldedatenübermittlung aufgefordert werden. Auf Art. 20 Abs. 3 GG, Art. 3 Abs. 3 SächsVerf (Bindung der Verwaltung an Recht und Gesetz) weise ich hin.

Meldedatenübermittlungen würden schließlich zu einem - wenn auch verkürzten - zentralen Einwohnerregister beim Abfallwirtschaftsamt des Landkreises führen, was den Intentionen des § 1 SächsMG (Meldebehörden sind die Gemeinden, und nur diese haben ein Melderegister zu führen) zuwiderliefe.

Datenschutzrechtlich nicht zu beanstanden wäre eine Mitteilung der Meldebehörden an das Abfallwirtschaftsamt, *wieviele* Personen zu einem bestimmten Stichtag unter einer bestimmten Adresse gemeldet waren.

5.3.2.5 Auswertung von Gästemeldescheinen durch die Polizei

Der Betreiber einer Pension wies mich auf ein Schreiben einer Polizeidirektion hin, wonach beabsichtigt sei, die Gästemeldescheine im Rahmen des § 19 Abs. 4 SächsMG zu kontrollieren. Hierzu sollte der Pensionsbetreiber die Meldescheine in *doppelter* Ausfertigung ausfüllen lassen, um jeweils ein Exemplar der Polizei zur Verfügung zu stellen. Ich habe die Polizeidirektion darauf hingewiesen, daß nach § 2 MVVO die doppelte Ausfertigung der Meldescheine für Beherbergungsstätten nicht vorgesehen und die Aufforderung an den Pensionsbetreiber nicht rechtmäßig sei.

Die Polizeidirektion begründete ihre Aufforderung damit, daß einmal von der Polizei abgeholte Gästemeldescheine nicht mehr an den Leiter des Beherbergungsbetriebes zurückgegeben werden müßten. Dieser Auffassung vermochte ich nicht zu folgen, weil

die (auf eigene Kosten) nach § 19 Abs. 1 SächsMG vom Leiter der Beherbergungsstätte zu beschaffenden und bereitzuhaltenden Meldescheine auch von diesem nach § 19 Abs. 3 SächsMG aufzubewahren und vor unbefugter Einsichtnahme zu sichern sind. Auch die Löschungsverpflichtung nach § 19 Abs. 4 SächsMG trifft den Leiter der Beherbergungsstätte, so daß im Ergebnis die Meldescheine nach deren Auswertung von der Polizei *zurückgegeben werden müssen*. Eine Aufbewahrung bei der Polizei würde nämlich dazu führen, daß dort eine nicht-automatisierte Datei im Sinne von § 3 Abs. 5 Nr. 2 SächsDSG mit personenbezogenen Daten einer Vielzahl von Betroffenen entstünde, die vom polizeilichen Aufgabenbereich nicht umfaßt ist. Dies käme einer unzulässigen Vorratsspeicherung gleich.

Das von mir beteiligte SMI hat meiner Bitte, die Polizeidienststellen über diese Rechtslage zu informieren, bisher nicht entsprochen; ich muß wohl weiter Überzeugungsarbeit leisten.

5.3.3 Melderegisterauskünfte an den nicht-öffentlichen Bereich

5.3.3.1 Auskünfte aus gemeindlichen Unterlagen an den Internationalen Suchdienst Arolsen (ISD)

Der humanitäre Auftrag des ISD, nationalsozialistisches Unrecht wiedergutmachen zu helfen (siehe auch Nr. 5.8.4 meines 2. Tätigkeitsberichtes), ist Ausgangspunkt für umfangreiche Nachforschungen in den Meldedatenbeständen der Gemeinden. Zusammen mit dem SMI hatte ich zu beurteilen, unter welchen Voraussetzungen dem ISD Einsicht in personenbezogene Unterlagen über den betroffenen Personenkreis (Vermißte, Verschleppte, Zwangsarbeiter usw.) gewährt werden kann.

Dem ISD und den sächsischen Gemeinden haben wir folgendes mitgeteilt:

1. In erster Linie dürfte es sich bei den für den ISD interessanten Unterlagen über die Betroffenen um *Archivgut* handeln. Insoweit ist für die Einsichtnahme das Sächsische Archivgesetz, insbesondere die §§ 13 in Verbindung mit 9 und 10, einschlägig.

2. Sollte es sich bei den Unterlagen nicht um Archivgut handeln, sondern um Daten, die ausnahmsweise dem SächsMG unterliegen (z. B. alte Meldekarteien), scheidet eine Durchsicht durch Mitarbeiter des ISD dann aus, wenn darin auch Daten nichtbetroffener Personen enthalten sind (es würden mehr Daten als für den ISD erforderlich übermittelt). Aber auch wenn die Meldebehörde eine Kartei ausschließlich über Betroffene zur Verfügung stellen könnte, schiede eine Durchsicht durch Mitarbeiter des ISD dann aus, wenn darin mehr Daten als melderechtlich vorgesehen (§ 5 SächsMG) enthalten wären (davon ist regelmäßig auszugehen).

   Allerdings bestünde die Möglichkeit, dem ISD aus diesen Karteien eine sog. Gruppenauskunft nach § 32 Abs. 3 SächsMG zu erteilen. Das für eine solche Gruppenauskunft erforderliche "öffentliche Interesse" ist wegen des humanitären Auftrags des ISD anzunehmen.

Da der für den ISD interessante Personenkreis jedoch überwiegend verzogen oder verstorben sein dürfte, haben die Meldebehörden einer Auskunftserteilung auch § 26 Abs. 4 SächsMG zugrundezulegen. Gegen eine Übermittlung der dort genannten Daten an den ISD habe ich keine Bedenken, weil die Auskünfte zur Behebung einer bestehenden Beweisnot unerläßlich sind. Die ansonsten erforderliche schriftliche Einwilligung der Betroffenen wird in aller Regel nicht (mehr) beigebracht werden können.

3. Sollte es sich um Unterlagen handeln, die weder Archivgut noch Meldedaten sind (z. B. eine eigene Fremdarbeiterkartei), so beurteilt sich die Datenübermittlung (einschließlich Durchsicht durch den ISD) nach §§ 3 Abs. 2 Nr. 5 Buchst. b, 15 Abs. 1 Nr. 2 SächsDSG (berechtigtes Interesse = ja; schutzwürdige Belange = nein). Die in § 15 Abs. 3 SächsDSG vorgesehene vorherige Anhörung und nachträgliche Unterrichtung der Betroffenen dürfte in aller Regel nicht (mehr) möglich sein (verzogen, verstorben). Behördliche Nachforschungen über den Verbleib der Betroffenen wären unverhältnismäßig - also ein schwerwiegender öffentlicher Belang -, so daß auch deshalb von den Verpflichtungen des § 15 Abs. 3 SächsDSG abgegangen werden kann.

4. Handelt es sich um Unterlagen, die besonderen Geheimhaltungsvorschriften (z. B. Sozialgeheimnis, Arztgeheimnis, Steuergeheimnis) unterliegen, sollte man versuchen, die Einwilligung der Betroffenen bzw. ihrer Hinterbliebenen einzuholen.

5.3.3.2 Gruppenauskünfte an Adreßbuchverlage

In den sächsischen Städten werden in zunehmendem Maße Adreßbücher herausgegeben. Hierzu übermitteln die Meldebehörden Einwohnerdaten an einen Adreßbuchverlag zum Zwecke der Veröffentlichung.

Zahlreiche Anfragen betroffener Einwohner, aber auch von Gemeinden, machten Defizite beim Vollzug des Sächsischen Meldegesetzes deutlich.

Nach § 33 Abs. 3 und 4 SächsMG darf die Meldebehörde Vor- und Familiennamen, Doktorgrad und Anschriften der volljährigen Einwohner in *alphabetischer Reihenfolge* der Familiennamen in Adreßbüchern und ähnlichen Nachschlagewerken veröffentlichen und an andere zum Zecke der Herausgabe solcher Werke übermitteln.

Von einer Veröffentlichung oder Übermittlung ausgeschlossen sind die Daten von Inhaftierten, Patienten in Krankenhäusern, Pflegeheimen und ähnlichen Einrichtungen sowie bei einer bestehenden Auskunftssperre. Außerdem scheidet eine Veröffentlichung oder Übermittlung dann aus, wenn der Betroffene gegenüber der Meldebehörde *widersprochen* hat. Auf dieses Widerspruchsrecht hat die Meldebehörde hinzuweisen
- bei der Anmeldung und
- spätestens zwei Monate vor der Veröffentlichung oder Übermittlung; dabei kann für die Ausübung des Widerspruchsrechts eine Frist bestimmt werden, die nicht weniger als einen Monat betragen darf.

Der Gesetzgeber ist bei der Schaffung dieser Bestimmung davon ausgegangen, daß Adreßbücher grundsätzlich im öffentlichen Interesse liegen, weil damit einem berechtigten Informationsbedürfnis der Öffentlichkeit entsprochen wird. Außerdem werden die Meldebehörden durch derartige Adreßbücher von zahlreich zu erwartenden Auskunftsbegehren entlastet. Als Ausgleich gegen den mit der Veröffentlichung personenbezogener Daten verbundenen Eingriff in das Recht auf informationelle Selbstbestimmung wurde den Einwohnern das Widerspruchsrecht eingeräumt.

Positiv bewerte ich die Einschränkung, daß die Einwohnerdaten nur in alphabetischer Reihenfolge - nicht also straßenweise - veröffentlicht werden dürfen. Die Meldebehörde sollte die Datenübermittlung an den Adreßbuchverlag von der Einhaltung dieser Auflage abhängig machen. Damit würde das hin und wieder festgestellte Angebot entfallen, den Adreßbuch-Datenbestand auch auf CD-ROM, also jederzeit umsortierbar, zur Verfügung zu stellen. Eine straßenweise Sortierung kann nämlich sehr wohl schutzwürdige Interessen der Betroffenen (z. B. alleinstehender Frauen) beeinträchtigen.

5.3.3.3 Gruppenauskünfte an politische Parteien, Wählergruppen und andere Träger von Wahlvorschlägen

Im "Superwahljahr" 1994 war zu erkennen, daß sich politische Parteien usw. in zunehmendem Maße zum Zwecke der Wahlwerbung Wähleranschriften von den Meldebehörden übermitteln ließen.

a) *Rechtsgrundlagen, Allgemeines*

Nach § 33 Abs. 1 SächsMG in Verbindung mit § 22 MRRG *darf* die Meldebehörde Parteien, Wählergruppen und anderen Trägern von Wahlvorschlägen (z. B. Wählergemeinschaften) in den sechs diesen Wahlen vorangehenden Monaten Auskünfte über
- Familiennamen
- Vornamen
- Doktorgrad
- gegenwärtige Anschrift

(nicht also Geburtsdatum)
von Gruppen von Wahlberechtigten (z. B. Jungwähler, Seniorenwähler) erteilen, für deren Zusammensetzung das Lebensalter bestimmend ist, sofern die Wahlberechtigten hiergegen nicht widersprochen haben (und wenn keine Auskunftssperre nach §§ 34 und 32 Abs. 4 gespeichert ist oder der Betroffene für eine JVA, für ein Krankenhaus, Pflegeheim oder eine ähnliche Einrichtung im Sinne von § 20 Abs. 1 SächsMG gemeldet ist).

Da als einziges Auswahlkriterium das Lebensalter der Wahlberechtigten maßgebend ist, scheidet eine (regionale) Auswahl z. B. nach Ortsteilen oder eine Auswahl nach Geschlecht generell aus. Ebenso ist eine Übermittlung des Gesamtwählerbestandes unzulässig. Auch dürfen außerhalb der Sechsmonatsfrist keine Wähleranschriften mitgeteilt werden (§ 33 Abs. 1 SächsMG geht als lex specialis § 32 Abs. 3 SächsMG vor).

Über die Herausgabe von Wähleranschriften an politische Parteien usw. nach § 33 Abs. 1 SächsMG entscheidet die jeweilige Meldebehörde nach pflichtgemäßem Ermessen (die Meldebehörde "darf" ....).

Bei der Entscheidung, politischen Parteien usw. Gruppenauskünfte nach § 33 Abs. 1 SächsMG zu erteilen, hat die Meldebehörde stets auch den Gleichbehandlungsgrundsatz (§ 5 Parteiengesetz) zu beachten (entweder erhalten grundsätzlich *alle*, also auch die von den Verfassungsschutzbehörden als extremistisch eingestuften politischen Parteien usw., die es beantragen, Gruppenauskünfte oder *keine*). Nur in konkreten Einzelfällen, wenn Tatsachen bekannt sind, die auf Unzuverlässigkeit der Partei schließen lassen (z. B. weil in der Vergangenheit massiv gegen datenschutzrechtliche Auflagen verstoßen worden ist), ist eine Auskunftsverweigerung denkbar.

Insbesondere weil auch extremistische Parteien (ebenso wie die etablierten Parteien) Wähleranschriften erhalten können, ist es wichtig,
- die Einwohner ausdrücklich und nachhaltig gemäß § 33 Abs. 4 Nrn. 1 und 2 SächsMG auf ihr Widerspruchsrecht hinzuweisen (bei der Anmeldung und durch ortsübliche Bekanntmachung, z. B. wiederholt in der Presse, gemeindlichen Mitteilungsblättern, an Ortstafeln)
- die Gruppenauskunft von restriktiven Auflagen abhängig zu machen.

b) *Widerspruchsrecht*

Die Wahlberechtigten haben gemäß § 33 Abs. 1 SächsMG (in Verbindung mit § 22 MRRG) das Recht, der Weitergabe ihrer Daten an politische Parteien usw. zu widersprechen.

Der Widerspruch ist an keine Form gebunden; er ist *nicht* zu begründen und er ist *kostenfrei.* Wird er schriftlich bei der für die Wahlberechtigten zuständigen Meldebehörde eingelegt, so sollte dies unter Angabe des Namens, Vornamens, Geburtsdatums sowie der gegenwärtigen (Haupt-) Wohnanschrift erfolgen. Bei persönlicher Vorsprache sollte sich der Widersprechende durch Vorlage von Personalpapieren ausweisen.

Die Wahlberechtigten können ihren Widerspruch gegen die Weitergabe ihrer Daten an politische Parteien usw. nur *einheitlich* geltend machen. Dies bedeutet, daß ein eingelegter Widerspruch *alle* Wahlen einschließt und gegenüber *allen* Parteien, Wählergruppen und anderen Trägern von Wahlvorschlägen gilt (keine Wahlfreiheit für den Betroffenen, welcher Partei usw. seine Daten übermittelt werden dürfen und welcher nicht). Die Meldebehörde darf deshalb nur uneingeschränkte Widersprüche beachten. Gegebenenfalls ist der Widerspruchsführer entsprechend aufzuklären.

Die Widersprüche der Wahlberechtigten werden im Melderegister zeitlich unbegrenzt gespeichert. Eine Löschung erfolgt nur bei Widerruf des Betroffenen.

c) *Entbehrlichkeit des Widerspruchs (insbesondere § 33 Abs. 4 SächsMG)*

Folgende Personen brauchen ihren Widerspruch nicht gesondert zu erklären:

- Einwohner, die bereits bei der Anmeldung erklärt haben, daß sie mit der Weitergabe ihrer Daten im Zusammenhang mit Wahlen usw. nicht einverstanden sind,
- Einwohner, bei denen eine Auskunftssperre nach § 34 Abs. 1 SächsMG, insbesondere wegen Gefahr für Leben, Gesundheit, persönliche Freiheit oder ähnliche schutzwürdige Belange (§ 32 Abs. 4 SächsMG), im Melderegister gespeichert ist,
- Einwohner, die für eine Justizvollzugsanstalt, für ein Krankenhaus, Pflegeheim oder eine ähnliche Einrichtung im Sinne von § 20 Abs. 1 SächsMG gemeldet sind.

d) *Datenschutzauflagen (§§ 33 Abs. 1 Satz 3, 32 Abs. 5 und 6 SächsMG)*

Die Meldebehörde sollte die Gruppenauskünfte an politische Parteien usw. von nachstehenden Auflagen abhängig machen (Mindeststandard):
- Die Wählerdaten dürfen nur zum Zwecke der Wahlwerbung verwendet werden (in diesem Zusammenhang empfiehlt es sich, nur Adreßaufkleber zur Verfügung zu stellen),
- sie dürfen Dritten nicht zugänglich gemacht werden,
- mit ihnen darf kein Datenabgleich und keine Verknüpfung mit anderen Dateien vorgenommen werden,
- sie dürfen nicht zusammen mit Adreßdaten anderer Herkunft gespeichert werden,
- sie sind *spätestens* einen Monat nach der Wahl zu löschen.

Von den Datenempfängern sollte eine entsprechende schriftliche Verpflichtungserklärung verlangt werden. Selbstverständlich kann die Erteilung der Gruppenauskunft von weiteren Auflagen abhängig gemacht werden, um sicherzustellen, daß die Datenempfänger ihren vorgenannten Verpflichtungen nachkommen. Außerdem sollten die Datenempfänger darauf hingewiesen werden, daß Verstöße gegen vorstehende Auflagen gemäß § 35 Abs. 2 Nrn. 3 und 4 SächsMG als Ordnungswidrigkeit mit einer Geldbuße bis zu 10.000,- DM geahndet werden können (§ 35 Abs. 3 SächsMG).

5.3.3.4 Telefonische (Melderegister-)Auskünfte

Grundsätzlich sehen die Auskunfts- und Übermittlungsvorschriften an Private (z. B. § 15 SächsDSG, § 32 SächsMG) eine besondere Form der Auskunftserteilung nicht vor. Damit sind telefonische Auskünfte nicht von vornherein ausgeschlossen, wenn die Identität des Auskunftssuchenden eindeutig feststeht. Bei Melderegisterauskünften an öffentliche Stellen (z. B. Polizei, Finanzamt) wäre z. B. die Vereinbarung eines in regelmäßigen Abständen wechselnden Kennwortes denkbar.

Telefonische Auskünfte an Private (z. B. Inkassobüros, Rechtsanwälte, Kreditauskunfteien) unterliegen jedoch anderen Voraussetzungen als Datenübermittlungen an öffentliche Stellen.

Beispielsweise sehen §§ 15 Abs. 3 SächsDSG, 32 Abs. 2 SächsMG u. a. eine Anhörung des Betroffenen *vor* der Auskunftserteilung vor. Dieser Verpflichtung kann die Behörde regelmäßig bei telefonischen Auskunftsersuchen nicht nachkommen. Ein weiteres - allerdings nicht datenschutzrelevantes - Argument, das gegen telefonische Auskünfte an Private spricht, ist die Kostenfrage (für Auskünfte sieht das SächsKV Gebühren vor), so daß generell an der *schriftlichen* Auskunftserteilung festzuhalten ist. Für das

Schriftformerfordernis spricht auch folgender Beschluß des Bundesverwaltungsgerichts vom 16. März 1988 - 1 B 153/87 (NJW 1988, 2123): *"Die Pflicht zur Führung wahrheitsgetreuer und vollständiger Akten besteht auch hinsichtlich der den Meldebehörden außerhalb der Führung des Melderegisters obliegenden Aufgaben, insbesondere der Führung von Akten über die Einbringung, die Behandlung und die Bescheidung von Anträgern auf Erteilung von erweiterten Auskünften aus dem Melderegister."*

5.3.4 Fragebogenaktion zur Feststellung der Hauptwohnung/Nebenwohnung; Verpflichtung zur Vorlage von Urkunden, Scheidungsurteil u. ä.

§ 12 Abs. 1 SächsMG bestimmt, daß bei mehreren Wohnungen eine Wohnung die *Hauptwohnung* ist.

Hauptwohnung ist die vorwiegend benutzte Wohnung des Einwohners. Hauptwohnung eines verheirateten Einwohners, der nicht dauernd getrennt von seiner Familie lebt, ist die vorwiegend benutzte Wohnung der Familie. In Zweifelsfällen ist die vorwiegend benutzte Wohnung dort, wo der Schwerpunkt der Lebensbeziehungen des Einwohners liegt (§ 12 Abs. 2 SächsMG).

Das Einwohneramt der Stadt Dresden hat zur Klärung der Hauptwohnung Fragebögen an alle mit mehreren Wohnungen gemeldeten Einwohner verschickt. Als Rechtsgrundlage wurde undifferenziert § 12 Abs. 2 SächsMG mit der Folge angegeben, daß auch diejenigen, deren Hauptwohnung sich nach § 12 Abs. 2 *Satz 2* SächsMG bestimmt, die Fragen nach
- Dauer des Aufenthalts in Dresden,
- Entfernung zwischen Dresden und Hauptwohnung,
- Häufigkeit der Fahrten zur Hauptwohnung,
- Eigenschaft als Student,
- Erwerbstätigkeit

beantworten mußten. Die Möglichkeit, eine Erklärung i. S. v. § 12 Abs. 2 Satz 2 (und Satz 3) SächsMG abzugeben, bestand nicht.

Vorstehende Fragen hätten nur dem von § 12 Abs. 2 *Satz 1* SächsMG betroffenen Personenkreis gestellt werden dürfen. Dies hätte in dem Erhebungsbogen deutlich gemacht werden müssen.

Die *Datenerhebung* bei den nicht dauernd von ihrer Familie getrennt lebenden Einwohnern, deren Hauptwohnung die vorwiegend benutzte Wohnung *der Familie* ist (§ 12 Abs. 2 Satz 2 SächsMG), war nicht erforderlich und daher unzulässig.

Weiter habe ich erfahren, daß die Meldebehörde bei der Anmeldung die Vorlage einer Geburtsurkunde, einer Heiratsurkunde und ggf. des Scheidungsurteils verlange. § 14 Nr. 1 SächsMG ermächtigt zwar die Meldebehörde auch Nachweise über die Richtigkeit der Angaben zu verlangen, jedoch nur, soweit es zur Bearbeitung eines meldepflichtigen Vorgangs *erforderlich* ist. Nachweise der bezeichneten Art dürfen deshalb nur gefordert

werden, wenn die Meldebehörde im Einzelfall begründete Zweifel an der Richtigkeit der Angaben des Anmeldenden hat.

Durch die gesetzliche Verpflichtung, bei der Anmeldung den Paß bzw. Personalausweis sowie die Abmeldebescheinigung vorzulegen (§ 13 Abs. 1 SächsMG), ist die Identität des Anmeldenden und die Richtigkeit seiner Angaben in aller Regel nachgewiesen. Die Vorlage der Geburts- und Heiratsurkunde kann daher nur die Ausnahme sein. Auch halte ich die Verpflichtung zur Vorlage des *Scheidungsurteils* für unverhältnismäßig. Gibt der Betroffene bei seiner Anmeldung an, geschieden zu sein, besteht per se kein Anlaß, an der Richtigkeit dieses Datums zu zweifeln (wegen der steuerlichen Auswirkung bei Lohnsteuerklasse 1). Gibt er hingegen an, ledig, verheiratet oder verwitwet zu sein, obwohl er geschieden ist, wird er den entsprechenden Scheidungsnachweis nicht von sich aus erbringen. Die Meldebehörde wird jedenfalls gemäß § 98 der Dienstanweisung für die Standesbeamten und ihre Aufsichtsbehörden (DA) von Personenstandsänderungen (also auch von der Scheidung) unterrichtet, so daß auf das Scheidungsurteil grundsätzlich verzichtet werden kann. Sollte in Ausnahmefällen der Nachweis, daß jemand geschieden ist, erbracht werden müssen, darf nur der *Tenor* des Scheidungsurteils (nicht also die Gründe) oder eine aktuelle standesamtliche Bescheinigung über den Familienstand "geschieden" verlangt werden.

Die Stadt begründet ihre Aufforderung zur Vorlage vorstehender Unterlagen mir gegenüber damit, daß viele Bürger über die Anzahl, Schreibweise und Reihenfolge ihrer Vornamen sowie über Eheschließungsort und -datum im unklaren seien. Das Scheidungsurteil trage bei der Anmeldung von Kindern zur Klärung bei, ob dem Anmeldenden tatsächlich das Personensorge- und Aufenthaltsbestimmungsrecht für diese Kinder zusteht.

Dem habe ich energisch widersprochen und verlangt, daß künftig auf die generelle Anforderung solcher Nachweise verzichtet wird. Die Stadt hat mir bestätigt, die Grundsätze der Verhältnismäßigkeit und Erforderlichkeit künftig auch auf diesem Gebiet zu beachten.

5.3.5 Übertragung des Meldewesens von den Landratsämtern auf die Gemeinden

Nach § 38 Abs. 1 SächsMG sind die Gemeinden (Meldebehörden) verpflichtet, bis spätestens *31. Dezember 1995* das Meldewesen von den Landratsämtern zu übernehmen. Hierfür haben sie die personellen, technischen und organisatorischen Voraussetzungen für eine ordnungsgemäße Wahrnehmung dieser Aufgaben zu schaffen. Ob diese Voraussetzungen erfüllt sind, wird vom Regierungspräsidium festgestellt.

Problematisch wird der Übergang des Meldewesens von den Landratsämtern auf die Gemeinden dann, wenn bisher die automatisierte Melderegisterführung im Auftrag durch ein privates Rechenzentrum erfolgte.

§ 38 Abs. 2 SächsMG geht nämlich davon aus, daß Private die Verarbeitung von Meldedaten im Auftrag der Meldebehörden bis längstens *31. Dezember 1995* nur dann vornehmen dürfen, wenn das Auftragsverhältnis bereits *bei Inkrafttreten des Sächsischen*

Meldegesetzes - also am 13. Mai 1993 - bestanden hat. Das aber hat zur Folge, daß die betroffenen Gemeinden nach diesem Zeitpunkt keinen Privaten mit der Verarbeitung von Meldedaten beauftragen durften.

Gespräche mit dem SMI zu diesem Thema dauern an.

5.3.6 Speicherung von Obdachlosendaten im Melderegister

Die Frage, ob Obdachlosendaten im Melderegister z. B. zum Zwecke der Erteilung von Aufenthaltsbescheinigungen gespeichert werden dürfen, mußte ich im Hinblick auf den abschließenden Datenkatalog des § 5 SächsMG verneinen.

5.3.7 Abgleich von Studentendaten durch eine Meldebehörde beim Studentenwerk

Aufgebrachte Studenten setzten mich davon in Kenntnis, daß die Meldebehörde gegen sie wegen unterlassener Anmeldung Bußgeldverfahren eingeleitet hätte. Pikanterweise wurde die Aufforderung zur Anmeldung und der Anhörungsbogen wegen des Meldeverstoßes (Ordnungswidrigkeit) in den Semesterferien an die Studentenadressen im Wohnheim verschickt. Die gesetzte Frist, die Anmeldung nachzuholen, konnten viele Studenten nicht erfüllen, weil sie sich in der vorlesungsfreien Zeit nicht am Studienort aufhielten.
Tatsächlich hat die Meldebehörde zur Feststellung, ob Studenten ihren An- bzw. Abmeldepflichten nach § 10 SächsMG ordnungsgemäß nachgekommen sind, das Studentenwerk unter Berufung auf § 14 Nr. 2 SächsMG und den Amtshilfegrundsatz aufgefordert, ihr eine Liste *über alle in Studentenwohnheimen wohnenden Personen* zur Verfügung zu stellen. Durch Abgleich dieser Liste mit dem Melderegister wurde festgestellt, daß von rund vierzehntausend überprüften Studenten ungefähr eintausend ihre Meldepflichten verletzt hatten.

Nach § 14 Nr. 2 SächsMG muß der Wohnungsgeber (hier: das Studentenwerk) zwar auf Verlangen der Meldebehörde Auskunft darüber geben, welche Personen bei ihm wohnen oder gewohnt haben, soweit dies zur Bearbeitung eines meldepflichtigen Vorgangs erforderlich ist; jedoch hat der Gesetzgeber durch die Verwendung des Wörtchens "*eines*" zum Ausdruck gebracht, daß das Auskunftsbegehren und die Auskunft des Wohnungsgebers nur *im konkreten Einzelfall* zur Bearbeitung der An- oder Abmeldung eines Betroffenen zulässig sind (z. B. wenn die Angaben des Meldepflichtigen über das Einzugs- oder Auszugsdatum nicht plausibel sind). Der Anforderung der Liste beim Studentenwerk lag kein konkreter Einzelfall zugrunde. Sie war daher - entgegen der Ansicht der Meldebehörde - nicht durch § 14 Nr. 2 SächsMG gedeckt und deshalb unzulässig.

Ich habe das Verhalten der Stadt beanstandet und mitgeteilt, daß auch die Berufung auf die allgemeine *Verpflichtung zur Amtshilfe* die Anforderung der Liste vom Studentenwerk nicht gerechtfertigt hat. Erheben und Übermitteln personenbezogener Daten sind nämlich niemals im Wege der Amtshilfe, sondern nur dann zulässig, wenn ein Gesetz dies erlaubt oder der Betroffene eingewilligt hat (vgl. Art. 33 SächsVerf, § 4 Abs. 1 SächsDSG; Datenschutz ist "amtshilfefest", wie das Bundesverfassungsgericht dies in ständiger

Rechtsprechung betont). Wie bereits dargelegt, läßt das Sächsische Meldegesetz Datenerhebungen beim Wohnungsgeber aber nur *im konkreten Einzelfall* zu.

Das SMI und das für die Universitätsstadt zuständige Regierungspräsidium teilen diese Auffassung. Das Regierungspräsidium hat die Stadt angewiesen, künftig § 14 Nr. 2 SächsMG nur noch unter Berücksichtigung der oben genannten Auslegung anzuwenden. Dem Vernehmen nach hat die Meldebehörde - wenn auch widerstrebend - die Weiterbetreibung der Bußgeldverfahren eingestellt. Gleichwohl werden die betroffenen Studenten ihre Universitätsstadt nicht in angenehmster Erinnerung behalten.

5.4 Wahlrecht

5.4.1 Landeswahlordnung und Verordnung des SMJus zur Durchführung des Gesetzes über Volksantrag, Volksbegehren und Volksentscheid

In meinen Stellungnahmen zum Entwurf der LWO (siehe Nr. 5.4.1 des 2. Tätigkeitsberichts) und der VVVGVO habe ich unter anderem vorgeschlagen, auf die Einrichtung "beweglicher Wahlvorstände", "beweglicher Stimmbezirksvorstände" sowie auf "Sonderwahlbezirke" und "Sonderstimmbezirke" für Patienten, Pflegebedürftige und Personen, die in sozialtherapeutischen Anstalten oder in Justizvollzugsanstalten untergebracht sind, zu verzichten und für diesen Personenkreis generell Briefwahl bzw. Briefabstimmung vorzusehen.

Diesen Vorschlägen ist man nicht gefolgt, obwohl die Betroffenen ein besonderes Interesse daran haben dürften, daß ihr Aufenthalt in solchen Einrichtungen nicht unnötigerweise Dritten bekannt wird. Die Verordnungsgeber (SMI und SMJus) haben insofern dem Grundrecht auf informationelle Selbstbestimmung keinen guten Dienst erwiesen.

Allerdings hat das SMI meine Hinweise aufgegriffen, daß Wahlberechtigten, für die eine Auskunftssperre wegen einer Gefahr für Leben, Gesundheit, persönliche Freiheit und andere schutzwürdige Belange im Melderegister eingetragen ist, beim öffentlich auszulegenden Wählerverzeichnis besonderes Augenmerk geschenkt wird.

5.4.2 Übersendung der Wählerverzeichnisse an das Statistische Landesamt für Wahlstatistikzwecke

Das Statistische Landesamt forderte verschiedene Wahlbehörden auf, zum Zwecke der Wahlstatistik (§ 51 Landeswahlgesetz) die kompletten Wählerverzeichnisse zu übersenden. Diese würden benötigt, um (statistisch) das Wähler-/Nichtwählerverhalten nach Geschlecht und Alter festzustellen.

Dazu genügen jedoch folgende Angaben:
- Vornamen (zur Feststellung des Geschlechts),
- Geburtsjahr,
- Tatsache, ob gewählt wurde oder nicht.

Da § 51 Landeswahlgesetz nicht normenklar regelt, welche Daten aus den Wählerverzeichnissen ans Statistische Landesamt zu übersenden sind, habe ich das SMI gebeten, die

Wahlbehörden zu veranlassen, nur vorstehende, für die Statistik erforderliche Daten zur Verfügung zu stellen. Dies kann z. B. durch ein dupliziertes und um die nicht erforderlichen Daten (Familiennamen, Tag und Monat der Geburt, Wohnadresse) reduziertes (z. B. durch Schwärzen) Wählerverzeichnis bewirkt werden.

Das SMI erwägt eine Änderung der die Wahlstatistik betreffenden Bestimmungen in meinem Sinne.

5.4.3 Befürchtungen von Nichtwählern

Mir bekannt gewordene Mutmaßungen, daß Nichtwählern ein besonderes Augenmerk durch staatliche Stellen geschenkt werden könnte, halte ich im Hinblick auf Art. 20 Abs. 2 GG, Art. 3 Abs. 3 SächsVerf (Gesetzmäßigkeit der Verwaltung) vom Grundsatz her für nicht gerechtfertigt. Das gesamte Wahlrecht des Bundes und der Länder enthält Bestimmungen über die Behandlung der Wählerverzeichnisse (einschließlich deren Sicherung und Vernichtung, z. B. §§ 82, 83 LWO), so daß für eine Zweckänderung kein Raum ist.

Der demokratische Grundsatz der *freien Wahl* schließt Zwang, Druck und alle die freie Willensentscheidung ernstlich beeinträchtigenden Wahlbeeinflussungen seitens des Staates aus (BVerfGE 7, 69; 15, 166; 47, 282; 66, 380), so daß auch Nichtwähler geschützt sind. Eine von diesen Grundsätzen abweichende Handlungsweise wäre rechtswidrig. Auf die §§ 107 ff. StGB weise ich hin.

5.4.4 Speicherung von Wahlausschlüssen

Im 2. Tätigkeitsbericht (vgl. Nr. 5.4.2) bin ich auf die seinerzeitigen Probleme der Wahlbehörden der neuen Bundesländer eingegangen, denen Ausschlüsse vom Wahlrecht und von der Wählbarkeit vielfach zwangsläufig nicht bekannt waren. Um ordnungsgemäße Wählerverzeichnisse erstellen zu können, mußte ein Datenabgleich zwischen den Meldebehörden und dem BZR erfolgen. Hierfür war eine Änderung des Bundeszentralregistergesetzes erforderlich (das 3. BZRÄndG trat am *20. April 1994* in Kraft).

Die praktische Umsetzung erfolgte durch Weisungen des SMI an den nachgeordneten Bereich. Dabei ordnete das SMI unter anderem an, daß in den Datenabgleich mit dem BZR die zum Stichtag 1. März 1994 gemeldeten Einwohner (*einschließlich Nebenwohnungen*) einzubeziehen seien.

Diese Forderung ließ sich mit dem durch § 64 Abs. 1 Kommunalwahlgesetz geänderten § 15 Abs. 1 Satz 2 SächsGemO nicht in Einklang bringen. § 15 Abs. 1 Satz 2 SächsGemO bestimmt nämlich (i. V. m. § 16 SächsGemO), daß nur derjenige wahlberechtigter Bürger ist, der (bei mehreren Wohnungen) seit mindestens drei Monaten seine *Hauptwohnung* in einer sächsischen Gemeinde hat. Wer demnach in Sachsen nur mit Nebenwohnung gemeldet ist (Hauptwohnung in einem anderen Bundesland), ist nicht Bürger im Sinne der Sächsischen Gemeindeordnung und damit auch nicht wahlberechtigt.

Da tatsächlich viele Meldebehörden die Weisung des SMI befolgten, führte dies zu einer *unzulässigen* Datenübermittlung von insgesamt 118.519 Datensätzen von den Meldebehörden an alle am Verfahren beteiligten Stellen.

Das SMI teilte allerdings mit, daß vom BZR keine Wahlausschlüsse bei den Nebenwohnungsinhabern rückgemeldet worden seien, so daß für die Betroffenen keine Nachteile entstanden sein dürften, zumal die Datenträger inzwischen gelöscht sind.

5.5 Kommunale Selbstverwaltung

5.5.1 Die Entwicklung der kommunalen Datenverarbeitung in Sachsen

Das bevorstehende Auslaufen der baden-württembergischen Verfahrenslizenzen sowie das Inkrafttreten des Sächsischen Meldegesetzes bewogen die Staatsregierung und den Sächsischen Städte- und Gemeindetag zu Überlegungen, die kommunale Datenverarbeitung auf nunmehr rechtlich einwandfreie Beine zu stellen. Die bisher in Sachsen praktizierte Auftragsdatenverarbeitung durch private Datenverarbeitungszentralen war nämlich in weiten Teilen rechtswidrig geworden. Soweit sich die Auftragsdatenverarbeitung auf hoheitsrechtliche Bereiche, insbesondere das Melde- und Sozialwesen, die Grund- und Gewerbesteuer sowie das Personalwesen bezieht, hat sie in öffentlicher Hand zu erfolgen.

Darüber hinaus machte die Datenzentrale Baden-Württemberg die weitere Lizenzvergabe für die EDV-Verfahren davon abhängig, daß der Lizenznehmer öffentlich-rechtlich organisiert sein müsse. Davon kann aber keine Rede sein, der SSG ist ein privatrechtlicher e. V.

So entschloß man sich im Jahre 1993 - gegen meine grundsätzlichen Bedenken (vgl. Nr. 5.3.1 meines 2. Tätigkeitsberichts) - durch die Gründung von drei kommunalen Datenverarbeitungszweckverbänden diesen Geboten zu entsprechen. Die Zweckverbände sollten spätestens am 1. Juli 1994 die kommunale Auftragsdatenverarbeitung übernehmen. Außerdem wurde durch den Erlaß des Gesetzes über die Errichtung der Sächsischen Anstalt für kommunale Datenverarbeitung (SAKDG) vom 15. Juli 1994 der Weg für die Schaffung einer öffentlich-rechtlichen Anstalt freigemacht, deren Aufgaben in § 4 SAKDG wie folgt bestimmt sind:

"(1) Aufgabe der SAKD ist es, auf dem Gebiet der Informationstechnik als gemeinsame Beratungs- und Koordinierungsstelle für die Kommunen zu wirken. Planungs-, Organisations-, Personal- und Finanzhoheit der Kommunen bleiben unberührt.
(2) Die SAKD vertritt die Kommunen im Koordinierungsausschuß nach § 12.
(3) Von der SAKD für den kommunalen Bereich erarbeitete Standards und Empfehlungen sind im Sächsischen Amtsblatt zu veröffentlichen.
(4) Die SAKD kann für Produkte und Verfahren der Informationstechnik Zertifikate vergeben.
(5) Die SAKD tritt selbst nicht als Anbieter von Hardware, Software und Organisationslösungen auf und erbringt keine eigenen Datenverarbeitungsleistungen.

(6) Näheres regelt die Satzung."

Mit § 15 SAKDG erfolgte eine Änderung des § 3 SächsMG wie folgt:

"§ 3 Datenverarbeitung im Auftrag der Meldebehörden
Mit der automatisierten Führung des Melderegisters dürfen sowohl in Auftrags- als auch in Unterauftragsverhältnissen nur Einrichtungen des Freistaates Sachsen sowie andere sächsische Gemeinden oder sonstige juristische Personen des öffentlichen Rechts, die der Aufsicht des Freistaates Sachsen unterstehen, beauftragt werden, wenn die Einhaltung dieses Gesetzes, des Sächsischen Datenschutzgesetzes (SächsDSG) vom 11. Dezember 1991 (SächsGVBl. S. 401) und anderer Rechtsvorschriften über den Datenschutz gewährleistet ist."

Gleichzeitig wurde die ursprünglich bis 31. Dezember 1993 vorgesehene und schon einmal hinausgeschobene Übergangsfrist des § 3 Abs. 2 SächsMG um ein weiteres Jahr, nämlich bis *31. Dezember 1995 verlängert*. § 38 Abs. 2 SächsMG lautet nunmehr wie folgt:

"(2) Soweit bei Inkrafttreten dieses Gesetzes Daten im Auftrag der Meldebehörden durch einen Auftragnehmer verarbeitet werden, der den Anforderungen des § 3 nicht entspricht, darf die Datenverarbeitung längstens bis zum 31. Dezember 1995 weitergeführt werden."

In der Praxis hat sich gezeigt, daß die drei Datenverarbeitungszweckverbände trotz wiederholter Fristverlängerung nicht in der Lage waren, die kommunale Datenverarbeitung von den *privaten* Datenverarbeitungszentralen in den öffentlichen Bereich überzuleiten. Zwei der drei Zweckverbände sind bis heute nicht funktionsfähig (kosten den Steuerzahler aber eine Menge Geld).

Aus dieser Misere heraus ließ der Sächsische Städte- und Gemeindetag Ende 1994 ein Gutachten des privaten Software-Entwicklers Ploenzke AG über die zweckmäßigste Form der kommunalen Auftragsdatenverarbeitung erstellen, um zumindest ab 1. Januar 1996 zu einer sachgerechten kommunalen Datenverarbeitungs-Infrastruktur in Sachsen zu gelangen (siehe auch SSG-Mitgliederrundschreiben Nr. 717/94 vom 16.12.1994, Az.: 048.60).

In meinem Gespräch mit dem Gutachter wurde als Zielsetzung des Gutachtens deutlich, daß die Zweckverbände *nicht* die kommunale Datenverarbeitung *durchführen*, sondern als *Koordinator* für die (kleineren) Gemeinden eine ordnungsgemäße Datenverarbeitung gewährleisten sollen, und zwar durch Schaffung der äußeren Bedingungen wie Beratung, Schulung, Betreuung (auch in Form von Soft- und Hardwareempfehlungen). Die eigentliche Auftragsdatenverarbeitung soll hingegen von den privaten Rechenzentren bevorzugt auf das öffentlich-rechtliche Rechenzentrum der Stadt Leipzig übergehen, wofür nach meinem Dafürhalten die Zweckverbände jedenfalls nicht benötigt werden. Da die Sächsische Anstalt für kommunale Datenverarbeitung Koordinierungs- und Beratungsaufgaben wahrnimmt, sind die Zweckverbände für kommunale Datenverarbeitung überflüssig. Sie puffern den notwendigen Einfluß der Einzelgemeinde auf die Datenverarbeitung ab und binden die Gemeinden öffentlich-rechtlich über Gebühr.

Aus alledem wird die bisherige Desorientierung und Konzeptlosigkeit der Verantwortlichen deutlich.

Die favorisierte *Zentralisierung* der kommunalen Auftragsdatenverarbeitung in *einem* öffentlich-rechtlichen Rechenzentrum ist einerseits datenschutzrechtlich abzulehnen und geht zum anderen an der technischen Entwicklung vorbei. Eine renommierte öffentlich-rechtliche Auftragsdatenverarbeitungs-Anstalt eines anderen Bundeslandes, die AKDB in Bayern, machte dies in einem Erfahrungsbericht wie folgt deutlich:

"Schon bald, nämlich 1976, wurde deutlich, daß die ursprüngliche Konzeption, acht regionale Gebietsrechenzentren zu errichten, wirtschaftlich nicht sinnvoll war; denn ab diesem Zeitpunkt zeichnete sich die technologische Weiterentwicklung hin zu leistungsfähigen, preiswerten, dialogorientierten, dezentralen Mehrplatzsystemen ab."

Zu der daraufhin dort rasant einsetzenden Dezentralisierung, die in den anderen Bundesländern nur schleppend begann, gibt die AKDB zu bedenken: "Andere Bundesländer stehen noch vor solchen, sicherlich zum Teil sehr schmerzhaften Anpassungsprozessen."
Diesen Äußerungen kann nur beigepflichtet werden. Ich appelliere deshalb an alle Beteiligten (SMI, SSG, SAKD, Kommunale Datenverarbeitungszweckverbände, nicht zuletzt aber an jede sächsische Gemeinde), die historische Stunde zu nutzen und in der verbleibenden Frist bis zum 31. Dezember 1995 für eine rechtlich einwandfreie, technikorientierte, preiswerte und zukunftsweisende kommunale Datenverarbeitungs-Infrastruktur zu sorgen. Dezentrale Lösungen werden nicht nur dem kommunalen Selbstbestimmungsrecht (Art. 28 Abs. 2 GG, Art. 82 Abs. 2 SächsVerf) am ehesten gerecht, sie verhindern unüberschaubare Datensammlungen, Verknüpfungsmöglichkeiten und unkontrollierten Datenverkehr. Alle Forderungen des Volkszählungsurteils sind um so leichter zu erfüllen, je ortsnäher und individueller die Daten verarbeitet werden.

5.5.2 "Beraterverträge" der Gemeinden und Wasser-/Abwasserzweckverbände

In Sachsen haben zahlreiche Gemeinden, insbesondere aber die Wasser- bzw. Abwasserzweckverbände mit privaten Unternehmen "Beraterverträge" geschlossen, um die eigentlichen Gemeinde- bzw. Zweckverbandsaufgaben "außer Hauses" erledigen zu lassen. Danach übernehmen Beratungsunternehmen gegen eine pauschale Vergütung pro beitragspflichtiger Grundstückseinheit verschiedene Arbeiten, die zur Beitragserhebung nach §§ 17 ff. SächsKAG und den entsprechenden Trinkwasser- bzw. Abwassersatzungen als notwendig angesehen werden.

Nach mir bekannt gewordenen Vertragsangeboten bieten die Beratungsunternehmen folgende Leistungen an:
a) Komplette Beratung in allen Fragen des kommunalen Abgabenrechts,
b) Beratung und Mitwirkung beim Entwurf von Beitrags- und Gebührensatzungen,
c) Erfassung der abgabepflichtigen Grundstücke und Grundstückseigentümer sowie der Berechnungsgrundlagen (maßstabsrelevante Flächen, Frontlänge, Zahl des Klein- und Großviehs usw.).
d) Erstellung versandfertiger Abgabebescheide,
e) Führung von Erhebungslisten/-dateien mit Daten über die Abgabepflichtigen und die Abgabeschuld.

Je nach Vertragsgestaltung nimmt das Unternehmen Aufgaben der öffentlichen Verwaltung wahr (§ 2 Abs. 2 SächsDSG) oder wird gemäß § 7 SächsDSG als Auftragnehmer tätig.

Ich habe nicht zu prüfen, ob die genannten Tätigkeiten kommunal- und haushaltsrechtlichen Grundsätzen zuwiderlaufen (Grundsatz der wirtschaftlichen und sparsamen Haushaltführung; Verbot, im Hinblick auf §§ 1 Abs. 1, 3 Abs. 1 Nr. 6 SächsVwKG die Kostenpauschale auf die Beitragspflichtigen umzulegen). In den Verträgen fehlen aber regelmäßig datenschutzrechtliche Regelungen, die den §§ 7 und 9 SächsDSG genügen.

Vor allem mangelt es an *schriftlichen* Festlegungen (vgl. auch Nrn. 6 bis 11 meiner Bekanntmachung zur Datenverarbeitung im Auftrag und zur Rechtsstellung des beauftragten Unternehmens vom 3. November 1993 - SächsABl. S. 1304) zu folgendem:
- Art und Umfang der Datenverarbeitung oder -nutzung;
- vom Auftragnehmer einzuhaltende personelle, technische und organisatorische Maßnahmen zur Gewährleistung des Datenschutzes, einschließlich der Abgrenzung der Datenverarbeitung zu anderen Unternehmensbereichen (zu den *personellen* Maßnahmen siehe unten);
- die Verpflichtung der Mitarbeiter des Auftragnehmers zur Wahrung des Datengeheimnisses gemäß § 6 SächsDSG (gegebenenfalls Verpflichtung nach dem Verpflichtungsgesetz);
- Zeitpunkt, Ort und Berechtigung bzw. Verpflichtung zur Anlieferung bzw. Abholung der Datenträger (Daten, Programme, vorgenommene Auswertungen bzw. Arbeitsergebnisse);
- Art und Weise des Transports, der Versendung sowie der Aufbewahrung von Datenträgern;

- Art und Dauer der Aufbewahrung der Datenträger beim Auftragnehmer (auch für den Fall der Beendigung des Auftragsverhältnisses);
- Zeitpunkt und Art der Vernichtung manueller Datenträger und von Ausschuß- oder Testmaterial;
- Maßnahmen bei Verlust oder Beschädigung von Datenträgern;
- Zeitpunkt und Maßnahmen zur Löschung von Ein- bzw. Ausgabedaten beim Auftragnehmer;
- Kontrollrechte des Auftraggebers und des Sächsischen Datenschutzbeauftragten;
- beiderseits durchzuführende Kontrollen der Verfahren;
- Beginn der Datenverarbeitung erst nach Freigabe der Verfahren durch den Auftraggeber;
- Festlegung der Verfügungsberechtigungen über die Daten (z. B. alleinige Verfügungsberechtigung des Auftraggebers) in den Phasen der Datenverarbeitung;
- Zulässigkeit der Beauftragung von Subunternehmen und Verpflichtung des Auftragnehmers, die Verfügungsberechtigung und das Kontrollrecht des Auftraggebers und des Sächsischen Datenschutzbeauftragten auch gegenüber dem Subunternehmen vertraglich abzusichern;
- Vertragsstrafen und Bestimmungen über eine fristlose Kündigung, falls der Auftragnehmer Datenschutzvorschriften verletzt.

Personelle Maßnahmen:

Zu den nach § 7 SächsDSG zu treffenden *personellen* Maßnahmen zur Gewährleistung einer datenschutzgerechten Auftragsdatenverarbeitung gehört neben der Feststellung der *fachlichen* Kompetenz auch die *persönliche* Zuverlässigkeit und Eignung des Auftragnehmerpersonals. Der Auftraggeber sollte die Auftragsvergabe davon abhängig machen, daß der in § 21 Abs. 1 Nr. 6 Buchst. f StUG genannte Personenkreis bei der "Gauck"-Behörde überprüft und für unbelastet befunden wurde.

Es ist u. a. Angelegenheit der Kommunalaufsichtsbehörden, sich auch für eine datenschutzgerechte Vertragsgestaltung einzusetzen.

Dies gilt um so mehr, als das SMU am 27. Oktober 1994 in einer Pressemitteilung von gravierenden Mängeln bei den Zweckverbänden berichtet hat, die vermuten lassen, daß dort auch Datenschutzbelange "auf der Strecke bleiben".

5.5.3 Personalüberprüfung auf MfS-/AfNS-Vergangenheit und auf Systemnähe im Kommunalbereich

5.5.3.1 MfS-/AfNS-Vergangenheit

Nach Art. 33 Abs. 2 GG, 91 Abs. 2 SächsVerf haben alle Bürger nach ihrer *Eignung, Befähigung und fachlichen Leistung* gleichen Zugang zu jedem öffentlichen Amt. Personen, die i. S. v. Art. 119 SächsVerf, § 6 Abs. 2 und 3 SächsBG belastet sind, fehlt regelmäßig die *Eignung* für die Bekleidung eines öffentlichen Amtes. Diese Personen dürfen auch im Hinblick auf §§ 61 Abs. 1 SächsGemO, 57 Abs. 1 SächsLKrO von den Gemeinden und Landkreisen nicht eingestellt oder weiterbeschäftigt werden.

Zwar hat der sächsische Gesetzgeber eine "Regelüberprüfung" zur Eignungsfeststellung für den öffentlichen Dienst nicht *ausdrücklich* gesetzlich festgelegt, jedoch ergibt sich die Pflicht der datenverarbeitenden Stellen (wozu ausnahmslos die Gemeinden und Landkreise gehören) zur Überprüfung des im öffentlichen Dienst mit der Datenverarbeitung betrauten Personals (bzw. der Bewerber) bereits aus § 9 Abs. 1 SächsDSG. Hiernach haben die datenverarbeitenden Stellen nämlich u. a. alle erforderlichen *personellen Maßnahmen* zur Gewährleistung des Datenschutzes zu treffen. Hierzu zählen Maßnahmen, die sich einerseits aufgrund mangelnder fachlicher Kompetenz, andererseits aber auch wegen *persönlicher Unzuverlässigkeit* des Betroffenen ergeben können. Diese Auslegung folgt aus dem Grundsatz, daß Rechtsnormen so ausgelegt werden müssen, daß die Grundrechte (hier: das Recht auf informationelle Selbstbestimmung) möglichst *optimale Wirksamkeit* erlangen. "Persönliche Zuverlässigkeit" im Hinblick auf den Umgang mit personenbezogenen Daten liegt bei Stasi-belastetem Personal oder belasteten Bewerbern grundsätzlich nicht vor. Zumindest ist eine Einzelfallprüfung erforderlich. Als personelle Maßnahme zur Gewährleistung des Datenschutzes i. S. v. § 9 Abs. 1 SächsDSG kommt also für diesen Personenkreis zumindest die Anfrage bei der "Gauck"-Behörde in Betracht.

Da die Ausübung der Personalhoheit - einer der Grundpfeiler des kommunalen Selbstverwaltungsrechts! - *im Rahmen der Gesetze* zu erfolgen hat (Art. 20 Abs. 3, 28 Abs. 2 GG, 82 Abs. 2 SächsVerf) und die Einstellung bzw. Beschäftigung von ungeeignetem Personal einen *Verstoß gegen den Grundsatz der Gesetzmäßigkeit der Verwaltung* darstellt, sind die Rechtsaufsichtsbehörden nach §§ 111 ff. SächsGemO, § 65 SächsLkrO gehalten tätig zu werden (siehe insbesondere auch Art. 89 Abs. 1 SächsVerf, wonach der Freistaat die Gesetzmäßigkeit der Verwaltung der Gemeinden und Landkreise und der anderen Gemeindeverbände *zu überwachen hat*). Die Verpflichtung der Rechtsaufsichtsbehörden zum Tätigwerden läßt sich außerdem im Hinblick auf den Schutz des Grundrechts auf informationelle Selbstbestimmung des Einzelnen auch aus dem Volkszählungsurteil des Bundesverfassungsgerichts (BVerfGE 65, 1 ff.) ableiten. Hiernach ergibt sich unmittelbar aus Art. 2 Abs. 1 GG, Art. 33 SächsV die *Verpflichtung* des Gesetzgebers, organisatorische und *verfahrensrechtliche Maßnahmen* zu treffen, welche der *Gefahr* einer Verletzung dieses Grundrechts *entgegenwirken*. Dieses Gebot gilt entsprechend für die Tätigkeit der Verwaltung (hier also der Aufsichtsbehörden), weil Art. 1 Abs. 3 GG auch die Verwaltung an die Grundrechte als unmittelbar geltendes Recht bindet.

Überließe man allein den Gemeinden und Landkreisen die Entscheidung, ob sie die Bewerber oder Bediensteten auf eine mögliche Stasi-Vergangenheit überprüfen, würde dies zudem nach meiner Auffassung gegen das Grundrecht auf *gleichen Zugang* zu den öffentlichen Ämtern (vgl. Art. 33 Abs. 2 GG, 91 Abs. 2 SächsVerf) verstoßen. Unterbleibt eine Überprüfung, so führt dies erfahrungsgemäß zu uferlosen Verdächtigungen, Behauptungen oder übler Nachrede hinsichtlich einzelner Bediensteter. Dies liegt nicht im Interesse der Verwaltung, deren Ansehen dadurch nachhaltig geschädigt wird. Ferner führt dies zu Verletzungen des Persönlichkeitsrechts der Betroffenen, ohne daß der Dienstherr sich nachhaltig schützend vor sie stellen kann.

Auch die Nichtbeachtung einer Verpflichtung zur gesetzlich vorgesehenen Datenverarbeitung (also die Unterlassung der Personalüberprüfung) ist ein Verstoß gegen datenschutzrechtliche Vorschriften.

Im Interesse einer ordnungsgemäßen Datenverarbeitung und zum Schutz des Rechts auf informationelle Selbstbestimmung habe ich das SMI gebeten, gemäß § 25 Satz 1 SächsDSG, die Gemeinden und Landkreise im Wege der Rechtsaufsicht (insbesondere nach § 115 SächsGemO) unter Hinweis auf die notwendigen beamten- und arbeitsrechtlichen Konsequenzen zu veranlassen, sämtliches Personal, das Umgang mit personenbezogenen Daten hat, im Sinne von Art. 119 SächsVerf, § 6 Abs. 2 und 3 SächsBG zu überprüfen. Dieser Bitte ist das SMI kürzlich nachgekommen.

Sollte ich bei meinen Kontrollen feststellen, daß Gemeinden und Landkreise ihrer Verpflichtung, nur "geeignetes" (also überprüftes) Personal in der Datenverarbeitung zu beschäftigen, nicht nachgekommen sind, werde ich dies gemäß § 26 SächsDSG beanstanden.

5.5.3.2 Systemnähe

Die Verwaltungsvorschrift der Sächsischen Staatsregierung zur Prüfung der persönlichen Eignung im Beamtenverhältnis vom 14. Dezember 1994 (SächsABl. 1995, S. 40) bringt - allerdings sehr spät - Klarheit, wie bei der Frage der *Verbeamtung* von Systemnahen zu verfahren ist. Für *Arbeitnehmer* (Angestellte, Arbeiter) im öffentlichen Dienst fehlen vergleichbare Regelungen.

So mußte ich feststellen, daß in Gemeinden und Landratsämtern teilweise Spitzenpositionen mit Angestellten besetzt wurden, die wegen ihrer Systemnähe niemals als Beamte hätten eingestellt werden dürfen. Ich habe die Eignung dieses Personenkreises im Hinblick auf §§ 9 SächsDSG, 57 Abs. 1 SächsLkrO, 61 Abs. 1 SächsGemO, wonach "geeignetes" Personal einzustellen ist und nur "geeignetes" Personal personenbezogene Daten verarbeiten darf, nachdrücklich in Frage gestellt. Folgende Überlegungen lagen zugrunde: Art. 33 Abs. 4 GG, § 2 Abs. 2 und 3 Beamtenrechtsrahmengesetz und § 5 Abs. 3 SächsBG gebieten es, daß hoheitsrechtliche Befugnisse *in der Regel* Beamten zu übertragen sind. Daraus folgt, daß nur *ausnahmsweise* hoheitsrechtliche Aufgaben auf Angestellte übertragen werden dürfen, wenn z. B. intensive Bemühungen des Dienstherrn, geeignete Beamte einzustellen, erfolglos blieben. Ob diese Gesichtspunkte beim Aufbau der sächsischen Verwaltung und bei der Besetzung hoheitsrechtlich geprägter

Dienstposten in ausreichendem Maße beachtet wurden, bezweifle ich. Jedenfalls vertrete ich die Auffassung, daß leitende Angestellte mit hoheitsrechtlichem Aufgabenbereich, was ihre fachliche und persönliche Eignung betrifft, materiell Beamten gleichzustellen und daher auch auf Systemnähe zu überprüfen sind. Es ginge an der Sache vorbei, wenn durch eine "Flucht" in privatrechtliche Arbeitsverträge hoheitsrechtliche Aufgaben auf belastete und damit unzuverlässige, also für den öffentlichen Dienst sowie für den Umgang mit personenbezogenen Daten nicht geeignete Angestellte übertragen würden. Leider mußte ich den Eindruck gewinnen, daß in Sachsen die Ernennung zum Beamten als persönliche Anerkennung ausgestaltet ist und nicht am übertragenen Aufgabenkreis orientiert wird.

Ich halte deshalb eine konsequentere Überprüfung dieses Personenkreises nicht nur auf MfS-/ AfNS-Vergangenheit, sondern auch auf Systemnähe für geboten.

Gespräche mit der Staatsregierung und dem Sächsischen Landesbeauftragten für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR werden weitergeführt. Bei der Staatsregierung erwarte ich mehr Problembewußtsein in diesen Fragen. § 9 SächsDSG läßt es nicht zu, belastete, erpreßbare oder sonst unzuverlässige Personen in der Bearbeitung personenbezogener Daten einzusetzen.

5.5.4 Überprüfung einer städtischen Urkundenstelle

Die Mitteilung, daß der Datenschutz in einer städtischen Urkundenstelle nicht gewährleistet sei, veranlaßte mich zu einer Überprüfung. Folgende Mängel mußte ich beanstanden:

Die Räume der Urkundenstelle waren im Erdgeschoß des Rathauses untergebracht und unzureichend vor unbefugtem Zutritt gesichert. Die Fenster waren ungesichert und auch die Schlösser in den beiden Zugangstüren boten keinen ausreichenden Schutz. Beide Schließzylinder standen 1 bzw. 1 1/2 cm vor und ermöglichten so ein Abdrehen. Ein Schließblech war darüber hinaus von außen abschraubbar. Es gab weder eine Alarmanlage noch Bewegungsmelder in den Räumen der Urkundenstelle.
Sämtliche Personenstandsbücher (seit 1876) waren in offenen Holzregalen untergebracht. Personenbezogene Karteien befanden sich in unverschließbaren Holzkarteikästen.

Die vorgefundene Situation stand im Widerspruch zu § 9 SächsDSG. Ich habe die Stadt aufgefordert, alle technischen und organisatorischen Maßnahmen zu treffen, um insbesondere den unbefugten Zugang zu den Personenstandsbüchern und sonstigen personenbezogenen Unterlagen und deren Verlust durch Feuer, Diebstahl etc. zu verhindern. Weiter war zu fordern, die innere Organisation der Urkundenstelle so zu gestalten, daß sie den besonderen Anforderungen des Datenschutzes gerecht wird. Ausschlaggebend hierfür sind nicht zuletzt § 31 der Dienstanweisung für die Standesbeamten und ihre Aufsichtsbehörden (DA) sowie Nr. 13.1 der Zweiten Verwaltungsvorschrift des Sächsischen Staatsministeriums des Innern zur Ausführung des Personenstandsgesetzes (2. PStGVwV) vom 5. Oktober 1992 (SächsABl. S. 1575), wonach insbesondere wegen der Einmaligkeit der Personenstandsbücher (dauernde

Aufbewahrung ist vorgeschrieben) *eine feuer- und einbruchssichere Unterbringung erforderlich ist.*

Aus datenschutz- und personenstandsrechtlichen Gründen habe ich verlangt, daß die erforderlichen technisch-organisatorischen Maßnahmen *unverzüglich* getroffen werden (z. B. einbruchssichere Türen und Fenster, Alarmanlage, Bewegungs- und Brandmelder bzw. feuer- und einbruchssichere Stahlschränke).

Die Stadt hat zunächst die schlimmsten Mängel behoben und wird meine Vorschläge bei einem bevorstehenden Umzug der Urkundenstelle in neue Räume beachten.

5.5.5 Unter welchen Voraussetzungen sind Gemeinderats- und Kreistagssitzungen öffentlich oder nichtöffentlich abzuhalten?

Zu dieser von einem Gemeindebediensteten gestellten Frage habe ich folgendes mitgeteilt:

Gemäß §§ 33 Abs. 1 SächsLKrO, 37 Abs. 1 SächsGemO sind die Sitzungen des Kreistages bzw. des Gemeinderates grundsätzlich *öffentlich* abzuhalten, es sei denn, das öffentliche Wohl oder *berechtigte Interessen einzelner* erfordern eine nichtöffentliche Behandlung. Berechtigte Interessen einzelner sind insbesondere berührt, wenn es zur Behandlung eines Tagesordnungspunktes *unabdingbar ist,* daß (sensible) personenbezogene Daten offenbart werden müssen. In diesem Fall *muß* also die Öffentlichkeit ausgeschlossen werden.
Die Frage, ob öffentlich oder nichtöffentlich verhandelt wird, muß auch deswegen besonders gründlich geprüft werden, weil die Redebeiträge in öffentlichen Sitzungen nicht nur den Anwesenden (Mitgliedern und Zuhörern) zugänglich sind, sondern sämtlichen Einwohnern aufgrund des Rechts auf Einsicht in die Niederschriften gemäß §§ 36 Abs. 2 Satz 5 SächsLKrO, 40 Abs. 2 Satz 5 SächsGemO in ihrem wesentlichen Inhalt zur Kenntnis gelangen können.

5.5.6 Sind Tonbandaufnahmen in öffentlichen Gemeinderats- oder Kreistagssitzungen zulässig?

Auf diese Frage habe ich mitgeteilt, daß das Aufzeichnen von Redebeiträgen in solchen Sitzungen zwar nicht nach § 201 Abs. 1 Nr. 1 StGB (Aufzeichnen des *nicht*öffentlich gesprochenen Wortes) strafbar ist, aber auch "öffentlich gesprochene Worte" durch das verfassungsrechtlich gewährleistete Persönlichkeitsrecht geschützt sind. Tonbandaufzeichnungen von Redebeiträgen (z. B. zu Protokollzwecken) sind daher nur mit Kenntnis und Einwilligung der Betroffenen zulässig.

5.5.7 Behandlung von Bauangelegenheiten durch den Gemeinderat bzw. den Bauausschuß bei Widerspruch gegen die Veröffentlichung der Bauherrndaten durch den Bauherrn bzw. Entwurfsverfasser

Die im Sächsischen Amtsblatt verbindlich vorgeschriebenen Bauantragsformulare sehen die Möglichkeit vor, daß der Bauherr bzw. Entwurfsverfasser der Veröffentlichung der Bauantragsdaten und der Weitergabe dieser Daten an Baustelleninformationsdienste widersprechen kann.

Demgegenüber schreibt § 36 Abs. 4 in Verbindung mit § 41 Abs. 5 SächsGemO vor, daß bei bevorstehenden *öffentlichen* Gemeinderats- bzw. Ausschußsitzungen die Tagesordnung grundsätzlich *ortsüblich bekanntzugeben* ist, was unter anderem durch *Veröffentlichung* im gemeindlichen Mitteilungsblatt geschehen kann. Da die Tagesordnung in Bauangelegenheiten aus Gründen der Bestimmtheit zwangsläufig personenbezogene Daten des Bauherrn enthalten muß, könnte dies dazu führen, daß ein vom Bauherrn bzw. Entwurfsverfasser eingelegter Widerspruch gegen die Veröffentlichung der Bauantragsdaten praktisch bedeutungslos würde.

Diese Problematik ist nach meiner Auffassung wie folgt zu lösen:

Die §§ 36 Abs. 4, 41 Abs. 5 SächsGemO sind unter Beachtung des *Grundsatzes der Verhältnismäßigkeit* so auszulegen, daß bei der Veröffentlichung der Tagesordnung nur diejenigen Daten bekannt gegeben werden dürfen, die zur Bezeichnung des Bauvorhabens - und damit im Interesse der Transparenz des gemeindlichen Handelns - *erforderlich* sind. Grundsätzlich genügt hierzu die Angabe des Bauortes (Straße und Hausnummer, in seltenen Fällen Flurnummer), die Art des Bauvorhabens (z. B. Garagenneubau, Zweifamilienhaus) und der Name des Bauherrn. Die *Anschrift* des Bauherrn ist hingegen bei Behandlung von Bauanträgen nicht von Bedeutung *und darf daher nicht bekannt gegeben werden*.
Diese Auslegung steht nicht im Widerspruch zu dem Sinn des auf den Bauanträgen eingeräumten Widerspruchsrechts gegen die Veröffentlichung oder Weitergabe der Bauherrendaten. Durch den Widerspruch will der Bauherr nämlich in erster Linie verhindern, daß er unerbetene Werbesendungen oder Vertreterbesuche erhält (= Beeinträchtigung schutzwürdiger Belange). Gezielte Werbung durch Firmen oder unerwünschte Vertreterbesuche setzen jedoch die Kenntnis der Anschrift des Bauherrn voraus, die - wie dargelegt - nicht bekanntgegeben werden darf.

Entsprechendes muß auch für die Mitteilung des Verhandlungsgegenstandes bei der Einberufung des Gemeinderats (oder des Ausschusses) durch den Bürgermeister (vgl. § 36 Abs. 3 SächsGemO) und für die Erörterung der Bauanträge in öffentlichen Sitzungen gelten (vgl. § 37 SächsGemO). Auch hier ist streng darauf zu achten, daß nur die *erforderlichen* personenbezogenen Daten offenbart werden. Ansonsten ist in *nichtöffentlicher* Sitzung zu verhandeln.

Der SSG und der SLT haben meine Bewertung in ihren Mitgliederrundschreiben veröffentlicht.

5.6 Baurecht / Wohnungswesen

5.6.1 Dürfen Wohnungsämter bei Anträgen auf Erteilung von Wohnungsberechtigungsscheinen Angaben zum Einkommen der Antragsteller verlangen?

Mehrere Bürger beschwerten sich darüber, daß Wohnungsämter bei Anträgen auf Erteilung von Wohnungsberechtigungsscheinen auch Angaben zum Einkommen verlangen.

Ich habe den Petenten mitgeteilt, daß nach § 25 des 2. WoBauG das Einkommen von Wohnungssuchenden, die sich für eine mit öffentlichen Mitteln geförderte Wohnung bewerben, eine bestimmte Grenze nicht überschreiten darf. Es ist daher grundsätzlich zulässig, wenn Wohnungsämter Fragen zu den gesetzlich festgelegten Einkommensgrenzen stellen ("Überschreitet Ihr Gesamteinkommen den Betrag von ...?"). Nicht zulässig, weil nicht *erforderlich*, wäre hingegen die Aufforderung zur Vorlage einer vom Arbeitgeber ausgestellten Verdienstbescheinigung über das genaue Jahreseinkommen des jeweiligen Antragstellers.

Anders ist die Rechstlage allerdings, wenn ein Antrag auf Erteilung eines Wohnungsberechtigungsscheins für eine im Beitrittsgebiet gelegene Wohnung gestellt wird, die bereits seit dem 1. September 1990 Kommunaleigentum ist. Für diese Wohnungen gilt nämlich (voraussichtlich bis zum 31. Dezember 1995) das DDR-Gesetz über die Gewährleistung von Belegungsrechten im kommunalen und genossenschaftlichen Wohnungswesen. Wohnungsberechtigungsscheine werden hiernach unabhängig vom Einkommen des Wohnungssuchenden erteilt.

5.6.2 Datenschutz bei der Wohnungsbauförderung

In meinem 1. Tätigkeitsbericht (5.6.3) habe ich die datenschutzrechtlichen Probleme bei der Beantragung von Fördermitteln nach den Wohnungsbauförderbestimmungen dargestellt. Erfreulicherweise konnte ich das SMI nach einem weiteren intensiven Schriftwechsel von meiner Auffassung überzeugen, wonach die Förderanträge (die auch sensible personenbezogene Daten, wie z. B. das Einkommen, enthalten) unmittelbar bei der Wohnungsbauförderungsstelle und nicht mehr bei dem für den Bauort zuständigen Bürgermeisteramt eingereicht werden sollten. Diese datenschutzgerechte Regelung wurde in die Wohnungsbauförderbestimmungen 1994 aufgenommen. Die Antragsberechtigten

brauchen nicht mehr zu befürchten, daß der Bürgermeister und das Gemeindepersonal Kenntnis von ihren Einkommensverhältnissen u. ä. erhalten.

5.7 Statistikwesen

5.7.1 Gebäude- und Wohnungszählung 1995

Im Jahre 1995 findet in den neuen Bundesländern sowie im ehemaligen Ost-Berlin gemäß § 1 Nr. 1 WoStatG die erste statistische 'Großerhebung' seit der Wiedervereinigung statt: Eine Zählung ausschließlich der Gebäude mit Wohnungen, ohne Volkszählung, die sich ausschließlich an die Eigentümer und Verwalter bzw. Erbbauberechtigten (vgl. § 9 Abs. 2 Nr. 1 i. V. m. § 4 Abs. 1 WoStatG) richtet und in der nach den Mietverhältnissen und der Belegung der Wohnung (anders als in der bereits durchgeführten Gebäude- und Wohnungsstichprobe von 1993 aufgrund § 1 Nr. 2 WoStatG) nicht gefragt wird.

Zweck der Erhebung ist es, der Gesetzgebung und politischen Planung einen genaueren - wohlgemerkt: statistischen - Überblick über den Zustand der Gebäude mit Wohnraum im Beitrittsgebiet zu verschaffen, für den es bisher an genügend vollständigen und neuen diesbezüglichen Daten fehlt.

Solche flächendeckenden Großzählungen haben es bekanntlich datenschutzrechtlich 'in sich'; als Neuheit kommt für die Statistischen Landesämter im Beitrittsgebiet hinzu, daß sie zum ersten Mal mit örtlichen Erhebungsstellen zu arbeiten haben. Das hat das SMI aber nicht davon abgehalten, mir die von ihm ausgearbeitete diesbezügliche besondere Regelung für Sachsen erst zwei Arbeitstage vor ihrer Einbringung ins Kabinett zur Verfügung zu stellen - ein klarer Verstoß wenn nicht gegen § 6 Abs. 8 SächsStatG, so doch jedenfalls gegen § 13 Abs. 5 Satz 4 GeschoSReg. Nicht der mir "zur Kenntnisnahme" (!) übersandte Entwurf einer *Verordnung der Sächsischen Staatsregierung zur Durchführung der Gebäude- und Wohnungszählung 1995 (GWZVO),* sondern eine überarbeitete Fassung wurde dann vom Kabinett verabschiedet; *nach* Veröffentlichung der Verordnung im Gesetz- und Verordnungsblatt (1994 S. 1589) erhielt ich auf Wunsch die amtliche Begründung dieser Fassung übermittelt.

Ich habe gegen die Verordnung mit Nachdruck rechtliche Bedenken geltend gemacht, denen sich jedoch das SMI, nachdem sich erst auf Vermittlung der Staatskanzlei ein Einverständnis abzuzeichnen schien, verschlossen hat.

Im einzelnen handelt es sich vor allem um folgendes:

Die GWZVO überträgt in § 1 die *örtliche* Durchführung der Erhebung auf die Gemeinden. Diese sollen "örtliche Erhebungsstellen" einrichten. Damit hält sich die Verordnung zwar im Rahmen der Verordnungs-Ermächtigung durch den Bundesgesetzgeber in § 6 WoStatG. Sie verstößt jedoch meiner Meinung nach gegen das Sächsische Statistikgesetz, dessen Anwendbarkeit sich aus dessen § 2 Abs. 1 Nr. 2 ergibt.

Das Sächsische Statistikgesetz sieht in § 4 Abs. 1 Satz 2 neben dem Statistischen Landesamt als der "zentralen Erhebungsstelle" für die Durchführung einzelner Aufgaben die Möglichkeit der Einrichtung und Einschaltung "weiterer Erhebungsstellen" vor. In § 4

Abs. 2 Satz 1 erlaubt das Gesetz darüber hinaus, daß dann, wenn kommunale Statistikstellen nach den besonderen Regeln des § 9 SächsStatG eingerichtet sind, diese die Aufgaben der (weiteren) Erhebungsstellen wahrnehmen dürfen.

§ 1 Abs. 1 GWZVO überträgt jedoch die örtliche Durchführung "örtlichen Erhebungsstellen" in kommunaler Trägerschaft, die *nicht* die Eigenschaft haben (müssen), kommunale Statistikstellen im Sinne von § 4 Abs. 2 Satz 1, § 9 SächsStatG zu sein (bzw. alle im Gesetz an diese gestellten Anforderungen zu erfüllen).

Ich halte es für höchst fraglich, daß § 4 Abs. 1 Satz 2 i. V. m. Abs. 2 Satz 1 SächsStatG dies zuläßt. Denn die Vorschrift ist aller Wahrscheinlichkeit nach dahin zu verstehen, daß die in § 4 Abs. 1 Satz 2 genannten "weiteren Erhebungsstellen" ausschließlich solche des Freistaates sind und daß weitere Erhebungsstellen in kommunaler Trägerschaft nur in § 4 Abs. 2 Satz 1 unter den besonderen dort genannten Voraussetzungen zugelassen sind.

Gibt die Entstehungsgeschichte, was im einzelnen an dieser Stelle zu weit führte, für diese Frage im Ergebnis nichts her, so spricht für die von mir für richtig gehaltene Auslegung zunächst ganz eindeutig die Stellung der Vorschriften § 4 Abs. 1 Satz 2 und Abs. 2 Satz 1 im Gesetz. Denn § 4 Abs. 1 Satz 3 und 4 sind allem Anschein nach auf solche weiteren Erhebungsstellen zugeschnitten, die an - von Hause aus gerade nicht mit Aufgaben von Statistiken betraute - öffentliche Stellen der Verwaltung *des Freistaates* angelehnt sind, hinsichtlich deren jedoch die Abschottung (Satz 3) sowie die Fachaufsicht durch das Statistische Landesamt (Satz 4) vorgeschrieben wird. Dafür wiederum spricht ebenfalls die Stellung im Gesetz: In § 3 und § 4 Abs. 1 Satz 1 SächsStatG ist ausschließlich vom Statistischen Landesamt, also von der Statistikverwaltung des *Freistaates*, die Rede. Das setzt sich in §§ 5, 6 (ausschließlich dessen letzten Absatzes; auch § 7 betrifft dann jedoch wieder ausschließlich öffentliche Stellen des *Landes*) fort.

Nimmt man nur den Wortlaut des § 4 Abs. 2 Satz 1 SächsStatG für sich, sind beide Auslegungen möglich. Diejenige - *weite* - Auslegung, der zufolge in § 4 Abs. 1 auch *weitere Erhebungsstellen* in kommunaler Trägerschaft vorgesehen sind, versteht Abs. 2 Satz 1 so: Gemeinden, die kommunale Statistikstellen haben, erhalten durch § 4 Abs. 2 Satz 1 das Recht, *diese* die ihnen (den Gemeinden) vom Staate übertragenen Statistik-Aufgaben wahrnehmen zu lassen, statt dafür zusätzlich eine gesonderte Erhebungsstelle (ad hoc) zu bilden. (Ansonsten verbliebe als Regelungszweck des § 4 Abs. 2 nur die Besonderheit des Satzes 2 der Vorschrift, der gegen Ende des Gesetzgebungsverfahrens, im Innenausschuß des Landtages, eingefügt worden ist.)

Versteht man stattdessen das Gesetz - *eng* - dahingehend, daß die Einschaltung von Erhebungsstellen in kommunaler Trägerschaft ausschließlich im zweiten Absatz der Vorschrift, genauer noch in dessen Satz 1, geregelt ist, dann ist es zwingend, daß die Vorschrift gerade die Voraussetzungen nennt, unter denen ausnahmsweise kommunale Stellen die Aufgaben von Erhebungsstellen wahrnehmen *dürfen* (so ist das "können" zu lesen). Dies wäre eine sehr *sinnvolle, grundrechtsfreundliche* Regelung:
Es liegt auf der Hand, daß die Datenerhebung durch eine Stelle, die einer *ortsnahen* und Stellen sehr vieler Zuständigkeiten unterhaltenden Organisation (Gemeinde) zugehört, das Grundrecht auf informationelle Selbstbestimmung in besonderer Weise gefährdet; die in § 4 Abs. 2 Satz 1 erteilte Erlaubnis wird daher nur unter besonders strengen, dem

Datenschutz dienenden Voraussetzungen erteilt - eben denjenigen des § 9 SächsStatG. Von diesen Voraussetzungen gilt nämlich nur ein *Teil* - § 9 Abs. 4 - kraft des (inhaltlich mit ihm übereinstimmenden) § 4 Abs. 3 SächsStatG auch für *alle* Erhebungsstellen, *nicht aber Abs. 1 Satz 2, 2 Satz 1, 3 und auch nicht 5*.

§ 4 Abs. 3 gilt dabei wegen der Stellung der Vorschrift eindeutig wie für die Erhebungsstellen nach Abs. 1 auch für die nach Abs. 2. Letzteres ist freilich überflüssig, wegen der schon genannten Übereinstimmung von § 4 Abs. 3 mit § 9 Abs. 4. Diese Gesetzes-Redundanz ist jedoch als Argument *gegen* die enge Auslegung von § 4 Abs. 1 und 2 *ungeeignet*. Denn sie ist, wie sich im einzelnen zeigen ließe, durch die Entstehungsgeschichte gut zu erklären: Gerade weil in § 4 ursprünglich an kommunale Erhebungsstellen nicht gedacht worden ist, ist die Möglichkeit gar nicht in den Blick gekommen, § 9 Abs. 4 durch eine Verweisung auf § 4 Abs. 3 (§ 4 Abs. 2 in den früheren Fassungen) zu ersetzen oder auch umgekehrt § 4 Abs. 1 um eine Verweisung auf § 9 Abs. 4 zu ergänzen.

Unter Gesichtspunkten des *Zweckes* des Schutzes des Grundrechts auf informationelle Selbstbestimmung ist die *enge* Auslegung des § 4 Abs. 1, wonach Erhebungsstellen in kommunaler Trägerschaft nur unter den Voraussetzungen des § 4 Abs. 2 SächsStatG in Frage kommen, *vorzuziehen* (und möglicherweise die verfassungskonforme Auslegung!). § 4 Abs. 2 hat nur eine sehr schwache Funktion, wenn man der gegenteiligen, weiten Auslegung des § 4 Abs. 1 folgt. Überdies erscheint es auch fraglich, ob die Fachaufsicht des Statistischen Landesamtes (§ 4 Abs. 1 Satz 4 SächsStatG) einen ausreichenden Ersatz für die oben genannten fehlenden verfahrensmäßigen Sicherungen bieten kann, welche § 9 SächsStatG vorsieht, die jedoch außerhalb dieser Vorschrift (und damit des Anwendungsbereiches des § 4 Abs. 2) nicht gelten.

Zwischenergebnis: Die überwiegenden Gründe sprechen dafür, daß im Bereich der Bindungswirkung des Sächsischen Statistikgesetzes, also für den sächsischen Verordnungsgeber, Kommunen als Träger von Erhebungsstellen nur nach den Vorschriften des § 4 Abs. 2 SächsStatG in Betracht kommen. Also nur dann, wenn sie eine *kommunale Statistikstelle* im Sinne des § 9 SächsStatG eingerichtet haben.

Daran ändert sich nichts dadurch, daß in § 6 Abs. 3 Satz 2 WoStatG der Bundesgesetzgeber den Landesgesetzgeber ermächtigt, die Aufgaben der Erhebungsstellen auf die Gemeinden und Gemeindeverbände zu übertragen. Dies ist als *Ermächtigung im Hinblick auf die gemeindliche Selbstverwaltung* zu verstehen - als Ermächtigung, die im Hinblick auf Art. 85 Abs. 1 Satz 1 SächsVerf, § 2 Abs. 2 Satz 1 SächsGemO nach der Rechtsprechung des Bundesverfassungsgerichts zu Art. 28 Abs. 2 GG *rechtlich nötig* ist (vgl. BVerfGE 26, 228, 237, bestätigt 56, 298, 309, sowie Quecke-Schmid, Gemeindeordnung für den Freistaat Sachsen, 1993, Rdnr. 47 zu § 2 und ferner ausführlich Stober, Kommunalrecht, 2. Auflage 1992, § 3 IV 1 a mit weiteren Nachweisen aus der Verfassungsgerichtsrechtsprechung).
§ 4 SächsStatG regelt hingegen, wie dargelegt, *unter dem Gesichtspunkt der Wahrung des Grundrechts auf informationelle Selbstbestimmung*, unter welchen Voraussetzungen in Sachsen kommunale Stellen mit der Erhebung personenbezogener Daten zu Zwecken der Statistik betraut werden dürfen.

Sofern die hier vertretene *enge* Auslegung des § 4 Abs. 1, 2 SächsStatG richtig ist, hat das folgende *Wirkungen* im Hinblick auf die GWZVO:

§ 1 Abs. 1 Satz 2 GWZVO besagt (stillschweigend), daß die örtliche Erhebungsstelle keine kommunale Statistikstelle im Sinne der §§ 9, 4 Abs. 2 SächsStatG sein muß. Die Vorschrift verstößt daher gegen den höherrangigen § 4 SächsStatG, insofern sie zu geringe Anforderungen an die organisatorischen Vorkehrungen zum Schutz des Grundrechts auf informationelle Selbstbestimmung stellt, indem sie die mit der Durchführung der Zählung betrauten Erhebungsstellen in kommunaler Trägerschaft der Geltung der §§ 4 Abs. 2, 9 SächsStatG entzieht. Deswegen müßten meiner Meinung nach in der Vorschrift zumindest die Worte "örtliche Erhebungsstellen" *nichtig* sein. (Möglicherweise ist aus anderen Gründen auch der Rest des Satzes 2 nichtig.) Maßgeblich wäre insoweit statt dessen die Regelung in § 4 Abs. 2 Satz 1 i. V. m. § 9 SächsStatG.

§ 1 Abs. 1 Satz 5 (i. V. m. Satz 3) GWZVO dürfte *nichtig* sein: § 9 SächsStatG ist meiner Meinung nach zu entnehmen, daß es in einer Gemeinde immer nur genau eine kommunale Statistikstelle geben darf.

§ 3 Abs. 2 Satz 1 und Satz 2 GWZVO sind *partielle Wiederholungen* der ohnehin geltenden gesetzlichen Regelung: Satz 1 ist neben § 4 Abs. 1 Satz 3 (und § 9 Abs. 1 Satz 2) SächsStatG überflüssig; Satz 2 schreibt dasselbe vor, was § 9 Abs. 1 Satz 2, a. E., SächsStatG für kommunale Statistikstellen zur Pflicht macht (§ 4 Abs. 1 Satz 3 SächsStatG bzw. der gleichlautende § 6 Abs. 1 Satz 2 WoStatG tun dies nicht in dieser Deutlichkeit). Auf diese Weise erweckt die Vorschrift, aber letzlich § 3 GWZVO insgesamt, den irreführenden Eindruck einer abschließenden, das Wohnungsstatistikgesetz ergänzenden Regelung, die für eine Anwendung des § 4 (Abs. 1 Satz 3; allerdings nach dem gegenwärtigen Stand der Bundesgesetzgebung durch § 6 Abs. 1 Satz 2 sowie Abs. 2 WoStatG gleichwertig ersetzt) oder gar des § 9 SächsStatG keinen Raum läßt. In der Vorschrift fehlt der Hinweis, daß § 9 Abs. 1 Satz 2 sowie Abs. 2-5 SächsStatG unberührt bleiben. Da die Verordnung in ihrem § 3 (zumindest Abs. 2) so auszulegen ist, daß sich *nicht* aus § 9 SächsStatG zusätzliche Anforderungen an Organisation und Verfahren der örtlichen Erhebungsstellen ergeben, verstößt sie insoweit nach der hier vertretenen Auffassung durch inhaltlichen Widerspruch gegen höherrangiges Recht.

Die Rechtsfolge dieses Verstoßes gegen höherrangiges Recht mag sich am Ende als Nichtigkeit oder als sogenannte *Überlagerung ohne Teilnichtigkeit* darstellen - im praktischen Ergebnis besteht letztlich kein Unterschied: Es gelten für den in § 3 GWZVO, vor allem in Abs. 2 der Vorschrift, geregelten Bereich der organisatorischen Vorkehrungen zum Schutz des Grundrechts auf informationelle Selbstbestimmung für die Durchführung der Gebäude- und Wohnungszählung 1995 auf jeden Fall (gegebenenfalls: auch) § 6 Abs. 2, Abs. 1 Satz 2 WoStatG und § 9 SächsStatG! *Diese Vorschriften müssen beachtet werden, und darauf in geeigneter Weise hinzuweisen ist die Pflicht des SMI.*

Auch für den Fall, daß die hier vertretene Auffassung, daß § 4 Abs. 1 Satz 2, Abs. 2 Satz 1 SächsStatG *weitere Erhebungsstellen* in kommunaler Trägerschaft nur in Gestalt kommunaler Statistikstellen gemäß § 9 SächsStatG zuläßt, nicht richtig sein sollte, weist die GWZVO folgende datenschutzrechtlichen Fehler auf:

Einen ähnlichen Fehler wie § 3 Abs. 2 Satz 1 und 2 GWZVO weist *§ 5 Satz 2* der Verordnung auf: Die Vorschrift wiederholt - eigentlich unnötigerweise - die unzweifelhaft geltenden Regelungen in § 6 Abs. 2 Satz 2 WoStatG bzw., entsprechend, in § 4 Abs. 3 Satz 2 oder § 9 Abs. 4 Satz 2 SächsStatG, sie tut dies jedoch *unvollständig*, dabei jedoch den Eindruck einer abschließenden, vollständigen Regelung machend: Nicht nur, daß die in den genannten gesetzlichen Regelungen ausgesprochene Ausdehnung der Geheimhaltung auch auf solche Erkenntnisse über Auskunftswillige, die lediglich *gelegentlich* der Tätigkeit eines Bediensteten der örtlichen Erhebungsstelle gewonnen werden, sowie auf die Zeit *nach* Beendigung der Tätigkeit in der Erhebungsstelle fehlt; vor allem wird der Eindruck erweckt, die Verpflichtung auf die Wahrung des Statistikgeheimnisses und zur Geheimhaltung brauche - entgegen den genannten Vorschriften - *nicht* schriftlich zu geschehen.
Rechtsfolge ist dementsprechend: An die Stelle der rechtswidrigen Regelung in § 5 Satz 2 GWZVO tritt im Wege der sogenannten Überlagerung oder sogar wegen Nichtigkeit diejenige im Wohnungsstatistikgesetz sowie im Sächsischen Statistikgesetz.

Sofern § 1 Abs. 1 Satz 2 GWZVO den Sinn haben sollte, daß die in ihm vorgesehenen örtlichen Erhebungsstellen gegebenenfalls neben etwa schon bestehende kommunale Statistikstellen (im Sinne des § 9 SächsStatG) zu treten hätten, fehlt es an einer Rechtsgrundlage für einen dahingehenden Eingriff in die Organisationshoheit der Gemeinde; eine solche Rechtsgrundlage ergibt sich insbesondere nicht aus dem Wohnungsstatistikgesetz. Das bedeutet, daß es den Gemeinden unbenommen ist, von der durch § 4 Abs. 2 Satz 1 SächsStatG unzweifelhaft eingeräumten Befugnis Gebrauch zu machen, die Aufgabe der weiteren bzw.örtlichen Erhebungsstellen durch die von ihr eingerichtete kommunale Statistikstelle wahrnehmen zu lassen. Der Bekanntmachung des SMI zu den örtlichen Erhebungsstellen und ihren Erhebungsbezirken gemäß § 1 Abs. 1 der GWZVO (vom 24. Januar 1995, SächsABl. S. 214) kommt insofern keinerlei rechtliche Verbindlichkeit zu.

Schließlich fehlte in diesem Falle in § 3 Abs. 2 GWZVO der klarstellende Hinweis, daß § 6 Abs. 2 sowie Abs. 1 Satz 2 WoStatG und - wichtiger - § 4 Abs. 1 Satz 3, Abs. 3 SächsStatG unberührt bleiben.

Sogar noch bestärkt sehe ich mich in den von mir geltend gemachten Einwänden (gegen die Verordnung der Staatsregierung) durch die Art der Argumente, mit denen SMI und SMJus (Normprüfungsausschuß) sie mir gegenüber zu entkräften versucht haben. Hoffentlich nimmt das datenschutzrechtliche Problembewußtsein bei der Statistikverwaltung des Freistaates im Hinblick auf die Durchführung der Gebäude- und Wohnungszählung 1995 zu.

Was die *praktischen Folgen* der von mir für die richtige gehaltenen *engen* Auslegung von § 4 Abs. 1 Satz 2, § 2 Abs. 2 Satz 1 SächsStatG betrifft, so handelt es sich um folgende *Forderungen*:

- Die personelle Trennung der örtlichen Erhebungsstelle von der übrigen Gemeindeverwaltung (Verwaltungsvollzug) muß den Anforderungen des § 9 Abs. 2 Satz 2 SächsStatG entsprechen, die Erhebungsstelle muß also mit eigenem Personal

ausgestattet sein, das während der Tätigkeit in der Stelle nicht mit Aufgaben des Verwaltungsvollzuges betraut ist; außerdem muß die Stelle gegen den Zutritt unbefugter Personen hinreichend geschützt sein.
Das ist in § 4 Abs. 1 Satz 2 SächsStatG nicht in dieser Deutlichkeit gefordert.

- Gemäß § 9 Abs. 2 Satz 1 SächsStatG ist bei der Verarbeitung von Einzelangaben in Datenverarbeitungsanlagen die Abschottung dieser Daten gegenüber anderen Verwaltungsdaten und ihre Zweckbindung durch zusätzliche organisatorische, personelle und technische Maßnahmen der Datensicherung (Datensicherheit, technischer Datenschutz) zu gewährleisten.
- Die Maßnahmen, die nach dem Vorstehenden erforderlich sind, sind vom Bürgermeister in einer schriftlichen Dienstanweisung genau festzulegen (§ 9 Abs. 3 SächsStatG).
- Gemäß § 9 Abs. 5 SächsStatG ist die Einrichtung der örtlichen Erhebungsstelle - eben als kommunaler Statistikstelle - der Rechtsaufsichtsbehörde (§ 112 SächsGemO) und dem Sächsischen Datenschutzbeauftragten schriftlich anzuzeigen.
- § 1 Abs. 1 Satz 5 GWZVO darf, weil nichtig, nicht beachtet werden: § 9 Abs. 1 Satz 1 SächsStatG ist zu entnehmen, daß es in einer Gemeinde immer nur genau eine kommunale Statistikstelle geben darf. Chemnitz, Dresden und Leipzig dürfen demnach, abweichend von der Bekanntmachung des SMI vom 24. Januar 1995 (SächsABl. 1995 S.214), jeweils nur *eine* Stelle - als kommunale Statistikstelle - mit der Durchführung der Gebäude- und Wohnungszählung 1995 beauftragen.

Unabhängig von der Auslegungsfrage zu § 4 Abs. 1 Satz 2, Abs. 2 Satz 1 SächsStatG gilt außerdem:
Abweichend von § 5 Abs. 2 GWZVO sind die in der örtlichen Erhebungsstelle Beschäftigten sowie die Erhebungsbeauftragten vor dem Beginn ihrer Tätigkeit schriftlich auf die Wahrung des Statistikgeheimnisses und zur Geheimhaltung auch solcher Erkenntnisse über Auskunftspflichtige zu verpflichten, die sie lediglich *gelegentlich* ihrer Tätigkeit gewinnen.

5.7.2 Weitergabe von Daten aus der allgemeinen Viehzählung an die Sächsische Tierseuchenkasse

Schwierigkeiten gibt es mit der Regelung des § 16 Abs. 4 SächsAGTierSG. Die von mir aus wohlerwogenen Gründen seinerzeit im Gesetzgebungsverfahren akzeptierte Vorschrift regelt, wie die Tierseuchenkasse an Angaben darüber kommt, wer mit welchen Tierbeständen als Tierbesitzer zu der Kasse beitragspflichtig ist, deren Aufgabe es ist, tierseuchenbedingte Schäden zu ersetzen und Vorbeuge- und Bekämpfungsmaßnahmen finanziell zu fördern (§ 6 SächsAGTierSG). Der Wortlaut

> "Grundlage für die Feststellung der Beitragsschuld sind die Ergebnisse der Viehzählung durch das Landesamt für Statistik. Die Gemeinde- oder Stadtverwaltung übergibt auf einem Formblatt die für die Beitragserhebung erforderlichen Angaben aus der Viehzählung"

besagt, daß Daten, die im Rahmen der allgemeinen Viehzählung nach §§ 18-20 AgrStatG erhoben werden, an die Sächsische Tierseuchenkasse übermittelt werden dürfen (und auch müssen).

Das Statistische Landesamt hat jedoch in der praktischen Durchführung der Viehzählung 1992 die Datenübermittlung von der Einwilligung des Betroffenen abhängig gemacht. Es hat nämlich auf dem Fragebogen dem Tierhalter die Möglichkeit geboten, durch eine entsprechende Eintragung die Behörde ausdrücklich dazu zu ermächtigen, die für die Viehzählung gemachten Angaben an die Tierseuchenkasse weiterzuleiten. Im Jahr 1994 hat das Statistische Landesamt sich gegenüber der Sächsischen Tierseuchenkasse nur dazu verstanden, daß zusammen mit seinen Vordrucken für die Viehzählung auch Erhebungsvordrucke der Tierseuchenkasse ausgeteilt werden durften (sogenannte *kombinierte Erhebung*, vgl. BVerfGE 65, 1, 61).

Gegenüber den vom Statistischen Landesamt, aber auch unabhängig davon von dem einen oder anderen aufmerksamen kommunalen Statistik-Verantwortlichen, vorgebrachten Einwänden gegen die Rechtsgültigkeit des § 16 Abs. 4 SächsAGTierSG - als bereichsspezifischer Ermächtigungsgrundlage sowohl für die in Frage stehende Datenerhebung (durch die Landestierseuchenkasse mit Hilfe der Gemeinden) wie auch für die Übermittlung aus der Durchführung der allgemeinen Viehzählung an die Landestierseuchenkasse - habe ich auf folgendes hingewiesen:

Die Vorschrift entspricht § 71 Abs. 1 Satz 1, 2. Halbs. TierSG. Dort werden die Länder ermächtigt, zu regeln, daß im Wege von Tierzählungen Daten über Viehbestände zum Zwecke der Beitragserhebung für Einrichtungen erhoben werden, die Träger der tierseuchenrechtlichen Entschädigung sind.

§ 16 Abs. 4 SächsAGTierSG verstößt auch, entgegen der Auffassung des Statistischen Landesamtes, nicht gegen § 16 Abs. 1 BStatG, der bestimmt, daß Einzelangaben über persönliche oder sachliche Verhältnisse, die für eine Bundesstatistik gemacht werden, von den mit der Durchführung Betrauten geheimzuhalten sind, soweit durch besondere Rechtsvorschrift nichts anderes bestimmt ist. Nicht nur, daß diese besondere Rechtsvorschrift nicht notwendig eine eine Bundesstatistik anordnende Rechtsvorschrift sein muß; sie muß auch keineswegs eine Rechtsvorschrift des *Bundes* sein. Für eine solche vom Wortlaut der Vorschrift nicht gebotene enge Auslegung gibt es keinen Grund.

Im Gegenteil: Der Gesetzgeber des Bundesstatistikgesetzes hat in der textlichen Umgebung des § 16 Abs. 1 in anderen Fällen durchaus ausdrücklich bestimmt, wenn er gerade ein Landesgesetz (§ 16 Abs. 5 Satz 2, § 25 BStatG) oder gerade ein Bundesgesetz (§ 24 Satz 1 Nr. 3 BStatG) voraussetzt. Es gibt auch nicht etwa verfassungsrechtliche Gründe dafür, daß der Bundesgesetzgeber im Bereich der ausschließlichen Gesetzgebung (Art. 73 Nr. 11 GG) bundesgesetzlich landesgesetzliche Ausnahmevorschriften nicht zulassen dürfe.

Eingewandt worden ist ferner, § 98 Abs. 1 AgrStatG verbiete eine Übermittlung von Einzelangaben außerhalb des durch § 16 Abs. 4 BStatG gesteckten Rahmens. Der Einwand verkennt jedoch, daß die allgemeine Ausnahmen-Zulassung in § 16 Abs. 1 Satz 1 a. E. BStatG *neben* den besonderen Rahmenregelungen für die (durch Rechtsvorschrift außerhalb des Bundesstatistikgesetzes geschehende) Zulassung von Übermittlungen von Einzelangaben in den Absätzen 4 und 5 des § 16 BStatG steht. Dieses *Nebeneinander* zweier Erlaubnisse für eine ausnahmsweise Zulassung von Übermittlungen ergibt sich deutlich aus § 16 Abs. 8 Satz 1 sowie Abs. 9 Satz 1 BStatG.
Das bedeutet: § 98 Abs. 1 AgrStatG macht in der von § 16 Abs. 4 Satz 2 BStatG vorgeschriebenen Weise von der in § 16 Abs. 4 Satz 1 BStatG gegebenen Möglichkeit Gebrauch, eine bestimmte Art von Übermittlungen aus dem Bereich der Statistikverwaltung nach außerhalb zu erlauben. Damit ist durch § 98 Abs. 1 AgrStatG nicht ausgeschlossen, daß eine andere besondere Rechtsvorschrift, welche also nicht die Eigenschaft hat, eine eine Bundesstatistik anordnende Rechtsvorschrift zu sein, eine Ausnahme vom Übermittlungsverbot des § 16 Abs. 1 Satz 1 BStatG enthält. Gerade eine solche Rechtsvorschrift ist aber, wie dargelegt, § 16 Abs. 4 SächsAGTierSG.

§ 16 Abs. 1 Satz 1 a. E. BStatG verstößt auch nicht etwa gegen das verfassungrechtliche Bestimmtheitsgebot (Gebot der Normenklarheit). Die Regelung erlaubt ja, wie dargelegt, Ausnahmen vom Verbot der Übermittlung personenbezogener Daten (Einzelangaben), die im Rahmen der Durchführung einer Statistik erhoben werden, nach außerhalb der Statistikverwaltung und bestimmt, daß diese Ausnahmen nicht in der die betreffende Statistik anordnende Rechtsvorschrift enthalten sein müssen (wie im Falle des § 16 Abs. 4 BStatG), sondern daß sie auch in anderen, besonderen Rechtsvorschriften enthalten sein dürfen. Dies könnte den Einwand begründen, in solchen Fällen könne entgegen den verfassungsrechtlichen Anforderungen (BVerfGE 65, 1, 62 unten) der Bürger aus der gesetzlichen Regelung nicht klar erkennen, daß seine Daten nicht allein zu statistischen Zwecken verwendet werden, zumal das Bundesverfassungsgericht in dieser Hinsicht allem Anschein nach im Hinblick auf eine Lockerung der Zweckbindung gesteigerte Anforderungen an die Normenklarheit stellt.

Das Bundesverfassungsgericht hat jedoch nicht verlangt, daß die die Zweckbindung einschränkende Übermittlungserlaubnis in dem die Statistik anordnenden Gesetz selbst enthalten sein muß. Wenn es (a. a. O.) von *der gesetzlichen Regelung* spricht, so ist dies, einen genauen Sprachgebrauch durch das Gericht unterstellt, eine Formulierung, welche die Gesamtheit der zur Datenverarbeitung ermächtigenden gesetzlichen Regelung (welche z. B. auch Verordnungen enthalten kann) meint. Dem entsprechen auch die auf der Grundlage der zitierten Erwägungen des Volkszählungsurteils vom Bundesverfassungsgericht ausgesprochenen konkreten Beanstandungen von Vorschriften, welche die Verwendung von gemäß dem Volkszählungsgesetz 1983 zu erhebenden Daten zu

nichtstatistischen Zwecken regeln sollten: Das Gericht hat nicht etwa gerügt, daß die Folgen der Einschränkung der Zweckbindung durch Erlaubnis eines Melderegisterabgleiches in einem *anderen* Gesetz als dem VZG 1983 geregelt waren. Vielmehr hat das Bundesverfassungsgericht gerügt, daß die melderechtlichen Übermittlungserlaubnisse und -pflichten zu breit gefächert und dadurch für den Bürger unübersichtlich seien ("nicht vorhersehbar", a. a. O. S. 64; "nicht mehr zu übersehen vermag", S. 65), um eine Verwendung aus einem ganz anderen Bereich stammender Daten erlaubt sein zu lassen. Tragender Grund der Verwerfung des Melderegisterabgleiches nach § 9 Abs. 1 VZG 1983 war, daß für den Betroffenen nicht erkennbar war, daß seine statistischen Angaben *in weitem Umfang an Behörden und öffentliche Stellen übermittelt werden konnten, ohne daß diese den statistischen Ursprung dieser Daten feststellen und dem Nachteilsverbot Rechnung hätten tragen können* (BVerfGE a.a.O. S. 65).

Die vorhandene Regelung in § 16 Abs. 4 SächsAGTierSG bzw. die Praxis des Jahres 1994, die auf eine *kombinierte Erhebung* (Bundesverfassungsgericht a. a. O. S. 61 unten, vgl. auch S. 66 oben) hinausläuft, sind also meines Erachtens nach dem gegenwärtigen Stand der Rechtsprechung des Bundesverfassungsgerichts *nicht* verfassungswidrig.

Bei dieser Einschätzung spielen auch Gegebenheiten der landwirtschaftlichen Viehhaltung, welche die Grundlage für die Angemessenheit einer Zwangsversicherung der Tierhalter, in Gestalt eben der Tierseuchenkasse, sind, neben seuchenmedizinischen Gründen eine Rolle; und ebenso der Grund des Schutzes der Landwirtschaft vor den - höheren - Kosten desjenigen Verwaltungsaufwandes, der nötig wäre, wenn man *auf andere Weise* als durch die in § 16 Abs. 4 SächsAGTierSG vorgesehenen Datenverarbeitung mit gleicher Wirksamkeit den Bestand der Versicherung dadurch sichert, daß eine 'Einladung' zum Betrug vermieden wird.

Diese Erwägungen gelten für eine etwaige Änderung (Präzisierung) des § 16 Abs. 4 SächsAGTierSG unverändert fort.

Allerdings wäre es der Wahrung des Grundrechts auf informationelle Selbstbestimmung zusätzlich förderlich, wenn statt der zeitweise vom Statistischen Landesamt aufgedruckten Einwilligungs-Frage ein klarer und verständlicher Hinweis darauf in den Vordruck aufgenommen würde, daß die im Wege der allgemeinen Viehzählung (auf der Grundlage des Agrarstatistikgesetzes) erhobenen Daten gemäß § 16 Abs. 4 Satz 1 des Landestierseuchengesetzes nicht ausschließlich zu statistischen Zwecken verwendet werden, sondern, eben aufgrund einer Ausnahmeregelung, der Sächsischen Landestierseuchenkasse zum Zwecke der Feststellung der Beitragsschuld übermittelt werden.

Eine Stellungnahme des Statistischen Landesamtes bzw. des SMI zu meiner letzten, ausführlichen Stellungnahme in dieser Sache steht schon seit einiger Zeit aus - genauso wie eine Erläuterung des Statistischen Landesamtes dazu, auf welcher Rechtsgrundlage es bei der Durchführung der Viehzählung Gemeinden als Erhebungsstellen hat tätig werden lassen.

5.7.3 Umfrage einer Stadtverwaltung zum Betrieb kommunaler Kindereinrichtungen

Der Vater eines Kindergartenkindes machte mich darauf aufmerksam, daß eine Stadtverwaltung - Sachgebiet Soziales - die Eltern aufforderte, einen Fragebogen auszufüllen, auf dem es u. a. hieß: "Sind Sie mit einer christlichen Erziehung durch einen kirchlichen freien Träger einverstanden?" und "Sind sie einverstanden, daß die Kindereinrichtung weiterhin von der Stadt verwaltet wird?" Mögliche Antworten jeweils: "ja, nein, egal,". Im unteren Teil des Fragebogens sollten die Erziehungsberechtigten den Namen ihres Kindes und ihre Anschrift angeben. Danach sollten die Erziehungsberechtigten den unterschriebenen Fragebogen in einem beigefügten Briefumschlag in der jeweiligen Einrichtung abgeben. Hinweise auf eine Rechtsgrundlage für die Durchführung dieser Erhebung oder auf eine Freiwilligkeit der Teilnahme und das weitere Verfahren (zum Beispiel auf eine frühzeitige Anonymisierung der personenbezogenen Daten und die Vernichtung der Fragebögen) enthielt der Fragebogen nicht.

Rechtlich gesehen handelte es sich bei dieser Umfrage um eine kommunale Statistik. Denn die Stadtverwaltung holte Daten nicht zur Regelung einzelner Rechtsverhältnisse, sondern zur Gewinnung von Erkenntnissen über Personengesamtheiten (sozialwissenschaftlich: "Kollektive") ein; die Statistikgesetze sprechen von "Daten über *Massenerscheinungen*". Da die Daten eigens bei den Einzelnen eingeholt wurden und nicht etwa aus ohnehin schon in der Verwaltung vorhandenen Unterlagen zusammengestellt wurden, handelte es sich auch um eine sogenannte *Primär*statistik. Solche Statistiken bedürfen stets einer *Rechtsvorschrift* als Grundlage, nach sächsischem Statistikrecht sogar auch im Falle der Freiwilligkeit (Erhebung *ohne* Auskunftspflicht; vgl. § 6 S. 1 SächsStatG, hier i. V. m. § 8 Abs. 1 S. 2, 2. HS.). Im Falle der Anordnung von Statistiken durch *Gemeinden* kommt als Rechtsgrundlage nur eine (kommunale) *Satzung* in Frage (§ 8 Abs. 1 Satz 2, 1. Halbs.).

Eine solche Satzung hatte die betreffende Stadt jedenfalls zum damaligen Zeitpunkt noch nicht. Auch konnte sie sich nicht auf die Ausnahmevorschrift des § 25 Satz 1 SächsStatG berufen. Danach dürfen zwar bereits bestehende Statistiken, die nach den Vorschriften des Sächsischen Statistikgesetzes durch Rechtsvorschrift oder von einer obersten Landesbehörde anzuordnen sind, bis zum 4. Juni 1995 ohne eine solche Rechtsgrundlage weiter durchgeführt werden. Diese Voraussetzung lag aber nicht vor, denn die betreffende Stadtverwaltung führte diese Statistik zum ersten Mal (und nach Inkrafttreten des Sächsischen Statistikgesetzes) durch.

Ferner hat die Umfrage gegen mehrere andere Vorschriften des Sächsischen Statistikgesetzes verstoßen. Diese sind auch dann zu beachten, wenn nach § 25 Satz 1 SächsStatG eine Satzung als Rechtsgrundlage nicht vorhanden sein muß (§ 25 S. 2 SächsStatG):

- Anstelle der Erhebung und Speicherung der statistischen *Hilfsmerkmale* Name und Anschrift des Kindes sowie Unterschrift von Erziehungsberechtigten, die eine Zuordnung des einzelnen Erhebungsbogens zu bestimmten Elternpaaren (Erziehungsberechtigten) ermöglichten, hätte eine fortlaufende Numerierung der

Fragebögen die Gefahr einer mehrfachen Teilnahme an der Umfrage genauso zuverlässig ausgeschlossen. Es hätte also ohne Gefährdung der Richtigkeit der Statistik die Umfrage von vornherein anonym durchgeführt werden können. Mithin ist gegen das Gebot der frühestmöglichen Anonymisierung (§ 1 Abs. 2, 2. Halbs. SächsStatG) verstoßen worden.

- Abgesehen davon ist *nach* der eigentlichen *Erhebung* § 14 Abs. 1 SächsStatG nicht beachtet worden: Die Hilfsmerkmale sind von den Erhebungsmerkmalen zum frühestmöglichen Zeitpunkt zu trennen und gesondert aufzubewahren sowie zu löschen, sobald die Überprüfung der Erhebungs- und Hilfsmerkmale auf ihre Schlüssigkeit und Vollständigkeit abgeschlossen ist.
  Dies hätte bedeutet, daß der Name des Kindes, die Anschrift sowie die Unterschrift des Erziehungsberechtigten unmittelbar nach Abschluß der Umfrage (Erhebungsphase) von dem Teil des Umfragebogens, auf dem die Fragen gestellt wurden, (körperlich) hätte getrennt werde müssen.
- Verstoßen worden ist ferner gegen § 9 SächsStatG, wonach Kommunalstatistiken von einer besonderen, für die Durchführung statistischer Aufgaben zuständigen Stelle durchzuführen sind, die von anderen Verwaltungsstellen abgeschottet sein muß.
  Vorliegend hätte das für diesbezüglichen *Verwaltungsvollzug* zuständige "Sachgebiet Soziales" gerade *nicht* mit der Durchführung und Auswertung der Umfrage beauftragt werden dürfen. Die Statistik hätte vielmehr von der für die Durchführung *statistischer Aufgaben* zuständigen Stelle der Stadtverwaltung durchgeführt werden müssen.
- Schließlich ist gegen § 20 SächsStatG verstoßen worden, wonach die zu Befragenden schriftlich u. a. über die Geheimhaltung (nach § 18 SächsStatG) und die Auskunftspflicht oder die Freiwilligkeit der Auskunftserteilung zu unterrichten sind.

Gegenüber der betreffenden Stadtverwaltung habe ich diese Verstöße gemäß § 26 SächsDSG beanstanden müssen.

Wie im einzelnen ersichtlich, hätte die wünschenswerte, ja vorbildliche Einbeziehung von Eltern in die Vorbereitung kommunaler Entscheidungen über Kindertageseinrichtungen ohne allzu großen Aufwand auch rechtmäßig durchgeführt werden können.

5.8 Archivwesen

5.8.1 Verbleib der bei Gemeinden und Landkreisen unter Verschluß gehaltenen Altdaten aus der Zeit von 1945 bis 1990

Der Gesetzgeber hat im Anschluß an § 35 SächsDSG in §§ 4 Abs. 2 Satz 2 und 3 sowie 5 Abs. 2 SächsArchG für die Daten aus der Zeit zwischen dem 8. Mai 1945 und dem 2. Oktober 1990 eine Sonderregelung vorgesehen: Sämtliche Unterlagen sind der staatlichen Archivverwaltung anzubieten und auf Anforderung herauszugeben. Nimmt man die Vorschrift des § 13 Abs. 1 SächsArchG hinzu, der zufolge, etwas vereinfacht, die kommunalen Träger der Selbstverwaltung ihr Archivgut *einschließlich des von ihnen übernommenen Archivgutes nach § 4 Abs. 2 SächsArchG*, also der 'Altdaten' archivieren, ist das Gesetz aufgrund seines Wortlautes so zu verstehen: Im Hinblick auf die Masse der Altdaten, die sich ja in kommunaler Hand befindet, hat die staatliche Archivverwaltung eine Ermessens-Entscheidung in folgender Weise zu treffen: Nicht alle Unterlagen haben sich die staatlichen Archive herausgeben zu lassen; aber sie dürfen auch nicht auf alle Unterlagen aus dieser Zeit verzichten und sie - zugunsten der Kommunen - freigeben.
Andererseits ist den Kommunen und Landkreisen die Archivierung von Unterlagen aus der Zeit von 1945 bis 1990 durch den zitierten Passus in § 13 SächsArchG (der übrigens in den abschließenden Beratungen vom Innenausschuß in das Gesetz eingefügt worden ist) zur Aufgabe gemacht worden. Sie dürfen also nicht alle Unterlagen aus dieser Zeit, die ihnen die staatliche Archivverwaltung überläßt, für nicht archivwürdig erachten und vernichten. Die Kommunen unterliegen insoweit der staatlichen *Rechtsaufsicht.*

Leider (siehe meinen 2. Tätigkeitsbericht unter 5.8.2) hat sich insofern kaum etwas getan: Das SMI sieht sich offenbar nicht in der Lage, eine nennenswerte Menge der unter § 4 Abs. 2 Satz 2 SächsArchG fallenden Unterlagen in den staatlichen Archiven zu archivieren. Soweit mir bekannt, beabsichtigt das SMI daher, statt einer Übernahme der von ihm als archivwürdig eingestuften Unterlagen diese den Kommunen zu überlassen. Sie sollen die Unterlagen *für die staatlichen Archive* und namentlich unter deren *Aufsicht* aufbewahren: Überlassung nur, wenn und solange das kommunale Archiv bestimmte räumliche und personelle Voraussetzungen erfüllt.

Ich habe größte Zweifel, ob dies im Sinne des sächsischen Gesetzgebers ist. Hier wird am Grundsatz der Selbstverwaltung vorbei eine Konstruktion gesucht, die Gemeinden partiell zur unteren staatlichen Archivverwaltung zu deklassieren.

Unabhängig davon gilt: Ich muß aus Datenschutzgründen darauf dringen, daß in den Vereinbarungen zwischen dem Freistaat und den Kommunen der Gegenstand der Vereinbarung, wenn ich mich laienhaft einmal so ausdrücken darf, *faszikel-scharf* schriftlich bestimmt wird. Das ist schon Voraussetzung einer rechtlichen Wirksamkeit, aber auch praktischen Durchführbarkeit einer solchen Vereinbarung. Außerdem sollte § 35 SächsDSG ja schließlich nicht 'für die Katz' gewesen sein!

Außerdem muß dies alles mit viel größerer Geschwindigkeit geschehen, als sie bisher zu verzeichnen war.

Ich habe im Februar 1993 an den Vorsitzenden des Innenausschusses geschrieben:

"Die staatlichen Archive, bei denen solche Altdaten aufbewahrt werden, die der Rehabilitierung oder dem Auskunftsanspruch einzelner dienen können oder deren Inhalt zeitgeschichtliche Bedeutung zukommt, sind vom Staatsministerium des Innern zu bestimmen. Im Interesse der inneren und äußeren Sicherheit dieser sensiblen Aktenbestände halte ich eine Konzentration auf wenige (leistungsfähige) staatliche Archive für geboten. Dabei dürften sich die Staatsarchive in Dresden, Leipzig und Chemnitz anbieten. Eine Entscheidung des Parlaments für die von mir vorgeschlagene Lösung wird später einen gewissen Mehraufwand der staatlichen Archivverwaltung erfordern, der im Interesse einer gebotenen Aufarbeitung der Vergangenheit zu berücksichtigen ist."

Damals wurde meine Meinung von Parlament und Regierung geteilt. Jetzt, wo es ans Arbeiten geht, wird gekniffen.

Vgl. zu diesem Problem ferner den nachstehenden Abschnitt.

5.8.2 Keine Anwendbarkeit des Sächsischen Archivgesetzes auf die Einsichtnahme in Altdaten, die noch nicht förmlich der staatlichen Archivverwaltung angeboten worden sind

Nachdem ich in einem an mich herangetragenen Einzelfall zunächst vom Gegenteil ausgegangen bin, also davon, daß sich die Einsichtnahme in Altdaten nach dem Sächsischen Archivgesetz richtet, habe ich nach gründlicherer Prüfung meine Meinung revidieren müssen.

Der Grund dafür ist folgender:

§§ 9 ff. SächsArchG gelten dem Wortlaut nach für *Archivgut.* Archivgut sind nach § 2 Abs. 1 SächsArchG, vereinfacht, *archivwürdige Unterlagen*. Aufgrund der systematischen Stellung der Vorschriften im Gesetz und aus Gründen der sinnvollen praktischen Anwendbarkeit können sich die §§ 9, 10 nur auf solche archivwürdigen Unterlagen beziehen, hinsichtlich deren das Vorliegen der Eigenschaft, archivwürdige Unterlagen zu sein, von zuständiger Stelle (konstitutiv) festgestellt worden ist.
Aus § 13 Abs. 1 i. V. m. Abs. 3 Satz 1 SächsArchG, der die entsprechende Anwendung - u. a. - der §§ 9 ff. SächsArchG regelt, ergibt sich nichts anderes. Die Kommunen *bewahren* nämlich seit dem Inkrafttreten des § 35 SächsDSG (gemäß dessen Abs. 2 Satz 2) diese Unterlagen unter Verschluß auf und haben sie, auch wenn eine förmliche Übernahme ins Kommunalarchiv stattgefunden haben sollte, seit Inkrafttreten des Sächsischen Archivgesetzes der staatlichen Archivverwaltung anzubieten und auf Verlangen herauszugeben (§ 5 Abs. 2 SächsArchG).

Darauf, inwieweit die Altdaten von Kommunen förmlich in ihr Archiv aufgenommen oder aber sonstwie aufbewahrt werden, kommt es nach allen Regeln, die das Archivgesetz diesbezüglich enthält, nicht an. Insbesondere wäre es unter dem Gesichtspunkt der archivischen Benutzbarkeit bzw. des Datenschutzes höchst bedenklich, wenn es die Kommune in der Hand hätte, nach Belieben die Unterlagen vor der Anbietung (an das

zuständige staatliche Archiv) in der einen oder aber der anderen Rechtsform aufzubewahren, mit womöglich unterschiedlichen Rechtsfolgen. Soweit Archivrecht nicht anwendbar ist, wäre nämlich, als Auffangregelung, das Sächsische Datenschutzgesetz maßgebend. Und dann ergeben sich in der Tat unterschiedliche Rechtsfolgen. *Das Archivgesetz gewährt hinsichtlich der auf Amtsträger bezogenen Daten großzügigere Einsicht als § 12 Abs. 2 Nr. 4 SächsDSG:* In dieser Vorschrift verlangt das Sächsische Datenschutzgesetz in jedem Fall, daß das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen am Unterbleiben der Kenntnisnahme von seinen Daten erheblich überwiegt. Dagegen macht das Archivgesetz, in § 10 Abs. 4 Satz 2, 1. Halbs., dies nur für den Fall der Verkürzung der Schutzfristen zur Voraussetzung, die als persönlichkeitsschutzbezogene Schutzfristen (§ 10 Abs. 1 Satz 3 SächsArchG) gemäß § 10 Abs. 2 Satz 3 SächsArchG *Amtsträgern* (in Ausübung ihrer Ämter) von vornherein nicht zugute kommt. Dem entspricht es, daß der allgemeine archivrechtliche Einsichtsanspruch des § 9 Abs. 1 SächsArchG und auch der archivrechtliche Auskunftsanspruch des *Betroffenen*, gemäß § 6 SächsArchG, namentlich dessen Abs. 3, weiter geht als die in § 17 SächsDSG insoweit eingeräumten Rechte.

Der Zustand, daß über die Archivwürdigkeit bzw. Archivierung der Altdaten aus dem nichtstaatlichen Bereich, namentlich der Kommunen, noch nicht - gemäß § 5 Abs. 2 i. V. m. Abs. 4 SächsArchG - entschieden ist, ist folglich der Erforschung des Handelns von Staat und herrschender Partei seit 1945, aber auch vor 1945, (auch) unter datenschutzrechtlichen Gesichtspunkten in einer Weise hinderlich, die vom Sächsischen Gesetzgeber, wie im Archivgesetz vom 17. Mai 1993 zum Ausdruck gebracht, *nicht gewollt* ist.

In der Praxis wird nach meinem Eindruck das Sächsische Archivgesetz angewandt; wie erwähnt habe auch ich zunächst diese sich hier aufdrängende Meinung geteilt. Es ist jedoch *dringend erforderlich*, für eine rasche und umfassende Durchführung des § 5 Abs. 2 SächsArchG zu sorgen, damit wir insoweit zu rechtsstaatlich sauberen Verhältnissen kommen, ohne das im Archivgesetz - auf meine Anregung - gewährte besondere Auskunftsrecht Betroffener im Hinblick auf Altdaten zu verkürzen.

5.9 Polizei

5.9.1 Automatisiertes Informationssystem der Polizei

Das polizeiliche Auskunftssystem Sachsen (PASS) soll die Polizeidienststellen des Freistaates Sachsen bei der Erfassung, Speicherung und Auswertung von polizeilich relevanten Informationen zu Straftaten, Personen und Sachen unterstützen. Das System bietet den Polizeidienststellen landesweit Zugriff und ermöglicht später einen Verbund mit dem bundesweiten Informationssystem der Polizei (INPOL-Bund). Gegenwärtig wird PASS als automatisiertes Abrufverfahren nach § 48 Abs. 1 SächsPolG i. V. m. § 8 Abs. 1 SächsDSG probeweise betrieben.

Datenschutzrechtlich kommt der Protokollierung von Abfragen große Bedeutung zu. Abfragen aus PASS werden derzeit lediglich von Hand protokolliert. So führen die an den Datenstationen eingesetzten Bediensteten schriftliche Nachweise über
- Namen und Dienststelle des Auskunftsersuchenden,
- Zeitpunkt der Auskunft,
- Zweck der Auskunft,
- Art und Umfang der Auskunft.

Ich habe dem SMI empfohlen, eine - für interne, aber auch meine Kontrollzwecke dringend erforderliche - automatisierte Zusatzprotokollierung in PASS einzuführen. Das SMI hat angekündigt, in der überarbeiteten PASS-Version diese datenschutzrechtliche Forderung zu berücksichtigen und eine erweiterte automatisierte Kontrollprotokollierung vorzusehen; lediglich der Umfang der Protokolldatensätze stehe noch nicht fest.

Ich habe das SMI gebeten, mich über die weiteren Entwicklungen zu PASS fortlaufend und umfassend zu unterrichten, weil ich nur so meine Beratungsfunktion effektiv erfüllen kann.

5.9.2 Richtlinien für die Führung kriminalpolizeilicher personenbezogener Sammlungen

Zu den Kriminalpolizeilichen Sammlungen (KpS) gehören automatisch geführte Dateien (wie z. B. PASS), manuell geführte Dateien (z. B. Lichtbilderkarteien), Listen (z. B. Fahndungslisten) und kriminalpolizeiliche personenbezogene Akten (z. B. Ermittlungs- oder Kriminalakten). Sie dienen in erster Linie dazu, die Ermittlungen der Polizei zu unterstützen und verdächtige Personen vorläufig festzunehmen. Ferner sollen sie Hinweise für die vorbeugende Verbrechensbekämpfung geben und den Ablauf und die Grundlagen polizeilichen Handelns dokumentieren.

Die Aufbewahrung der KpS ist jedoch nur so lange zulässig, wie sie die Polizei zu ihrer rechtmäßigen Aufgabenerfüllung benötigt. Gegeneinander abzuwägen sind hierbei das öffentliche Interesse, zu Zwecken der Strafverfolgung, Strafvollstreckung oder Gefahrenabwehr auf polizeiliche Erkenntnisse zurückgreifen zu können, und das Interesse des Einzelnen, solchen Einwirkungen der öffentlichen Gewalt nicht grundlos ausgesetzt zu sein. Aus diesem Grunde ist beispielsweise die Aufbewahrung der KpS zum Zweck der

(vorbeugenden) Verbrechensbekämpfung nur zulässig, "wenn Tatsachen die Annahme rechtfertigen, daß wegen Art und Ausführung der Tat, die der Betroffene begangen hat oder deren er verdächtig war, die Gefahr der Wiederholung besteht". Die Folge ist, daß nach den KpS-Richtlinien die Kriminalpolizeilichen Sammlungen - jeweils fallabhängig - nach bestimmten Fristen auszusondern oder zu löschen sind.

Das SMI plant, die KpS-Richtlinien neu zu regeln und an das 1994 geänderte Sächsische Polizeigesetz anzupassen. Weil die Datenverarbeitungsvorschriften dieses Gesetzes aber zum großen Teil ausfüllungsbedürftige Generalklauseln oder bloße Verweisungen auf das Sächsische Datenschutzgesetz sind, habe ich empfohlen, konkretisierende Regelungen in die KpS-Richtlinien aufzunehmen. Dies sind Regelungen
- zur Auskunftserteilung,
- zu den Zuständigkeiten in bezug auf die Führung der KpS,
- zu den nach § 50 SächsPolG vorgeschriebenen Errichtungsanordnungen,
- zur Datenübermittlung,
- zur Art der Sperrung und Löschung,
- zum Zweckbindungsgrundsatz nach § 43 Abs. 1 Satz 2 SächsPolG.

Auch wenn diese Bereiche zum Teil bereits durch bestehende Verwaltungsvorschriften abgedeckt sind (z. B. für die polizeiliche Auskunftserteilung), ist es sinnvoll, die Führung von Kriminalakten insgesamt und zusammenhängend zu regeln.

Das SMI hat mir zugesichert, mich bei der Neuregelung der KpS-Richtlinien so frühzeitig wie möglich zu beteiligen.

5.9.3 Projekt "Mobiles Polizei-Büro-System"

Aus Zeitungsmeldungen erfuhr ich, daß die Sächsische Polizei ein tragbares "Mobiles-Polizei-Büro-System" (M.O.P.S.) einführen will. Das System, an dessen Entwicklung das Landespolizeipräsidium Dresden beteiligt war, sollte zunächst dazu dienen, die Polizeibeamten von Schreib- und Büroarbeiten zu entlasten und zu ermöglichen, daß Informationen am Tat- oder Unfallort selbst elektronisch erfaßt, aufbereitet und ausgedruckt werden können.

Die Eingabe von Informationen erfolgt dabei nicht über eine Tastatur, sondern handschriftlich mit einem Stift, der direkt über das Display eines sogenannten Pentops geführt wird. Um Unbefugten den Zugang zu diesem System zu verwehren, erhalten die Polizeibediensteten personengebundene Chipkarten, ohne die das Gerät nicht bedienbar ist. Zum Dienstende - oder nach Erreichen der Speicherkapazität von ungefähr 20 Vorgängen - erfolgt eine Datensicherung auf dem stationären Personalcomputer der Dienststelle. Auf dem Pentop werden diese Daten dann gelöscht.

Das SMI beabsichtigt nunmehr, die Nutzungsmöglichkeiten zu erweitern: So soll das System mit den automatisierten Polizeidateien kompatibel werden, um damit dem Polizeibeamten "vor Ort" umfassenden Zugriff auf diese Datenbestände (darunter Fahndungs- und Verkehrsdaten) zu ermöglichen.

Ich habe das SMI aufgefordert, den Umfang der geplanten Online-Anschlüsse klar zu umreißen. Besondere Bedeutung kommt angesichts der flächendeckenden Zugriffsmöglichkeiten einem tragfähigen Datenschutzkonzept zu, das mir bislang noch nicht vorgelegt wurde. Dem Projekt werde ich besondere Aufmerksamkeit widmen.

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

Nach meinen Feststellungen finden im Freistaat Sachsen Hinweise auf die sexuelle Orientierung von Zeugen und Opfern sowie der "antihomosexuelle" Hintergrund einer Straftat Eingang in kriminalpolizeiliche personenbezogene Sammlungen. Ein Beispiel hierfür ist das beim Landeskriminalamt Sachsen geführte Polizeiliche Auskunftssystem Sachsen (PASS). In dieser Datei werden bei den Angaben zum Opfer auch Hinweise auf seine sexuelle Orientierung (z. B. Homosexualität) aufgenommen. Nach Auskunft des SMI geschieht dies, wenn besondere Tatumstände vermuten lassen, daß derartige Merkmale des Opfers eine markante Rolle für den Straftäter gespielt haben.

Ich habe das SMI in diesem Zusammenhang aufgefordert, die Möglichkeit einer Recherche nach Homosexuellen in PASS technisch auszuschließen, da sie zur Aufgabenerfüllung der Polizei nicht erforderlich ist. Auch wenn die Speicherung personenbezogener Daten von Homosexuellen unter bestimmten Umständen für die Aufklärung konkreter Straftaten erforderlich sein kann, muß verhindert werden, daß die Polizei Listen sämtlicher gespeicherter Homosexueller erstellen kann. Die Kenntnis des bloßen Datums "homosexuell" ist für die Polizeiarbeit nicht erforderlich. Weder sind Homosexuelle potentielle Straftäter, noch sind sie generell gefährdet, das Opfer einer Straftat zu werden. Nur wenn ein homosexueller Beschuldigter verdächtig ist, eine Straftat mit homosexuellem Hintergrund begangen zu haben und Anhaltspunkte für eine Wiederholungsgefahr vorliegen, wäre eine Speicherung dieses Merkmals zu der vorbeugenden Straftatenbekämpfung im Einzelfall zulässig. Bei einem Opfer, Geschädigten, Anzeigeerstatter, Zeugen oder Hinweisgeber kann die Speicherung des Datums "homosexuell" grundsätzlich nur für die Aufklärung von Straftaten, also für einzelne Ermittlungsverfahren erforderlich sein (z. B. bei einem vermuteten antihomosexuellen Hintergrund der Tat). Andere Gründe für eine Speicherung sind für mich nicht ersichtlich. Spätestens nach Abschluß des Ermittlungsverfahrens wären diese Daten deshalb grundsätzlich zu löschen.

Ich werde mich entschieden für einen datenschutzgerechten Umgang mit dem Datum "homosexuell" einsetzen. Gleiches gilt - es sei hier rein prophylaktisch erwähnt - für Dateien über Ausländer, Gastwirte, Bedienstete der Bauverwaltung, Prostituierte, Taxifahrer etc. Sie mögen im Einzelfall als Tipgeber, Zeugen oder "Kunden" der Polizei in Betracht kommen, eine Abstemplung in einer Kartei wird es in Sachsen aber nicht geben.

5.9.5 SMI-Erlaß zum Fahndungsabgleich mit Hotelmeldescheinen

Mit einem Erlaß hatte das SMI die Polizeipräsidien Chemnitz, Dresden und Leipzig angewiesen, im Zeitraum vom 1. November bis 31. Dezember 1994 "schwerpunktmäßig Hotelmeldescheine ... fahndungsmäßig zu überprüfen". Der Erlaß weist zuvor in allgemeiner Form auf die in § 19 Abs. 4 SächsMG normierte Befugnis der Polizeidienststellen hin, die ausgefüllten Meldescheine der Beherbergungsstätten vorgelegt oder übermittelt zu bekommen. Der Erlaß enthält jedoch keinen Hinweis darauf, daß die Ausübung dieser Befugnis von den in § 19 Abs. 4 SächsMG genannten Voraussetzungen abhängt: Danach muß das Vorlegen oder die Übermittlung der Meldescheine zur Gefahrenabwehr, zur Strafverfolgung oder zur Aufklärung des Schicksals von Vermißten oder von Unfallopfern erforderlich sein.

Als einzige Anlaßorientierung wird ein "hohes Vollzugsdefizit aufgrund fehlender polizeilicher Kontrollen" genannt.

Der Erlaß war somit als Anweisung zu einer ereignisunabhängigen, allgemeinen Fahndung anzusehen. Bei dieser Fahndungsart geht es nicht um Gefahrenabwehr - denn eine konkrete, unmittelbare Gefahr ist nicht erkennbar -, sondern einzig um Strafverfolgung. Weil aber bei einer ereignisunabhängigen Fahndung ein Bezug zu einem individuellen Verhalten oder einem bestimmten Anlaß fehlt und das einschlägige Strafverfahrensrecht für solche - nicht polizeirechtlich begründeten - Fahndungsmaßnahmen eine entsprechende Befugniszuweisung nicht enthält, entbehrt die angeordnete Maßnahme einer rechtlichen Grundlage.

Ich habe das SMI aufgefordert, die angewiesenen Polizeipräsidien über die Rechtslage in vollständiger Form unterrichten, wobei der stets fallbezogene Charakter von Fahndungsmaßnahmen hervorzuheben sein wird. Eine pauschale Erhebung birgt schließlich die Gefahr, daß komplette Verzeichnisse von Übernachtungsgästen bei der Polizei entstehen und Daten Unbescholtener gespeichert werden, ohne daß dies mit der Erfüllung polizeilicher Aufgaben gerechtfertigt werden kann.

Die Polizei ist gut beraten, nicht "wild in der Gegend herum" zu ermitteln, sondern sich auf ihre konkret ersichtlichen Aufgaben zu konzentrieren; dabei werde ich sie unterstützen.

Eine Stellungnahme des SMI steht noch aus.

5.9.6 Datenabgleich mit "Rotlichtsündern"

Ein Landratsamt stellte mir die Frage, ob eine Polizeidirektion bei ihm regelmäßig Listen "geblitzter Fahrzeuge" anfordern dürfe. Mit ihrem schriftlichen Ersuchen wollte die Polizeidirektion Fahndungsabgleiche mit den beim Landratsamt vorliegenden Verkehrsüberwachungsdaten ermöglichen.

Datenabgleiche dieser Art beziehen eine Vielzahl von Unverdächtigen in die Fahndung ein, was der Zweckbindung dieser Verwaltungsdaten zuwider läuft. Eine solche der

Rasterfahndung (die nur zur Verfolgung von Straftaten von erheblicher Bedeutung und zur Abwehr einer konkreten Gefahr zulässig ist) nahekommende polizeiliche Maßnahme darf deshalb nur im rechtsstaatlich gesicherten Rahmen erfolgen, das heißt, es muß spezialgesetzlich geregelt sein, unter welchen Voraussetzungen Durchbrechungen der Zweckbindung durch Abgleiche mit Verwaltungsdaten vorgenommen werden dürfen. Beispielhaft sei an dieser Stelle § 35 Abs. 4 StVG erwähnt: Nach dieser Vorschrift übergibt das Bundeskriminalamt dem Kraftfahrt-Bundesamt in regelmäßigen Abständen den gesamten Datenbestand der mit Haftbefehl gesuchten Personen auf einem Datenträger, der dann dort mit den im zentralen Fahrzeugregister gespeicherten Halterdaten verglichen wird. Die Trefferfälle werden an das Bundeskriminalamt übermittelt.

Anders als dieses Verfahren entbehrt das Vorhaben der Polizeidirektion einer hinreichenden rechtlichen Absicherung. Als ereignisunabhängiger allgemeiner Fahndung im Bereich der Strafverfolgung fehlt diesem Vorgehen ein Bezug zu einem individuellen Verhalten oder einem Ereignis. Eine entsprechende Befugniszuweisung ist im Strafverfahrensrecht, das hier allein als Rechtsgrundlage in Frage käme, jedoch nicht enthalten.

Ich habe diesen Fall mit dem sächsischen LKA erörtert, das die Fachaufsicht über die Polizeidirektion führt. Mir wurde zugesichert, bei der Neufassung der einschlägigen Dienstanweisung meine datenschutzrechtliche Kritik zu berücksichtigen. Wichtig wird insbesondere sein, daß nur Daten aus Bußgeldverfahren übermittelt werden, die zur Erfüllung einer konkreten Ermittlungsmaßnahme der ersuchenden Polizeidienststelle geeignet sind, und damit das verfassungmäßige Verhältnismäßigkeitsgebot beachtet wird.

5.9.7 Polizei fordert Ärzte zur Offenbarung von Patientendaten auf

Gesucht war einer, der im Streit einen Menschen erstochen hatte. In einem Schreiben forderte eine Polizeidirektion alle in einem kassenärztlichen Bezirk zugelassenen Ärzte - kommentarlos - auf, Hinweise auf eine an einem bestimmten Tag erfolgte Behandlung von Schnitt- und Stichverletzungen zu geben, die dem Täter durch sein Opfer beigebracht worden.

Das Schreiben machte es notwendig, dem SMI und der Kassenärztlichen Vereinigung Sachsen die datenschutzrechtliche Unzulässigkeit des Ersuchens aufzuzeigen:

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

Schweigepflicht grundsätzlich nicht rechtfertigt. Nur bei besonders schweren und mit einer noch bestehenden, nachhaltigen Störung des Rechtsfriedens verbundenen Verbrechen (Wiederholungstäter schwerster Delikte; terroristische Gewalttaten) kann die Durchbrechung des Arztgeheimnisses zu Zwecken der Strafverfolgung gerechtfertigt sein. Die Rechtsordnung rechtfertigt dies, wenn tatsächliche Anhaltspunkte für die Gefahr der Wiederholung schwerster Straftaten bestehen. Dem Schreiben der Polizeidirektion war jedoch insofern nichts zu entnehmen; vielmehr war von einer einmaligen Konfliktkonstellation auszugehen: Also davon, daß ein Arzt, der aufgrund des Schreibens der Polizeidirektion einen "Hinweis" auf die Person des mutmaßlichen Täters geben würde, sich gemäß § 203 StGB strafbar machen würde.

Ich verkenne nicht den Erfolgs- und Zeitdruck der Kriminalpolizei bei der Ermittlungstätigkeit, zumal bei Tötungsdelikten. Auch ist zu berücksichtigen, daß es sich bei der Frage, ob das Strafverfolgungsinteresse bezüglich bereits begangener Delikte das Arztgeheimnis ausnahmsweise zu durchbrechen geeignet ist, um eine nicht ganz einfache Rechtsfrage handelt. Auf der anderen Seite muß jedoch klar sein, daß die ärztliche Schweigepflicht (wie auch andere Schweigepflichten, z. B. die anwaltliche) nur ausnahmsweise und unter sehr engen Voraussetzungen durchbrochen werden darf. Im Bereich der Strafverfolgung kommt dies praktisch nur in Betracht, wenn die Gefahr der Wiederholung schwerster Straftaten besteht.

Das SMI hat meine Kritik aufgenommen und sofort umgesetzt. Per Erlaß sind die sächsischen Polizeidienststellen nunmehr angewiesen, unter Beachtung meiner Rechtsauffassung von Hilfeersuchen an Ärzte oder andere Berufsgruppen, die Träger eines Berufsgeheimnisses sind, "in aller Regel abzusehen". Sollten "Ausnahmefälle" auftreten, sind die Dienststellen gehalten, einen ausdrücklichen Hinweis auf das Berufsgeheimnis und das etwaige Zeugnisverweigerungsrecht der angesprochenen Berufsgruppe zu geben. Damit ist eine datenschutzgerechte Lösung gefunden worden.

5.9.8 Polizeiermittlungen zu Scheinehen

Im Februar/März 1995 erregten polizeiliche Ermittlungen zu Scheinehen Aufsehen in der Öffentlichkeit. Bei meiner umfassenden datenschutzrechtlichen Kontrolle habe ich folgenden Sachverhalt festgestellt:

Anfang des Jahres 1994 ging beim LKA eine Anzeige ein, die Hinweise auf eine Scheinehe zwischen einer Deutschen und einem Türken in Dresden enthielt. Da das LKA Zusammenhänge zur organisierten Kriminalität (OK) sah, nahm ein Ermittlungsbeamter des LKA bei der Ausländerbehörde Dresden (Einwohneramt) Einsicht in die dort zu türkischen Staatsangehörigen geführte Kartei, um sämtliche in Dresden lebenden deutsch-türkischen Ehepaare zu ermitteln. Die Kartei wies 15 deutsch-türkische Ehen aus. Weitere Ermittlungen beim Standesamt Dresden ergaben, daß in den Jahren 1993/94 sieben deutsch-türkische Ehen geschlossen worden waren. Nur in diesen Fällen hielt das LKA einen Bezug zur organisierten Kriminalität für möglich. Das LKA prüfte diese sieben Fälle auf "OK-Bezug", konnte einen solchen aber nicht feststellen. Daraufhin gab das LKA das Verfahren ohne nähere Erläuterungen an die Polizeidirektion Dresden ab. Auch aus den Akten war der Umfang der durchgeführten Ermittlungen im einzelnen nicht

ersichtlich. Daher nahm die Polizeidirektion Dresden nach Rücksprache mit der Staatsanwaltschaft bei der Ausländerbehörde und beim Standesamt Ermittlungen vor, die auch nach Auffassung der Polizeidirektion in der überwiegenden Anzahl der Fälle keinen Anfangsverdacht für den Straftatbestand einer Scheinehe ergaben. Trotzdem lud die Polizeidirektion Dresden, nicht zuletzt aufgrund einer unklar formulierten staatsanwaltschaftlichen Verfügung, 14 Betroffene als Beschuldigte vor. Mitte März 1995 liefen noch gegen drei Einzelpersonen Verfahren. Die übrigen Verfahren hat die Staatsanwaltschaft inzwischen eingestellt. Die Polizeidirektion Dresden hat mir zugesichert, sämtliche Daten aus den eingestellten Verfahren zu löschen.

Ich habe diesen Sachverhalt datenschutzrechtlich bewertet:

- Die stark lückenhafte Aktenführung hatte zur Folge, daß die Polizeidirektion nicht klar erkennen konnte, welche Ermittlungen das LKA bereits vorgenommen hatte. Die Polizeidirektion führte deswegen teilweise die gleichen - und damit nicht erforderlichen - Ermittlungen durch wie das LKA. Des weiteren erschwerte die fehlende Dokumentation eine ordentliche polizeiinterne und externe Prüfung des Verwaltungsablaufs (z. B. durch meine Dienststelle). Der Präsident des LKA hat diesen Mißstand erkannt, gerügt und ist aufsichtsrechtlich tätig geworden. Wegen dieser einsichtigen Haltung besteht keine Veranlassung, die Aktenführung formell zu beanstanden.

- Das aus den Ausländerkarteikarten ersichtliche Datum zur Staatsangehörigkeit des Ehegatten ist in dem in der Ausländerdateienverordnung genannten und abschließenden Datensatz nicht aufgeführt. Ich werde darauf hinwirken, daß dieses Datum gelöscht wird. Allerdings handelt es sich um ein "offenes Datum", weil die Ausländerbehörde nach dem Ausländerzentralregistergesetz jederzeit automatisiert auf dieses Datum zugreifen kann. Ein gravierender Verstoß ist daher nicht festzustellen.

- Die Vernehmung sämtlicher Betroffenen als "Beschuldigter", also die Einleitung konkreter gegen diese Personen gerichteter Ermittlungsverfahren, war zumindest in elf Fällen unberechtigt, weil ein hinreichender Anfangsverdacht im Sinne der Strafprozeßordnung offenkundig nicht in bezug auf jeden Einzelnen vorlag. Hierauf weise ich die Polizeidirektion Dresden sowie die Staatsanwaltschaft hin.

- Ob die Daten aus den eingestellten Ermittlungsverfahren tatsächlich gelöscht wurden, werde ich in allen Einzelfällen überprüfen.

Fazit: Teilweise mangelhafte Ermittlungen zeigten wenig Feingefühl im Umgang mit sensiblen Daten, jedoch besteht insbesondere wegen der kooperativen und problembewußten Haltung der zuständigen Behördenleiter kein Anlaß zu einer förmlichen Beanstandung.

Den Innenausschuß des Sächsischen Landtages habe ich vom Ergebnis meiner datenschutzrechtlichen Kontrolle unterrichtet.

5.9.9 Präventionsräte

Über die Gründung eines Präventionsrates habe ich im Vorjahr berichtet (2. Tätigkeitsbericht, 5.10.7). Inzwischen werden weitere Überlegungen zu entsprechenden Organisationsstrukturen angestellt: Der "Runde Tisch gegen Gewalt" empfahl im Juni 1994, landesweit Gremien zur Verhütung von Kriminalität und Gewalt zu bilden: Ziel dieser Gremien solle es sein, die Zusammenarbeit zwischen den zuständigen Behörden und Organisationen zu verbessern. Zur Unterstützung der Gremien solle eine Geschäftsstelle beim SMI eingerichtet werden.

Da in Pirna - bereits seit längerem - ein Präventionsrat besteht, habe ich mit einigen seiner Mitglieder ein Informationsgespräch geführt. Mir wurde mitgeteilt, daß der Präventionsrat Pirna vom Landrat und der örtlichen Polizeidienststelle im November 1993 ins Leben gerufen worden sei, weil die Bevölkerung durch die Klein- und Massenkriminalität aktuell beunruhigt sei. Ehrenamtliche Mitglieder des Präventionsrates seien Vertreter des Sozialamts und des Jugendamts sowie der Kirche und der Polizei. Der Präventionsrat habe weder Eingriffsbefugnisse noch ein Interesse an personenbezogenen Daten, sondern er beschäftige sich ausschließlich mit öffentlich bekannten Problemen oder Lagebildern. Die Verfolgung oder Verhinderung einzelner Straftaten obliege allein den hierfür zuständigen Polizeibehörden. Der Präventionsrat versuche, Probleme - insbesondere bei der Jugend - aufzudecken, Lösungen hierfür anzubieten und dann an die für die Gefahrenabwehr zuständigen Stellen weiterzugeben. Ziele des Projektes seien unter anderem der Abbau "kriminogener Gelegenheitsstrukturen" sowie die Verbesserung von Kommunikation und Zusammenarbeit zwischen den Behörden.

Ergebnis des Gesprächs war, daß offenbar für die Arbeit der Präventionsräte sach- und nicht personenbezogene Fragen im Vordergrund stehen. Trotzdem gehe ich davon aus, daß bei der Verfolgung der genannten Ziele auch Belange des Datenschutzes berührt werden können. Ich werde mich deshalb auch weiterhin fortlaufend über den Stand der Entwicklung der Präventionsräte unterrichten lassen.

In diesem Zusammenhang würde ich es begrüßen, wenn die beteiligten öffentlichen Stellen auch von sich aus Kontakt mit meiner Dienststelle aufnähmen.

Nicht unerwähnt möchte ich lassen, daß dem SMI zum Zeitpunkt meiner ersten Anfrage bereits die detaillierte Projektbeschreibung des Landkreises Pirna vorlag - eine inhaltliche Antwort wurde mir mangels "näherer Informationen" jedoch nicht zuteil. Hier muß die Zusammenarbeit innerhalb des SMI verbessert werden.

5.10. Verfassungsschutz

5.10.1 Beteiligung des Sächsischen Datenschutzbeauftragten durch das Landesamt für Verfassungsschutz

Das Landesamt für Verfassungsschutz (LfV) hat sich im Berichtszeitraum offen für datenschutzrechtliche Belange gezeigt. So erhielt meine Dienststelle im Rahmen der nach § 8 Abs. 2 SächsVSG obligatorischen Anhörung vor Erlaß und vor wesentlichen Änderungen von Dateierrichtungsanordnungen stets frühzeitig Kenntnis. Meine Empfehlungen wurden dabei zum größten Teil aufgegriffen und umgesetzt. Auch ist hervorzuheben, daß sich das Landesamt im Zusammenhang mit Auskunftsersuchen nach § 9 SächsVSG mit mir mehrfach in Verbindung gesetzt hat, um dem Informationsrecht der Betroffenen möglichst weit entgegenzukommen.

Darüber hinaus wurde ich umfassend in Überlegungen des LfV eingebunden, die amtsinternen Meldewege datenschutzgerecht zu strukturieren.

5.10.2 Personeller Sabotageschutz

Im Rahmen ihrer Mitwirkungsaufgaben werden die Verfassungsschutzbehörden des Bundes und der Länder an den Sicherheitsüberprüfungen der Beschäftigten beteiligt, denen im öffentlichen Interesse geheimhaltungsbedürftige Tatsachen anvertraut werden (personeller Geheimschutz) oder die an sicherheitsempfindlichen Stellen von lebens- oder verteidigungswichtigen Einrichtungen beschäftigt sind oder werden sollen (personeller Sabotageschutz). Während für den personellen Geheimschutz durch die jüngst in Kraft getretenen Sicherheitsüberprüfungsgesetze des Bundes und der Länder - in Sachsen wird ein entsprechendes Gesetz erarbeitet - bereichsspezifische Datenverarbeitungsregelungen geschaffen wurden, existieren für den personellen Sabotageschutz lediglich im Atom- und im Luftfahrtverkehrsgesetz einschlägige Überprüfungsregelungen. Angesichts der Überlegungen des Bundesministers des Innern, nicht nur Beschäftigte im Atombereich sowie der Flughäfen, sondern auch in allerlei anderen Einrichtungen zu überprüfen, ist es notwendig, die gesetzlichen Anknüpfungskriterien "lebens- und verteidigungswichtig" (§ 3 Abs. 1 Nr. 2 BVerfSchG und § 3 Abs. 2 Nr. 2 SächsVSG) im Interesse des Persönlichkeitsrechts der Betroffenen eng auszulegen. Die Sicherheitsüberprüfungen müssen auf die Bereiche beschränkt bleiben, in denen einer erheblichen Bedrohung für das Leben zahlreicher Menschen vorgebeugt werden muß. Sollen in solchen Bereichen Sicherheitsüberprüfungen durchgeführt werden, müssen hierfür klare gesetzliche Grundlagen geschaffen werden, wie dies mit dem Atomgesetz und dem Luftverkehrsgesetz geschehen ist. So müssen die zu schützenden Arten von Einrichtungen - zumindest durch Rechtsvorschrift - abschließend festgelegt sein. Im einzelnen sind folgende Grundsätze zu beachten:

Die Sicherheitsüberprüfung darf erst erfolgen, wenn durch die zuständige Behörde die "sicherheitsempfindlichen Stellen" genau festgelegt sind. Für die Überprüfung muß die Zustimmung des Betroffenen als Verfahrensvoraussetzung vorliegen. Die im Rahmen der Überprüfung gewonnenen Daten (darunter auch Informationen über politische Anschauungen, Alkoholkonsum, sexuelle Gewohnheiten und Anfälligkeiten) müßten

einer strengen Zweckbindung unterliegen, die durch angemessene organisatorische Vorkehrungen sicherzustellen ist. Die Betroffenen müssen eigene Verfahrensrechte erhalten, wozu insbesondere das rechtliche Gehör vor einer ablehnenden Entscheidung zählt. Auch sollte ihnen ein angemessener Auskunftsanspruch sowie ein umfassendes Akteneinsichtsrecht eingeräumt werden. Schließlich sind ergänzende Regelungen zur effektiven Datenschutzkontrolle notwendig; hier ist an die Einbeziehung der Datenverarbeitung in Akten bei nicht-öffentlichen Stellen zu denken.

Alle Vorhaben, die auf eine Erweiterung der Sicherheitsüberprüfung beim vorbeugenden personellen Sabotageschutz zielen, sollten stets im Auge haben, daß sensible Daten erhoben werden, ohne daß der Betroffene dazu Anlaß geboten hätte; auch wenn die Überprüfung unbescholtener Personen nur einen bloßen - letztlich unbegründeten - Verdacht ergibt, kann dies bereits erheblichen Einfluß auf das berufliche Fortkommen nehmen.

Ferner ist zu bedenken, daß die Daten erhoben werden, bevor der Betroffene mit einer sicherheitsempfindlichen Funktion betraut wird. Ergibt die Überprüfung ein Sicherheitsrisiko, so darf dies nur dazu führen, daß der "neue Job" nicht übertragen wird; auf den "alten Job" (der ja keine Sicherheitsüberprüfung erforderte) darf das keinen - auch keinen versteckten - Einfluß haben. Ich weiß, daß hier mancher stutzt; aber das ist der Rechtsstaat!

5.11 Sonstiges

5.11.1 Stellungnahme zum Gesetz über den Sächsischen Ausländerbeauftragten

Dieses Gesetz ist am 28. Januar 1994 beschlossen worden. Entgegen § 13 Abs. 5 Satz 4 GeschoSReg hat mich die Staatsregierung am Gesetzgebungsverfahren nicht beteiligt, obwohl das Gesetz "den Umgang mit personenbezogenen Daten berührt".

Hervorzuheben ist § 5 Abs. 3 SächsAuslBeauftrG. Hiernach haben die Mitarbeiter des Ausländerbeauftragten, auch nach Beendigung ihrer Tätigkeit, über die ihnen bei ihrer Tätigkeit bekanntgewordenen Angelegenheiten Verschwiegenheit zu bewahren. Dies soll nach § 5 Abs. 3 Satz 2 SächsAuslBeauftrG allerdings nicht für Tatsachen gelten, die "ihrer Bedeutung nach keiner Geheimhaltung bedürfen". Diese Vorschrift darf *verfassungskonform* nicht als *Offenbarungsbefugnis für (belanglose) personenbezogene Daten* interpretiert werden. Das Grundrecht auf informationelle Selbstbestimmung ist nämlich *umfassend* gewährleistet. *Jedes personenbezogene Datum*, so bedeutungslos es auch erscheinen mag, ist in seinen Schutzbereich einbezogen, weil - so das Bundesverfassungsgericht - es erst der (auch spätere) Verwendungszusammenhang ist, der die Brisanz einer Information ausmacht. Es ist nur zulässig, durch gesetzliche Regelungen in dieses Grundrecht einzugreifen, wenn diese Regelungen dem Gebot der Normenklarheit sowie dem Verhältnismäßigkeitsgrundsatz entsprechen. Diesen Anforderungen genügt § 5 Abs. 3 Satz 2 SächsAuslBeauftrG nicht. Eigenständige Bedeutung hat die Vorschrift also nur für Tatsachen ohne Personenbezug.

Ich habe dem Sächsischen Ausländerbeauftragten dies erläutert. Er hat auch für seine Mitarbeiter zugesichert, *keine* bei seiner Tätigkeit bekannt gewordenen *personenbezogenen Daten* zu offenbaren, es sei denn, ein Gesetz läßt dies ausdrücklich zu.

5.11.2 Datenübermittlung durch die Landesaufnahmestelle für Aussiedler des Freistaates Sachsen an den Caritasverband

Zuständig für die Erstaufnahme und Grundversorgung der dem Land vom Bundesverwaltungsamt zugewiesenen Aussiedler ist die *Landesaufnahmestelle* für Aussiedler des Freistaates Sachsen. Nach kurzem Aufenthalt dort (in der Regel nach 10 bis 14 Tagen) teilt die Landesaufnahmestelle die Betroffenen den zuständigen *Eingliederungsbehörden* zur vorläufigen Unterbringung zu.

Der Caritasverband fragte an, ob die Landesaufnahmestelle berechtigt sei, personenbezogene Daten der Aussiedler (insbesondere das Datum "Zugehörigkeit zu einer öffentlich-rechtlichen Religiongesellschaft") zu Betreuungszwecken an ihn zu übermitteln.

Diese Frage konnte ich nicht uneingeschränkt bejahen. Das Sächsische Aussiedlereingliederungsgesetz sieht nämlich die Übermittlung von Aussiedlerdaten durch die Landesaufnahmestelle nur an Arbeitsämter, den Suchdienst des Roten Kreuzes oder den kirchlichen Suchdienst vor. Daher darf die Landesaufnahmestelle personenbezogene Daten von Aussiedlern an den Caritasverband nur mit vorheriger schriftlicher Einwilligung der Betroffenen übermitteln.

5.11.3 Straßenverkehrswesen: Automatisierter Abruf von Fahrzeug- und Halterdaten

Eine Stadtverwaltung beabsichtigte die Einrichtung eines automatisierten Verfahrens zum Abruf von Fahrzeug- und Halterdaten durch kommunale Verkehrsüberwachungsdienste. Ich habe der Stadt erklärt, warum dies nicht zulässig ist: Zwar sind Einrichtung und Betrieb automatisierter Abrufverfahren innerhalb einer öffentlichen Stelle (zum Beispiel Stadtverwaltung) nach dem Sächsischen Datenschutzgesetz unter bestimmten Voraussetzungen zulässig. Dieses Gesetz findet in diesem Falle jedoch als sogenanntes "Auffanggesetz" keine Anwendung, weil der Bundesgesetzgeber den automatisierten Abruf von Fahrzeug- und Halterdaten in § 36 Abs. 1 und 2 StVG *besonders* und *abschließend* geregelt hat (vgl. § 2 Abs. 4 SächsDSG). Hiernach dürfen diese Daten nur von den Zulassungsstellen, den Polizeien des Bundes und der Länder sowie vom Zoll aus dem zentralen Fahrzeugregister (KBA Flensburg) und von den Polizeidienststellen aus dem örtlichen Fahrzeugregister im automatisierten Verfahren abgerufen werden (Polizeidienststellen im Sinne von § 36 Abs. 2 Satz 2 StVG sind ausschließlich die Polizeivollzugsdienststellen und keine kommunalen Verkehrsüberwachungsdienste).

Das SMI, das meine Auffassung teilt, hat den nachgeordneten Bereich entsprechend unterrichtet.

Vgl. ferner Abschnitt 9.2.

6 Finanzen

6.1 Pflicht des Finanzamts zur Auskunft über Informanten

Ein Petent, der von einem Finanzamt aufgefordert worden war, die Angaben in seiner Steuererklärung zu ergänzen, vermutete hinter dem Schreiben des Finanzamts den gezielten Hinweis eines Informanten. Er bat mich um Auskunft über sein Einsichtsrecht in die eigenen Steuerakten und um Mitteilung, ob das Finanzamt ihm Namen und Anschrift des Informanten nennen müsse.

Ich habe dem Petenten erläutert, daß die dem Finanzamt vorliegende Information nicht zwingend von einem privaten Informanten stammen müsse. Vielmehr seien im Besteuerungsverfahren verschiedene Stellen den Finanzbehörden gegenüber zu Mitteilungen gesetzlich verpflichtet, (z. B. Kreditinstitute und Nachlaßgerichte in Erbschaftsangelegenheiten, Notare bei Grundstücksveräußerungen, Kfz-Zulassungsstellen in Zulassungsangelegenheiten). Außerdem würden die Finanzämter für Zwecke der Besteuerung Kontrollmitteilungen fertigen und sich untereinander die im Rahmen ihrer örtlichen oder sachlichen Zuständigkeit festgestellten Besteuerungsgrundlagen mitteilen. Auch auf die *Verordnung über Mitteilungen an die Finanzbehörden durch andere Behörden und öffentlich-rechtliche Rundfunkanstalten*, nach der sich ab dem 1. Januar 1994 zusätzliche Mitteilungspflichten für Behörden ergeben haben (z. B. über Zahlungen für Lieferungen und Leistungen, die nicht erkennbar im Rahmen einer gewerblichen, land- und forstwirtschaftlichen oder freiberuflichen Tätigkeit erbracht werden), habe ich den Petenten hingewiesen. Möglicherweise konnte sich der Petent bereits aufgrund dieser Erläuterungen erklären, auf welchem Weg das Finanzamt Kenntnis steuerlicher Tatbestände erhalten hatte.

Die AO enthält keine spezielle Vorschrift über Form, Art und Inhalt von Auskünften an den Steuerpflichtigen oder über sein Akteneinsichtsrecht. Lediglich die Mitteilung von Besteuerungsgrundlagen ist in § 364 AO zwingend vorgeschrieben. Allerdings können die Finanzbehörden nach dem Anwendungserlaß (AEAO) zu § 364 AO Akteneinsicht gewähren, wobei sie sicherzustellen haben, daß *die Verhältnisse eines anderen* nicht unbefugt offenbart werden - also das Steuergeheimnis nicht verletzt wird (§ 30 AO).

Vor 1977 sprach § 30 AO von den Verhältnissen eines "Steuerpflichtigen"; damals gehörten zu den Verhältnissen also nur Angaben über solche Umstände, die das Besteuerungsverfahren eines Einzelnen (z. B. eines Anzeigenerstatters) beeinflussen konnten. Seit 1977 spricht § 30 AO von den Verhältnissen eines "anderen", also von allen personenbezogenen Daten, somit auch etwa denen eines Anzeigenerstatters. Zum geschützten Personenkreis des § 30 AO gehören nicht nur die Steuerpflichtigen sondern alle Personen, deren Daten einem Amtsträger der Steuerverwaltung bekannt werden. Falls Informanten per se Gefahr liefen, daß ihre Namen grundsätzlich weitergegeben würden, würde nicht nur eine wesentliche Erkenntnisquelle der Steuerverwaltung verstopft, vielmehr würde auch ihr Persönlichkeitsrecht tangiert.

Anders sieht es aber im (Steuer-)Strafverfahren aus: Wenn der Anzeigenerstatter vorsätzlich (d. h. auch: besonders leichtfertig) falsche Angaben gemacht hat, ist die Offenbarung seines Namens und seines Verhaltens zulässig. Denn der Angezeigte muß

die Möglichkeit haben, sich gegen ungerechtfertigte Angriffe auf seine Ehre und sein Vermögen zu wehren. Auch das Grundrecht auf rechtliches Gehör in einem fairen Verfahren (Rechtsstaatsprinzip des Art. 20 Abs. 2 GG sowie Art. 103 Abs. 1 GG, wozu auch die vollständige Akteneinsicht gehört) gebietet die Waffengleichheit und gleiche Erkenntnisquellen (siehe zum gesamten Fragenkomplex auch das Urteil des BFH vom 8. Februar 1994, Az. VII R 88/92).

Wer dem Finanzamt eine Anzeige erstattet, sollte wissen, daß seine Daten immer dann ungeschützt sind, wenn sich herausstellt, daß er allzu sorglos mit der Wahrheit umgegangen ist.

6.2 Bearbeitung der Steuerangelegenheiten von Amtsangehörigen der Finanzämter durch ein Nachbarfinanzamt

Nach § 23 Abs. 1 Nr. 4 der Geschäftsordnung für die Finanzämter hat der Vorsteher eines Finanzamts die steuerlichen Angelegenheiten von Amtsangehörigen zu zeichnen, um gegenseitigen Begünstigungen und Steuerhinterziehungen durch Amtsangehörige zu begegnen. Gegen diese an sich begrüßenswerte Regelung bestehen insoweit datenschutzrechtliche Bedenken, als der Dienstvorgesetzte auf diese Weise Einblick in die Einkommens- und Vermögensverhältnisse seiner Mitarbeiter erhält (siehe auch 2. Tätigkeitsbericht, Nr. 6.2).

Auf meine Anregung hat das SMF nunmehr verfügt, daß Mitarbeiter, deren Beschäftigungs-Finanzamt gleichzeitig das für ihre steuerlichen Angelegenheiten zuständige Finanzamt ist, die Besteuerung durch ein anderes Finanzamt beantragen können. Ein solcher Antrag braucht nicht begründet zu werden. Den Anträgen haben die Finanzämter auf der Grundlage von § 27 AO durch Abschluß einer Zuständigkeitsvereinbarung mit einem Nachbar-Finanzamt oder - in Städten mit mehreren Finanzämtern - einem anderen Finanzamt innerhalb der Wohnsitzgemeinde zu entsprechen.

Ich begrüße die seitens des SMF getroffene Regelung.

6.3 Eintragung von Pauschbeträgen für Behinderte auf Lohnsteuerkarten

Mit der erstmaligen Eintragung eines Behinderten-Pauschbetrages auf der Lohnsteuerkarte übersenden die Finanzämter stets eine entsprechende Mitteilung an die Meldebehörde der Wohnsitzgemeinde, damit diese den Pauschbetrag bei der Ausstellung künftiger Lohnsteuerkarten von Amts wegen berücksichtigen kann.

Dieses an sich bürgerfreundliche Verfahren, das nur eine einmalige Antragstellung erfordert, ist jedoch aus datenschutzrechtlicher Sicht nicht unproblematisch. Denn insbesondere bei kleineren Gemeinden oder einem Arbeitgeberwechsel wünscht der Betroffene oftmals nicht, daß der Gemeindeverwaltung bzw. dem neuen Arbeitgeber Daten seiner Behinderung oder - bei Übertragung des Pauschbetrages - Daten des

behinderten Ehegatten oder behinderter Kinder bekannt werden. Ich könnte mir vorstellen, daß es die Betroffenen in solchen Fällen vorziehen, jährlich erneut einen Antrag auf Lohnsteuer-Ermäßigung zu stellen, um die Eintragung stets vom Finanzamt vornehmen zu lassen, oder ganz auf einen Freibetrag auf der Lohnsteuerkarte zu verzichten.

Deshalb haben die Datenschutzbeauftragten des Bundes und der Länder die bisherige Praxis kritisiert und gefordert, den Behinderten das Recht einzuräumen, der Datenübermittlung an die Gemeinde zu widersprechen. Auch wenn nach § 39 a Abs. 2 Satz 1 EStG die Gemeinden *nach Anweisung der Finanzämter* die Pauschbeträge für Behinderte auf den Lohnsteuerkarten einzutragen haben und die Finanzämter dazu nach Abschnitt 108 Abs. 11 der Lohnsteuerrichtlinien die betreffenden Arbeitnehmer und die erforderlichen Merkmale mitteilen, schließt dies nicht aus, daß die Finanzämter auf Wunsch der Betroffenen von einer Mitteilung an die Wohnsitzgemeinde absehen können. Eine Gesetzesänderung wäre dazu nicht erforderlich.

Ich habe zu dieser Frage Stellungnahmen des SMF und SMS eingeholt. Das SMS teilt meine Bedenken grundsätzlich. Das SMF vertritt jedoch übereinstimmend mit den anderen obersten Finanzbehörden des Bundes und der Länder die Auffassung, daß § 39 a Abs. 2 EStG ein Wahlrecht für den Behinderten ausschließt. Zudem wird befürchtet, in einer Vielzahl von Fällen könnte unbegründet widersprochen weden, was zu einer Beeinträchtigung des bisher bewährten Eintragungsverfahren führen würde.

Um für den Antragsteller die Datenübermittlung zwischen Finanzamt und Wohnsitzgemeinde transparent zu machen, enthalten ab 1995 die bundeseinheitlichen Antragsvordrucke jedoch folgenden Hinweis:

> "Mir ist bekannt, daß erforderlichenfalls Angaben über Kindschaftsverhältnisse und Pauschbeträge für Behinderte der für die Ausstellung von Lohnsteuerkarten zuständigen Gemeinde mitgeteilt werden."

Gelöst ist das Problem damit noch nicht.

6.4 Eintragung der Konfessionszugehörigkeit des Ehegatten auf der Lohnsteuerkarte

Die Religionszugehörigkeit gehört ihrem Wesen nach zu den besonders privaten Daten. Seit Jahren sind deshalb die Datenschutzbeauftragten des Bundes und der Länder dafür eingetreten, daß die Kirchensteuermerkmale nur dann auf der Lohnsteuerkarte eingetragen werden, wenn der Arbeitgeber diese Angabe für den Lohnsteuertabzug wirklich benötigt. Nunmehr konnte - erstmals für die Lohnsteuerkarten 1995 - erreicht werden, daß die Konfessionszugehörigkeit beider Ehegatten von der ausstellenden Gemeinde nur noch dann auf der Lohnsteuerkarte angegeben wird, wenn sie unterschiedlichen Konfessionen angehören. Denn nur in diesen Fällen wird die Eintragung auch erforderlich sein, weil die einbehaltene Kirchensteuer je zur Hälfte an die Kirche des Arbeitnehmers und die Kirche seines Ehegatten abzuführen ist (Halbteilung der Kirchensteuer). Ist der Ehegatte konfessionslos, glaubensverschieden (Angehöriger einer zur Erhebung von Kirchensteuer nicht berechtigten Kirche) oder derselben Konfession zugehörig, so ist die

Kirchenlohnsteuer nur an die Kirche des Arbeitnehmers abzuführen, womit sich eine Eintragung für den Ehegatten erübrigt.

6.5 Automatisierte Datenübermittlung der Vermessungsämter an die Finanzbehörden

Das SMF informierte mich über die beabsichtigte automatisierte Datenübermittlung der Vermessungsämter an das Landesamt für Finanzen. Die Datenübermittlungen sollen jeweils zum 1. Januar eines Jahres für Zwecke des steuerlichen Bewertungsverfahrens für den Grundbesitz erfolgen. Es legte mir den Entwurf einer entsprechenden Vereinbarung mit dem SMI vor. Der Umfang der zu übermittelnden Daten, den ich anhand der Datensatzbeschreibungen geprüft habe, sowie die zur Gewährleistung der Datensicherheit getroffenen Vorkehrungen waren nicht zu beanstanden. Der regelmäßigen Datenübermittlung steht nach meiner Auffassung auch der Wortlaut des § 29 Abs. 3 BewG nicht entgegen, wonach die nach Bundes- oder Landesrecht zuständigen Behörden den Finanzämtern alle rechtlichen und tatsächlichen Umstände mitzuteilen haben, die für die Feststellung der Einheitswerte des Grundbesitzes von Bedeutung sein können.

7 Kultus

7.1 Schule

7.1.1 Novellierung der "Schulformularverwaltungsvorschrift" vom 9. März 1992, speziell "2.2. Schülerkartei"

Bei der Klärung von Anfragen von Schulleitern und von Erziehungsberechtigten bin ich auf folgendes Problem gestoßen:
Zur Anmeldung von Schülern in den Schulen nach
-§ 3 Abs. 4 der Schulordnung Grundschulen (SOGS)
-§ 3 Abs. 4 Schulordnung Mittelschulen (SOMI)
-§ 3 Abs. 6 Schulordnung Gymnasien (SOGY)
-§ 9 Abs. 4 Schulordnung Berufsschulen (BSO)
-§ 5 Abs. 3 Schulordnung beruflicher Gymnasien (BGySO)
werden sowohl Daten erhoben, die in entsprechenden Feldern der Schülerkartei (gem. 2.2. Schulformularverwaltungsvorschrift) gespeichert werden können, als auch solche, die nicht auf der Schülerkartei vorgesehen sind. Unterschiedliche Begriffe führen dabei zu Irritationen, wie mit diesen Daten umzugehen ist.

Beispielsweise fällt auf:
1. Nach der Schulformularverwaltungsvorschrift ist auf der Schülerkartei das Datum "Bekenntnis" vorgesehen. In den Schulordnungen wird der Begriff "Religionszugehörigkeit" benutzt.
2. Während alle Schulordnungen das Geschlecht des Schülers erheben, ist dafür auf der Schülerkartei kein Platz vorgesehen.
3. Auch für die Notfalladresse im Zusammenhang mit der Telefonnummer (entsprechend den meisten Schulordnungen) gibt es in der Schülerkartei keinen Platz.
4. Zum Speichern der Angabe von Art und Grad einer Behinderung, chronischen Erkrankungen - ein schützenswertes personenbezogenes Datum, das nur mit Einwilligung der Erziehungsberechtigten erfaßt wird - ist auf der Schülerkartei kein Platz vorgesehen. Es ist unklar, wo dieses sensible Datum gespeichert werden soll.
5. Datenschutzrechtlich bedenklich ist überdies das Feld "Bemerkungen", welches Freiräume schafft für unzulässige schülerbezogene Notizen. Wenn Schülerkarteikarten in Gebrauch sind (und von Verlagen angeboten werden), die auch die gesamte Rückseite für "freie Eintragungen" vorsehen, so ist das aus meiner Sicht nicht akzeptabel. Sofern nicht gänzlich auf dieses Formularfeld verzichtet wird - was ich dringend empfehle -, so wäre doch zumindest ein restriktiver Hinweis angebracht, welche Eintragungen in dieses Feld vorgenommen werden dürfen und welche zu unterlassen sind.

Nach § 17 des Sächsischen Datenschutzgesetzes stehen den betroffenen Erziehungsberechtigten und Schülern umfangreiche Rechte auf Auskunft zu. Eine entsprechende Gestaltung der Schülerkartei sollte diese Auskunftserteilung unterstützen. In diesem Zusammenhang habe ich einen Zusatzvermerk auf der Karte angeregt, in den die Empfänger von Datenübermittlungen aus der Schülerkartei aufzunehmen sind. Solche Angaben würden einen transparenten Umgang der Schule mit den Daten auf der Schülerkartei für die betroffenen Erziehungsberechtigten und Schüler unterstützen.

Die jetzige unklare Verfahrensweise kann dazu führen, daß diese Transparenz der Datenhaltung und -verarbeitung für die betroffenen Eltern und Schüler nach und nach verloren geht. All das führt letztlich zu datenschutzrechtlich bedenklichem, aber auch vermeidbarem Verwaltungsaufwand. Daher habe ich dem SMK vorgeschlagen, die Schulformularverwaltungsvorschrift bezüglich der Schülerkartei zu überarbeiten. Meine Bereitschaft, an der datenschutzgerechten Gestaltung mitzuwirken, habe ich erklärt.

7.1.2 Anmeldeformular für die Mittelschule

Mit einer Eingabe wandte sich ein Vater an mich, dessen Sohn schon seit zwei Jahren die Mittelschule besucht. Er sei verwundert, daß er für seinen Sohn erneut ein Anmeldeformular ausfüllen müsse. Er bat um datenschutzrechtliche Prüfung des Formulars, welches ihm die Schule zugesandt hatte.

Meine Recherchen führten zu folgendem Ergebnis: Nach der Schulordnung Mittelschulen (SOMI), die seit 10. September 1993 in Kraft ist, werden bei der Anmeldung der Schüler Daten gemäß § 3 Abs. 4 SOMI erhoben. Diese Angaben gehen über das hinaus, was die betreffende Mittelschule bisher über den Schüler in der Schülerkartei gespeichert hatte. Solche zusätzlichen Angaben waren z. B. die Telefonnummer, Notfalladresse, Art und Grad einer Behinderung und chronische Krankheiten (die beiden letzten Angaben werden nur mit Einwilligung des Erziehungsberechtigten erfaßt).

Um diese Daten zu erheben, entwickelte der Schulleiter ein Formular, das den Schülern übergeben wurde. Das Formular enthielt Datenschutzmängel. Es wurden Daten erhoben, die über das hinausgingen, was die SOMI vorschreibt. Während nach der Schulordnung nur die Angabe "Telefonnummer, Notfalladresse" anzugeben war, wurden auf dem Schulformular die Angabe der privaten Telefonnummer, auch der dienstlichen Telefonnummer von Vater und Mutter (nicht der Erziehungsberechtigten) verlangt. Aus der Nichtangabe eines dienstlichen Telefons kann möglicherweise auf Arbeitlosigkeit geschlossen werden. Die Erfassung eines derartigen Datums in einem Schulformular kann nicht zugelassen werden.

Zu unterschreiben war das Formular von Vater und Mutter, nicht von den Erziehungsberechtigten. Diese Anforderung ist ungenau, weil vielfach "Vater und Mutter" nicht die Erziehungsberechtigten sind.

Der spezielle Zweck dieser Erhebung war außerdem nicht die Anmeldung, sondern die Aktualisierung vorhandener Unterlagen. Dieser Zweck war auf dem Formular nicht vermerkt; die Rechtsgrundlage fehlte.

Die Einwilligung zur Angabe der Behinderung und chronischer Krankheiten des Schüler war nicht deutlich hervorgehoben formuliert, der Zweck (Beachtung bei erster Hilfe, beim Sportunterricht, Eingehen auf gesundheitliche Probleme) nicht erwähnt.

Aufgrund meiner datenschutzrechtlichen Hinweise hat der Schulleiter drei neue Formulare entwickelt:

1. Formular für die Nacherfassung bisher nicht erhobener Daten (für Schüler, die vor dem Inkrafttreten der SOMI in der Schule angemeldet worden waren und für die noch Daten gemäß der neuen Schulordnung fehlen)
2. Formular für eine Neuanmeldung gemäß § 3 Abs. 4 der SOMI
3. Formular zur Anzeige von Veränderungen in den Schülerunterlagen gegenüber der ursprünglichen Anmeldung (z. B. Änderung von Telefonnummer, Notfalladresse).

Diese neuen Formulare entsprachen datenschutzrechtlichen Anforderungen. Der Schulleiter zog sofort das ursprüngliche Formular ein. Bereits ausgegebene Formulare - so wurden die Eltern informiert - brauchten von den Eltern nicht mehr ausgefüllt zu werden. Bereits eingesammelte Formulare wurden an die Erziehungsberechtigten zurückgegeben. Künftig wird in der Schule nur noch mit den neuentwickelten Formularen gearbeitet.

An das SMK habe ich ein Muster dieser nun datenschutzgerechten Formulare geschickt, mit dem Hinweis, daß möglicherweise auch andere Schulen an einem solchen Formular Interesse haben. Das SMK teilte mir daraufhin mit, daß die Formulare von den Schulen selbst erstellt werden. Es war nicht bereit, meine Anregung zur Unterstützung der Schulleiter bei dieser datenschutzgerechten Erhebung von Schülerdaten aufzugreifen.

7.1.3 Unfallanzeige für Kinder, Schüler, Studierende

Bundesweit wird immer noch für die Anzeige von Unfällen in Bildungseinrichtungen eine spezielle Unfallanzeige nach der allgemeinen Verwaltungsvorschrift über die Neufassung des Musters für Unfallanzeigen vom 31.7.1973, gemäß § 1555 RVO erlassen vom Bundesminister für Arbeit und Sozialordnung, benutzt. In diesem Formularfossil aus der Vorzeit des Datenschutzes ist nicht einmal die Rechtsgrundlage für die Erhebung der Daten angegeben.

Die Anzeige muß der Leiter der Bildungseinrichtung oder dessen Beauftragter erstatten, wenn ein Kind, Schüler oder Studierender im Zusammenhang mit dem Besuch eines Kindergartens, einer Schule oder einer Hochschule einen Unfall erleidet. Die Anzeige ist innerhalb von drei Tagen nach Bekanntwerden des Unfalls an den Sächsischen Gemeindeunfallversicherungsverband zu richten.

Aus Eingaben und auf Schulungsveranstaltungen für Lehrer erfuhr ich, daß in einigen Schulen für den Fall eines Unfalls "vorsorglich", z. B. bei der Anmeldung des Kindes, die Krankenkasse, teilweise mit ergänzenden Daten, (ob pflicht-, freiwillig, familien- oder privatversichert) erhoben und gespeichert wird, um das entsprechende Feld der Anzeige im Falle eines Unfalls ausfüllen zu können.

Diese Praxis in Schulen ist nicht nur rechtswidrig, sondern auch sinnlos.

Wenn das Datum "Krankenkasse" z. B. bei der Anmeldung für eine Grund-/Mittelschule oder ein Gymnasium erhoben wird, so wird damit gegen die entsprechende Schulordnung verstoßen (§ 3 Abs. 4 SOGS bzw. § 3 Abs. 4 SOMI oder § 3 Abs. 6 SOGY). Diese Schulordnungen enthalten einen abschließenden Katalog der zulässigen Daten, die bei der Anmeldung erhoben werden. Die Angabe der Krankenkasse ist nicht vorgesehen.

Zuweilen wird dieses Datum auch auf "freiwilliger Basis" erhoben und so mit Einverständnis der Befragten eine unzulässige Umgehung der Schulordnung versucht.

Hinzu kommt noch, daß die Erziehungsberechtigten die Krankenkassen auch wechseln - was in Zukunft zunehmen wird - und dann meist vergessen, eine entsprechende Änderung der Schule mitzuteilen. Demzufolge kann der Schulleiter, der solche Daten sammelt, gar nicht sicher sein, daß seine Daten aktuell sind.

Daher erfragen häufig Rettungsdienste nicht die Krankenkasse von den Schulen, weil sie wissen, daß dieses Datum - sofern es nicht direkt bei den Erziehungsberechtigten erfaßt wird - häufig fehlerhaft ist und eine Nacherfassung doppelte Arbeit bereitet.

Allenfalls ist zu überlegen, ob aufgrund der besonderen Situation der Schüler bei einer Heimunterbringung die Erhebung des Datums "Krankenkasse" zulässig ist.

7.1.4 Erstellung von Familienstammbäumen durch Schüler

Gegen die Erstellung von Familienstammbäumen durch Schüler bestehen datenschutzrechtliche Bedenken.

Zu begrüßen ist, daß sich die Schüler mit der Familiengeschichte befassen. Andererseits besteht jedoch die Gefahr, daß sensible personenbezogene Daten bekannt werden, beispielsweise Unehelichkeit des Kindes oder Scheidung der Eltern. Dies kann die zarten Gemüter der Kinder, besonders unter dem Druck des Klassenverbandes, stark belasten.

Daher bin ich mit dem SMK übereingekommen, in Zukunft in den Klassen nur noch einen Musterstammbaum zu erstellen, also einen Stammbaum, der keine Angaben zu tatsächlichen Personen enthält. Dieser Musterstammbaum kann mit den Daten von einer oder zweier Familien ausgefüllt werden, wenn die Erziehungsberechtigten eingewilligt haben. Man kann aber auch einen lustigen erfundenen Stammbaum erarbeiten.

Ähnlich gelagerte Probleme ergeben sich, insbesondere in den Grundschulklassen, in denen stark umfeld- und familienbezogene Unterrichtsthemen, etwa im Heimatkundeunterricht, besprochen werden. Gemäß Lehrplan "Grundschule; Heimatkunde/Sachkunde" soll beispielsweise in Klasse 1, Lernbereich 1, das Leben in der Familie vorgestellt werden. In der Klasse wird über Arbeit und Beruf der Eltern gesprochen. Ich verkenne nicht, daß diese Vorgaben ein wesentlicher Bestandteil des Ziels sind, dem Kind, wie es im Lehrplan heißt, "Hilfe bei der Erschließung seiner Lebensumwelt" zu geben. Jedoch läßt sich ein Spannungsverhältnis zum ebenfalls berechtigten Anliegen des Schutzes des Rechts auf informationelle Selbstbestimmung und der Privatsphäre von Eltern und Kindern nicht leugnen.

Hier einen Ausgleich zu finden, muß Ziel der Lehrplangestaltung und der Fortbildung sein. Besonders das Feingefühl unserer Lehrer ist hier gefragt.

7.2 Datenschutz im kirchlichen Bereich

Im Berichtszeitraum war ich im wesentlichen mit zwei Vorgängen aus dem Bereich der Kirchen befaßt:

Zum einen trat das SMK mit der Bitte an mich heran, mein Einvernehmen gemäß § 14 Satz 2 SächsDSG mit der Feststellung "*ausreichende Datenschutzregelungen*" im Bereich des Bistums Dresden-Meißen zu erklären. In diesem Jurisdiktionsbezirk galt seit dem 1. Januar 1994 die neugefaßte "Anordnung über den kirchlichen Datenschutz - KDO" und mit Wirkung vom 1. Juli 1994 die "Verordnung zur Durchführung der Anordnung über den kirchlichen Datenschutz (KDO-DVO)". Beide Regelungen entsprechen weitgehend den Standards des Bundesdatenschutzgesetzes von 1990; auf meine entsprechenden Ausführungen in meinem 2. Tätigkeitsbericht unter 7.2 verweise ich. Ich hatte daher keine Bedenken, mein Einvernehmen gemäß § 14 SächsDSG zu erklären.

Das SMK hat mich ferner davon in Kenntnis gesetzt, daß das Katholische Büro Sachsen für die beiden katholischen Jurisdiktionsbezirke eine Feststellung gemäß § 30 Abs. 3 SächsMG beantragt habe. § 30 Abs. 3 SächsMG erlaubt Datenübermittlungen von den Meldebehörden an öffentlich-rechtliche Religionsgesellschaften, wenn sichergestellt ist, daß bei dem Empfänger *ausreichende Datenschutzmaßnahmen getroffen* sind. Da der Wortlaut dieser Vorschrift im Gegensatz zu dem allgemeiner gehaltenen § 14 SächsDSG eine konkrete Prüfung der Datenschutzpraxis der Kirchen nahezulegen schien, bat mich das SMK um eine Abstimmung des zur Feststellung erforderlichen Verfahrens. Das SMK bezog sich dabei auf meine Ausführungen im 2. Tätigkeitsbericht, wonach eine Einzelfallkontrolle innerkirchlicher Vorgänge staatlichen Behörden, also auch mir, nicht zusteht.

Dem SMK habe ich daraufhin im Hinblick auf § 30 Abs. 3 SächsMG folgendes mitgeteilt: Die genannte Vorschrift ist wortgleich mit § 19 Abs. 3 MRRG. "Ausreichende Datenschutzmaßnahmen" sind dann "getroffen", wenn die jeweilige Religionsgesellschaft in ihren (innerkirchlichen) Bereichen die rechtlichen und tatsächlichen Voraussetzungen für einen angemessenen Datenschutz trifft, insbesondere also Regelungen über die Verwendung der Daten erläßt sowie technische und organisatorische Maßnahmen zur Ausführung dieser Regelungen trifft und schließlich eine rechtswirksame - innerkirchliche - Datenschutzkontrolle sichergestellt ist. Der Bundesgesetzgeber ist nach der Begründung des Regierungsentwurfs zu § 19 MRRG davon ausgegangen, daß diese Vorschriften bei den beiden großen Amtskirchen durch die bestehenden Datenschutzvorschriften schon weitgehend verwirklicht sind. Ich habe festgestellt, daß in beiden Jurisdiktionsbezirken mit Wirkung vom 1. Januar 1994 datenschutzrechtliche Regelungen, nämlich die beiden oben genannten Anordnungen, gelten, die in ihren Standards zwar nicht in jeder Beziehung dem 1990 neugefaßten Bundesdatenschutzgesetz entsprechen, gleichwohl jedoch die Anforderungen an einen effektiven und verfahrensmäßig gesicherten Schutz des Rechts auf informationelle Selbstbestimmung keinesfalls unterschreiten. So schreibt z. B. § 16 KDO die Bestellung eines unabhängigen Datenschutzbeauftragten und § 4 KDO in Verbindung mit Abschnitt II. KDO-DVO die schriftliche Verpflichtung der bei der Datenverarbeitung tätigen Personen auf das Datengeheimnis vor. Die Rechte der Kirchenmitglieder auf Auskunft, Berichtigung oder Löschung ihrer personenbezogenen Daten sind in §§ 13, 14 KDO gesichert. Die Verbindlichkeit dieser Regelungen für alle in

§ 1 Abs. 2 KDO genannten Stellen ab dem 1. Januar 1994 ergibt sich aus der Jurisdiktionsgewalt des Bischofs, wie sie in der Schlußzeichnung der Anordnung zum Ausdruck kommt (§ 20 KDO). Die in der KDO vorgesehenen konkreten technisch-organisatorischen Maßnahmen (§ 6 KDO in Verbindung mit Abschnitt III. KDO-DVO) stimmen wörtlich mit § 9 Abs. 1 SächsDSG überein. Aus meinen Gesprächen mit den Datenschutzbeauftragten beider Bistümer sowie aus meinem mit diesen Stellen geführten Schriftwechsel habe ich zudem den Eindruck gewonnen, daß die von der KDO und der KDO-DVO vorgeschriebenen Datenschutzmaßnahmen in die Praxis umgesetzt werden.

Das SMK hat daraufhin sowohl die vom Bistum Dresden-Meißen beantragte Feststellung gemäß § 14 SächsDSG als auch die vom Katholischen Büro Sachsen für beide Jurisdiktionsbezirke beantragte Feststellung gemäß § 30 Abs. 3 SächsMG getroffen und im Amtsblatt des SMK veröffentlicht (Amtsblatt des SMK Nr. 1 vom 20. Januar 1995).

8 Justiz

8.1 Entwurf eines Strafverfahrensänderungsgesetzes

Mit dem vom Bundesrat eingebrachten Entwurf eines Strafverfahrensänderungsgesetzes sollen für die Datenverarbeitung im Strafverfahren - längst überfällige - bereichsspezifische Regelung geschaffen werden; das Recht auf informationelle Selbstbestimmung soll mit den Erfordernissen einer funktionstüchtigen Strafrechtspflege in Einklang gebracht werden.

Zum Entwurf, der mir frühzeitig vom SMJus zugeleitet wurde, habe ich eingehend Stellung genommen. Zentraler Punkt meiner Kritik war, daß der Entwurf den Strafverfolgungsbehörden weite, nicht normenklar umrissene Handlungsspielräume eröffnet und damit den vom Bundesverfassungsgericht im Volkszählungsurteil aufgestellten Maßstäben für Eingriffe in das Recht auf informationelle Selbstbestimmung nicht gerecht wird. Zahlreiche Generalklauseln stellen das Grundrecht auf informationelle Selbstbestimmung hinter die Erfordernisse der behördlichen Aufgabenerfüllung zurück. Eine konkrete, auf den Einzelfall bezogene Interessenabwägung wird nicht vorgenommen. Der Entwurf bedarf insoweit dringend einer Überarbeitung. Im weiteren Verlauf des Gesetzgebungsverfahrens werde ich mich deshalb weiterhin darum bemühen, daß die Verarbeitung personenbezogener Daten im Strafverfahren nur unter konkreten gesetzlichen Vorgaben zulässig ist und daß in jedem Einzelfall die schutzwürdigen Interessen des Betroffenen zu berücksichtigen sind.

So sollte beispielsweise die Akteneinsicht für nicht am Strafverfahren beteiligte Dritte nur ausnahmsweise dann gewährt werden, wenn eine bloße Auskunft aus der Akte zur Aufgabenerfüllung oder zur Wahrnehmung der berechtigten Interessen nicht ausreicht und das Interesse des Betroffenen an der Geheimhaltung das Interesse an der Akteneinsicht nicht überwiegt. Letzteres wird z. B. grundsätzlich dann der Fall sein, wenn die Akten Informationen aus Telefonüberwachungsmaßnahmen nach §§ 100 a, 100 c und 110 StPO enthalten. Um einen Mißbrauch der durch Akteneinsicht erlangten sensiblen Daten zu verhindern, sollte es ferner unter Strafe gestellt werden, Informationen einer gesetzlichen Zweckbindungsregelung zuwider zu verwenden.

Bislang berücksichtigt der Entwurf lediglich *eine* datenschutzrechtliche Empfehlung: So dürfen nach § 476 Abs. 5 StPO des jetzigen Entwurfs personenbezogene Daten aus Strafverfahren nicht schon dann veröffentlicht werden, wenn dies für die Darstellung von Forschungsergebnissen über Ereignisse der Zeitgeschichte unerläßlich ist. Hinzukommen muß vielmehr - entsprechend meiner Anregung -, daß überwiegende schutzwürdige Interessen des Betroffenen nicht entgegenstehen.

Inzwischen hat die Bundesregierung angekündigt, alsbald einen eigenen Entwurf vorzulegen; ich kann nur hoffen, daß dort hinreichend bestimmte Regelungen zugunsten des Grundrechts auf Schutz der Privatsphäre formuliert werden.

8.2 Geschäftsstellenautomation bei der Staatsanwaltschaft

Schon in meinem 1. und 2. Tätigkeitsbericht habe ich über das automatisierte Aktenverwaltungssystem SIJUS-Straf berichtet.

Datenschutzrechtlich bedenklich an diesem System war hauptsächlich die fehlende Löschkomponente. Da die Datenspeicherung in der zentralen Namenskartei von SIJUS-Straf allein dem Auffinden der Akten dient, müssen diese Daten gelöscht werden, sobald die dazugehörenden Akten nach den Aufbewahrungsbestimmungen auszusondern sind. Um dies sicherstellen zu können, habe ich dem SMJus vorgeschlagen, in SIJUS-Straf eine automatische Löschkomponente einzurichten.

Das SMJus teilte mir zwischenzeitlich mit, daß in einem ersten Schritt die Programme für die Datensperre und die manuelle Löschung einzelner Datensätze realisiert wurden. Für die automatische Datenlöschung sei das Feinkonzept bereits in Auftrag gegeben worden. Mit der Fertigstellung der automatischen Löschkomponente sei im Laufe des Jahres 1995 zu rechnen.

8.3 Verwendung von Einwilligungsformularen durch Strafverfolgungsbehörden

Veranlaßt durch die Praxis von Strafverfolgungsbehörden anderer Bundesländer, Einwilligungen von Beschuldigten, Zeugen und sonstigen Personen einzuholen, um sich bei anderen Stellen (Arbeitgeber, Sozialleistungsträger, Banken etc.) Auskünfte erteilen zu lassen, habe ich das SMJus und das SMI um Stellungnahme gebeten.

Aus datenschutzrechtlicher Sicht ist eine Einwilligung im Rahmen eines Ermittlungsverfahrens generell bedenklich. Auch wenn es dem Beschuldigten formal freisteht, eine Einwilligung zu erteilen, liegt es nahe, daß er seine Einwilligung oft nur deshalb geben wird, weil er befürchtet, sich bei einer Verweigerung der Einwilligung (erst recht) verdächtig zu machen. Eine formularmäßige Einwilligung ist im übrigen auch nicht erforderlich: Die Staatsanwaltschaft oder die Polizei haben grundsätzlich nach § 161 StPO, § 67 ff. SGB X, § 30 Abs. 4 AO die Möglichkeit, auch ohne Einwilligung des Beschuldigten die für die Ermittlungstätigkeit erforderlichen Daten von anderen Behörden zu erhalten. Selbst wenn die Staatsanwaltschaft oder die Polizei im Einzelfall eine für die Ermittlungstätigkeit erforderliche Information nicht erhielte, rechtfertigte dies nicht die Einführung einer formularmäßigen Einwilligung. In einem solchen (seltenen) Einzelfall könnte die Strafverfolgungsbehörde die Einwilligung des Beschuldigten auch ohne Formblatt einholen. Ein Formblatt birgt stets die Gefahr, eine Einwilligung ohne einzelfallbezogene Erforderlichkeitsprüfung einzuholen und unnütze Daten zu sammeln.

SMJus und SMI teilten mir auf meine Nachfrage mit, daß in Sachsen solche Formulare nicht eingesetzt würden und daß dies - aufgrund der vorgenannten Erwägungen - auch nicht geplant sei.

8.4 Mitteilung der Staatsanwaltschaften und Gerichte über den Ausgang eines Strafverfahrens

Nach § 43 Abs. 2 SächsPolG sind bei der Polizei zum Zweck der Strafverfolgung gespeicherte personenbezogene Daten zu löschen, wenn der der Speicherung zugrunde liegende Verdacht entfällt. Eine ähnliche Regelung treffen die "Richtlinien des SMI für die Führung kriminalpolizeilicher personenbezogener Sammlungen in den Polizeidienststellen des Freistaates Sachsen" vom 15. Juli 1993. Demgemäß sind polizeiliche Unterlagen auszusondern, wenn eine der Polizei bekannte Entscheidung der Staatsanwaltschaft oder eines Gerichts ergibt, daß die Gründe, die zur Aufnahme in eine kriminalpolizeiliche Sammlung geführt haben, nicht zutreffen.

So müssen polizeiliche Unterlagen nach diesen Vorschriften ausgesondert werden, wenn ein rechtskräftiger Freispruch vorliegt oder der ursprüngliche Tatverdacht weggefallen ist. Auch Verfahrenseinstellungen nach § 170 Abs. 2 StPO können zur Aussonderung der Unterlagen führen, es sei denn, die Polizei ist der Ansicht, daß trotz der Einstellung überwiegende Gründe dafür sprechen, daß die betreffende Person eine Straftat begangen hat.

Um den Polizeidienststellen zu ermöglichen, die Zulässigkeit der weiteren Speicherung zu prüfen, haben die Staatsanwaltschaften oder die Gerichte die Möglichkeit, auf der Rückseite des Erfassungsbogens des polizeilichen Informationssystems PASS den Verfahrensausgang der sachbearbeitenden Polizeidienststelle mitzuteilen. Leider mußte ich feststellen, daß dieser Vordruck nicht durchgängig ausgefüllt wurde. Da die Polizeidienststellen ohne diese Mitteilungen nicht in der Lage sind, die Zulässigkeit der polizeilichen Speicherung zu überprüfen, habe ich das SMJus gebeten, die Staatsanwaltschaften und Gerichte auf die datenschutzrechtlich gebotene Mitteilung hinzuweisen - offenbar mit Erfolg, denn das Ministerium hat mir inzwischen zugesichert, geeignete Maßnahmen zu ergreifen.

8.5 Verwaltungsvorschrift über die Feststellung von Alkohol im Blut

Nach § 81 a StPO muß jeder Beschuldigte, dessen Blutalkoholgehalt für ein Bußgeld- oder Strafverfahren von Bedeutung sein kann, hinnehmen, sich durch einen Arzt eine Blutprobe entnehmen zu lassen (übrigens: "Ins Tütchen blasen" muß niemand). Dabei wird folgendermaßen verfahren: Sofern die Polizei eine Blutentnahme für erforderlich hält, führt sie den Betroffenen zu einem Arzt, damit dieser eine Blutprobe entnehmen kann. Diese Blutprobe wird sodann zu einer Untersuchungsstelle gebracht, die den Alkoholgehalt des Blutes ermittelt. In Sachsen gibt es drei Untersuchungsstellen: Die Landesuntersuchungsanstalt für das Gesundheits- und Veterinärwesen in Chemnitz, das Institutsklinikum der Technischen Universität Dresden und das Institut für Gerichtliche Medizin der Universität Leipzig. Diese Stellen erhalten eine Ausfertigung des vom Arzt und Polizeibeamten ausgefüllten Blutentnahmeprotokolls. In dieses - bundeseinheitlich verwendete - Protokoll werden unter anderem die Personalien des Betroffenen, der Anlaß der Blutentnahme, die körperliche, geistige und seelische Verfassung des Betroffenen und dessen eigene Angaben über etwaige Krankheiten oder eingenommene Medikamente aufgenommen. Im Protokoll sind somit äußerst sensible Daten enthalten.

Dieses Verfahren soll nun bundeseinheitlich durch eine Verwaltungsvorschrift geregelt werden. Vom SMJus wurde mir ein Entwurf des interministeriellen Ausschusses zu einer "Bundeseinheitlichen Verwaltungsvorschrift über die Feststellung von Alkohol im Blut bei Straftaten und Ordnungswidrigkeiten und über die Sicherstellung und Beschlagnahme von Fahrausweisen" zur Stellungnahme zugeleitet.

Als einen wesentlichen Mangel dieses Entwurfs habe ich angesehen, daß in der Ausfertigung des Protokolls, welches an die Untersuchungsstelle übersandt wird, der Name des Betroffenen nicht geschwärzt werden soll. Dieses Datum ist weder für die wissenschaftliche Forschung noch für die Erstattung eines Gutachtens in der Hauptverhandlung erforderlich. Eine Verwechslungsgefahr ist durch die Identifizierungsmerkmale des Protokolls, wie Identifikationsnummer, Geburtsjahr und Geschlecht ausgeschlossen. Für den Fall, daß die Protokollausfertigungen der besseren Übersichtlichkeit wegen nach Namen und nicht nach Nummern geordnet werden müssen, könnten die Namen zumindest auf die Anfangsbuchstaben verkürzt und die Nummern als zusätzliches Ordnungskriterium verwendet werden. Auf jeden Fall muß verhindert werden, daß bei den Untersuchungsstellen Sammlungen mit personenbezogenen Daten entstehen, die diese für Ihre Aufgabenerfüllung nicht benötigen. Außerdem gehen "interessante Fälle" (z. B. von Politikern oder Schauspielern) die Untersuchungsstellen nichts an.

Ferner habe ich mich gegen die in der Verwaltungsvorschrift vorgeschriebene 10jährige Aufbewahrungsfrist für die Aufzeichnungen und Ergebnisse der Alkoholbestimmung bei der Untersuchungsstelle ausgesprochen. In Anbetracht der Tatsache, daß die Blutproben nach der Verwaltungsvorschrift im Regelfall nur zwei Jahre aufbewahrt werden, sollten die dazugehörenden Ergebnisse der Alkoholbestimmung auch nur entsprechend lange aufbewahrt werden. Es ist für mich nicht ersichtlich, welchen Wert die Aufzeichnungen danach noch haben sollten, zumal sich die in den Aufzeichnungen enthaltenen Daten ebenfalls in den Ermittlungsakten (Gutachten) bei den Justizbehörden befinden.

Das SMJus, als stimmberechtigtes Mitglied im interministeriellen Ausschuß, hat sich meiner Auffassung zur Aufbewahrungsfrist für die Aufzeichnungen und Ergebnisse der Alkoholbestimmung angeschlossen und ihre Verkürzung auf fünf Jahre für angemessen gehalten. Auch meine weiteren Anregungen hat es an den interministeriellen Ausschuß weitergeleitet.

Meine Empfehlungen wurden in der nunmehr vorliegenden Endfassung der bundeseinheitlichen Verwaltungsvorschrift, die in Sachsen zum 1. Juni 1995 in Kraft gesetzt werden soll, im Ansatz aufgegriffen. So wurde die Aufbewahrungsfrist für die bei den Untersuchungsstellen aufbewahrten Unterlagen auf sechs Jahre verkürzt. Auch dürfen aus dem Protokoll, welches an die Untersuchungsstellen übersandt wird, "zumindest" Anschrift, Geburtstag und Geburtsmonat nicht mehr ersichtlich sein. Aus dieser Formulierung geht hervor, daß es den Ländern überlassen bleiben soll, die Protokollausfertigungen weitergehend zu anonymisieren. Ich werde mich dafür einsetzen, daß in Sachsen auch der Name aus dem Protokoll entfernt wird.

8.6 Automatisierte Datenverarbeitung im Justizvollzug

Im Freistaat Sachsen soll künftig ein "Informations- und Verwaltungssystem" (IVS) die Daten der Gefangenen erfassen, verwalten und recherchierbar machen, also die bisher von den Vollzugsgeschäftsstellen der Justizvollzugsanstalten manuell erledigten Aufgaben computergestützt erledigen.

Ich will sicherstellen, daß die Zugriffsmöglichkeiten der Bediensteten auf diejenigen Daten beschränkt werden, die sie für ihre konkrete Aufgabenerfüllung benötigen: So sind Informationen über das Bekenntnis, den Beruf und die Zahl der Vorstrafen grundsätzlich für die Aufgabenerfüllung der meisten Bediensteten einer Justizvollzugsanstalt nicht erforderlich. Auf diese Daten dürfen diese Personen deshalb weder Schreib- noch Lesezugriff erhalten.

Kritisiert habe ich an der Programmbeschreibung, daß sie keine konkreten Voraussetzungen nennt, unter denen die Datenverarbeitung erlaubt ist, sondern nur allgemein die bereits bestehenden Aufgaben und Tätigkeiten der Justizvollzugsbehörden beschreibt und die zukünftig rechnergestützt zu erledigenden Aufgaben daran anpaßt. Mit anderen Worten: Alles, was bisher manuell erlaubt war, soll nun auch technikgestützt erlaubt sein.

Dies wäre weniger bedenklich, wenn die zur Zeit manuell ausgeführten Datenverarbeitungen datenschutzrechtlichen Anforderungen genügen würden. Die einschlägigen Rechtsgrundlagen (Strafvollzugsgesetz, Verwaltungsvorschriften) enthalten aber keine ausreichenden datenschutzrechtlichen Regelungen. Ich habe deshalb vorgeschlagen, in der Programmbeschreibung die Voraussetzungen für die Datenverarbeitung näher zu konkretisieren. Auch sind die in der Programmbeschreibung verwendeten allgemeinen Begriffe wie "sonstige Daten" oder "entsprechende Behörden oder "für spätere Auskünfte an die Polizei, Staatsanwaltschaft usw." der Klarstellung halber durch eine Aufzählung der Daten und Behörden zu ersetzen. Nur so kann der Bedienstete sicher beurteilen, an welche Stellen er welche Daten unter welchen Voraussetzungen übermitteln darf.

Darüber hinaus fehlen in der Programmbeschreibung konkrete Angaben zu den nach § 9 SächsDSG zu treffenden personellen, technischen und organisatorischen Maßnahmen zur Gewährleistung des Datenschutzes (§ 9 SächsDSG).

Das SMJus hat mir geantwortet, daß meine Anregungen zum Teil in einer neuen Programmbeschreibung berücksichtigt werden. So sollen beispielsweise die zu erfassenden Daten beschrieben und auch die Behörden aufgeführt werden, an welche die Daten übermittelt werden. Auch der Umfang der mitgeteilten Daten und die konkreten Voraussetzungen für eine Auskunftserteilung sollen, soweit eben möglich, festgelegt werden. Nur die Personen erhalten Zugriff zu den Daten, die sie für ihre konkrete Aufgabenerfüllung benötigen. Das SMJus hat mir ebenfalls die für das Programm vorgesehenen personellen, technischen und organisatorischen Maßnahmen zur Gewährleistung des Datenschutzes erläutert.

Am IVS-Vorhaben wird deutlich, daß eine frühzeitige Beteiligung meiner Dienststelle regelmäßig zu datenschutzgerechten und aus Verwaltungssicht praxisbezogenen Lösungen führt.

8.7 Gefangene: Selbstauskunft durch Kreditsicherungsinstitute

Ein Gefangener fragte mich, ob es zulässig sei, daß eine Justizvollzugsanstalt ihm die Auflage erteilt, eine Auskunft eines Kreditsicherungsinstitutes ("Selbstauskunft der Schufa") vorzulegen. Andernfalls würden für die Zukunft keine Vollzugslockerungen genehmigt.

Auf meine Nachfrage teilte mir die Justizvollzugsanstalt mit, daß diese Schufa-Auskunft für die Durchführung von Schuldenregulierungsprogrammen erforderlich sei, da die Schulden der Gefangenen auf andere Weise nicht verbindlich festgestellt werden könnten. Diese Programme dienten dem Vollzugsziel der Resozialisierung, weil eine gesellschaftliche Wiedereingliederung nur dann erfolgversprechend sei, wenn den Gefangenen bei der Entlassung kein unübersichtliches Schuldenpaket drücke. Ich konnte die Klarstellung herbeiführen, daß die Selbstauskünfte nicht schematisch angefordert werden, sondern nur dann, wenn Schulden im Einzelfall einen kriminogenen Faktor darstellen und sie auf andere Weise nicht feststellbar sind.

Ich möchte betonen, daß auch ich es für eminent wichtig halte, daß den Gefangenen Schuldenregulierungsprogramme angeboten werden. Trotzdem kann meiner Auffassung nach das Verlangen nach einer Selbstauskunft nur ausnahmsweise zulässig sein, wenn es zur Aufgabenerfüllung der Justizvollzugsanstalt zwingend erforderlich ist. Eine Schufa-Auskunft über den Gefangenen ist jedoch (zumindest generell) schon deshalb nicht erforderlich, weil die Justizvollzugsanstalt ausreichend andere Möglichkeiten hat, sich über die finanzielle Situation eines Gefangenen zu informieren. So wird der Gefangene bereits im Aufnahmeverfahren zu seiner finanziellen Situation befragt, oder es ergeben sich aus Urteilen Anhaltspunkte für entsprechende Verpflichtungen (z. B. auf Zahlung von Schadensersatz oder auf Zahlung der Gerichtskosten). Auch aus Anfragen von Kreditinstituten oder anderen Gläubigern oder aus eingehenden Pfändungs- und Überweisungsbeschlüssen erfährt die Justizvollzugsanstalt von den Schulden eines Gefangenen. Schließlich hat auch die Ein- und Auszahlungsstelle der Anstalt einen gewissen Überblick über die finanziellen Aktivitäten des Gefangenen.

Die Justizvollzugsanstalt ist somit meines Erachtens in den meisten Fällen auch ohne eine Schufa-Auskunft des Gefangenen in der Lage, sich über die finanzielle Situation eines Gefangenen zu informieren. Selbst wenn die Schulden auf diese Weise nicht umfassend erfaßt werden können - was im übrigen auch nicht durch die Auskunft erreicht werden kann -, sollte der Gefangene nur in begründeten Ausnahmefällen zur Einholung einer Selbstauskunft aufgefordert werden. Auch wenn Schulden im Einzelfall das Motiv für die Begehung von Straftaten waren und eine Wiedereingliederung des Gefangenen nur dann erfolgversprechend ist, wenn ihn bei der Entlassung keine Schuldenlast drückt, darf beim Gefangenen nicht der Eindruck enstehen, daß er die Auskunft erteilen muß, um eine günstige Sozialprognose und die damit verbundenen Vollzugslockerungen zu erhalten.

Von einer Freiwilligkeit der Auskunft kann nämlich in einer solchen Situation nicht mehr die Rede sein.

8.8 EDV-geführtes Grundbuch

Das SMJus betreibt zusammen mit dem Bayerischen Staatsministerium der Justiz das Pilotprojekt eines EDV-geführten Grundbuches. Die Landesjustizverwaltung von Sachsen-Anhalt ist dem Projekt inzwischen beigetreten; die Landesjustizverwaltung Hamburg kommt demnächst hinzu.

Den Entwicklungsstand des EDV-geführten Grundbuchs, das auf den Bestimmungen des Registerverfahrensbeschleunigungsgesetzes aufbaut, habe ich bei zwei Kontrollbesuchen im Grundbuchamt Dresden überprüft:

Seit Januar 1995 läuft der Testbetrieb, bei dem zunächst zwischen dem Grundbuchamt Dresden und der Rechenzentrale der Justiz das Programm auf seine technische Funktionsfähigkeit hin geprüft wird. Danach soll der Betrieb auf die Einsichtnahme externer Benutzer, die von Justizangestellten fingiert wird, erweitert werden. Parallel zum EDV-Testbetrieb wird das Grundbuch manuell weitergeführt.

Das System des EDV-geführten Grundbuchs weist folgende technische Merkmale auf:

Hard- und Software

Die Systemarchitektur von SOLUM-STAR besitzt drei Ebenen. Innerhalb eines Grundbuchamtes wird das Client-Server-Modell verwendet. Der Nutzer (Rechtspfleger) arbeitet mit einem PC, der als Client an einem Server hängt. Dieser wiederum ist mit einem RISC-Rechner in dem für Sachsen zentralen Grundbuchrechenzentrum verbunden.

Die Verbindung zum zentralen Rechenzentrum wird über ISDN-Wählleitungen mit Routern hergestellt.

Auf den PCs läuft außer MS-DOS und Word für Windows keine Anwendung. SOLUM-STAR befindet sich auf dem Server und wird über das Netz aufgerufen.

Im zentralen Rechenzentrum befindet sich eine Jukebox, auf der optische Platten (WORM-Write Once, Read Many) gelesen und beschrieben werden können.

Zum Drucken werden dokumentenechte Laserdrucker verwendet, die im Netz eingebunden sind.

Datenverarbeitung

Nach Legitimation durch Paßwort (und geplant: Chipkarte) erhält der Rechtspfleger Zugriff auf die SOLUM-STAR-Funktionalitäten (Recherche, Verändern, Speichern, Drucken). Innerhalb der Anwendung ist ein einfacher Wechsel zwischen den Funktionalitäten nur durch Rückgang in das Grundmenü möglich. Hat der Rechtspfleger den Datensatz verändert, so kann er ihn auf dem Server nach Abgabe seiner elektronischen Unterschrift abspeichern. Vom Server zum zentralen Rechenzentrum werden mehrmals täglich (bisher geplant 2mal) die Veränderungen übertragen und dort auf WORM gespeichert. Diese ist etwa zur Hälfte mit den Grunddaten belegt und wird schrittweise um die Veränderungen ergänzt.

Systemsicherheit / Stabilität

Beim Datenaustausch zwischen Server und Client erfolgt eine Prüfung, ob die Dateien fehlerhaft sind. Auf dem Server wird mehrmals täglich gesichert. Auf zentraler Ebene wird es ein Back-Up-Rechenzentrum geben. Der Server ist durch USV (Unabhängige Stromversorgung) vor Ausfällen geschützt; für die Clients ist Gleiches im Gespräch.

Zur Stabilität von SOLUM-STAR kann man erst nach dem Testbetrieb Näheres sagen.

Die Sicherheit in der externen Verbindung soll zum einen durch Router, die fest eingestellt und nicht selbstlernend sind, und zum anderen durch eine Verschlüsselung der Daten (public key - secret key, zusätzlich geplant mit Chipkarte) gewährleistet werden.

Zugangsberechtigung und Protokollierung

Bei der Zugangsberechtigung gibt es drei große Gruppen:
- berechtigte Mitarbeiter (in der Regel Rechtspfleger)
- externe Nutzer
- Systemadministratoren (wahrscheinlich aus dem zentralen Rechenzentrum)

Berechtigte Mitarbeiter können den vollen Funktionsumfang nutzen. Sie müssen sich mit Nutzerkennung, Paßwort und Chipkarte identifizieren. Ihre Aktivitäten werden vollständig protokolliert.
Die Gruppe “externe Nutzer” unterteilt sich in drei Untergruppen:
- Notare (Identifikation im Abrufverfahren durch Nutzerkennung und Chipkarte)
- Kreditinstitute (Identifikation im Abrufverfahren durch Nutzerkennung, Chipkarte und Abrufartangabe)
- Sonstige (Verfahrensgang wie bisher beim manuellen Grundbuch, ggf. Einsichtnahme am Schirm unter Aufsicht eines Grundbuchbeamten oder Erhalt eines Grundbuchauszuges)

Die Protokollierung (Zugang und Tätigkeiten) erfolgt vollständig. Externe Nutzer, die dem automatischen Abrufverfahren angeschlossen sind und dabei ein berechtigtes Interesse nachweisen müssen (z. B. Kreditinstitute), müssen allerdings im Gegensatz zum manuellen Grundbuch nur im Menü das Vorliegen einer Berechtigung bestätigen, ohne daß dies sofort überprüft wird. Dies soll nach der Grundbuchverfügung (GBV) mit einer nachträglichen Kontrollmöglichkeit durch die Justizverwaltung ausgeglichen werden.

Zur Systemadministrierung können bis jetzt noch keine näheren Aussagen gemacht werden, da diese durch das zentrale Rechenzentrum geschieht, was bisher noch nicht im Testbetrieb einbezogen war. Vorgesehen ist die Systembetreuung im zentralen Rechenzentrum, wobei ein Auswertungsprogramm (unter anderem zur Gebührenabrechnung) verwendet werden soll.

Tests und Wartung

Die Wartung erfolgt durch eine Privatfirma, deren Mitarbeiter verpflichtet sind und Zugang nur unter Kontrolle haben. Bei Datenfehlern oder -zerstörung auf den WORM-Platten im zentralen Rechenzentrum wird eine Berliner Spezialfirma mit der Reparatur beauftragt.

Für die Tests werden veraltete Echtdaten verwendet. Eine Anonymisierung findet nicht statt.

Räumliche Unterbringung

Die Clients stehen an den Plätzen der Rechtspfleger. Der Server soll in einem speziellen Raum des Grundbuchamtes installiert werden. Die beiden zentralen Rechenzentren werden Hochsicherheitsrechenzentren. Ein detailliertes Sicherheitskonzept existiert anscheinend noch nicht.

Erfassung der Altdaten

Das SMJus bildet drei, später sechs, Umstellungsgruppen, die alle alten Grundbücher manuell erfassen.

Beim derzeitigen Stand des EDV-geführten Grundbuches stellen sich drei Probleme:

- Eine objektbezogene Differenzierung der Zugriffsberechtigung ist nur grob möglich. Zwar muß z. B. der Notar beim automatischen Abruf die Nummer des Grundbuchblattes angeben, so daß er immer nur Zugang zu diesem konkreten Blatt erhält. Eine Sperrung bestimmter Abteilungen oder gar Einträge ist zur Zeit allerdings nicht möglich.

- Die Auswertung der Protokolle wird einseitig unter den Aspekten der Datensicherheit und der Gebührenabrechnung betrachtet. Darüber hinaus muß aber auch das Auskunftsinteresse des einzelnen Bürgers berücksichtigt werden. Es genügt also nicht, die Auswertung der Protokolldaten auf das zentrale Rechenzentrum zu beschränken, denn der Grundstückseigentümer wendet sich an das für ihn zuständige Grundbuchamt, wenn er Auskunft über die sein Grundstück betreffenden Einsichtnahmen haben will.

- Des weiteren wurden die Protokollaufbewahrungsfristen noch nicht geregelt.

Mit der auf ganz Sachsen ausgedehnten Anwendung des EDV-geführten Grundbuches ist nach Auskunft des SMJus nicht innerhalb der nächsten zwei bis drei Jahre zu rechnen.

8.9 Auskünfte an die Presse

Der Präsident eines sächsischen Gerichts fragte mich im Rahmen eines förmlichen Ersuchens nach § 27 Abs. 4 SächsDSG, ob es zulässig sei, daß sein Gericht die Tagesordnungen (Sitzungslisten) vor dem Termintage an die Presse übermittelt. Erst hierdurch erfuhr ich, daß das SMJus im Dezember 1994 eine Verwaltungsvorschrift über das Justizpressewesen erlassen hatte. An der Vorbereitung dieser Vorschrift, die zu tiefgreifenden Beeinträchtigungen des Persönlichkeitsrechts der Verfahrensbeteiligten führen kann, war ich vom SMJus nicht beteiligt worden. Ich habe dieses Versäumnis gegenüber der Hausleitung zur Sprache gebracht.

Für Presseauskünfte durch die Justiz ist folgende Rechtslage zu beachten:

- Bereichsspezifische Übermittlungsregelungen mit Gesetzesqualität (z. B. ein "Justizmitteilungsgesetz") fehlen nach wie vor.
- Die bundeseinheitlichen Justizverwaltungsvorschriften MiStra und MiZi kommen wegen fehlender Normqualität als Rechtsgrundlage für Datenübermittlungen nicht in Betracht. Schon im Jahre 1976 (also sieben Jahre vor dem Volkszählungsurteil) hatte das Bundesverfassungsgericht ausgeführt, daß die MiStra mangels gesetzlicher Regelung nur noch für eine Übergangsfrist angewandt werden könne (BVerfGE 41, 251).
- Aus demselben Grunde kommt die Verwaltungsvorschrift des SMJus über das Justizpressewesen als befugnisbegründende Datenübermittlungsnorm nicht in Betracht.
- Eine Übermittlungsverpflichtung für die Justiz könnte § 4 Abs. 1 SächsPresseG begründen. Danach sind alle Behörden verpflichtet, den Vertretern der Presse und des Rundfunks, die sich als solche ausweisen (Presseausweise werden bei "journalistischer Tätigkeit" von Berufsverbänden, Gewerkschaften und Verlagshäusern ausgegeben), die der Erfüllung ihrer Aufgabe dienenden Auskünfte zu erteilen, sofern nicht das Sächsische Pressegesetz oder allgemeine Rechtsvorschriften dem entgegenstehen. Nach § 4 Abs. 2 Nr. 1 SächsPresseG darf die Auskunft jedoch verweigert werden, "wenn und soweit Vorschriften über die Geheimhaltung und über den Persönlichkeitsschutz entgegenstehen".

  Als hier einschlägige Vorschrift über den Persönlichkeitsschutz kommt das Sächsische Datenschutzgesetz in Betracht. Nach § 15 Abs. 1 Nr. 2 SächsDSG ist die Übermittlung personenbezogener Daten an andere als die in §§ 13, 14 und 16 genannten Personen oder Stellen zulässig, wenn der Empfänger ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft darlegt und der Betroffene kein schutzwürdiges Interesse am Unterbleiben der Übermittlung hat. § 15 Abs. 3 SächsDSG setzt jedoch voraus, daß in den Fällen des Abs. 1 Nr. 2 der Betroffene vor der Übermittlung zu hören und im Fall der Übermittlung zu unterrichten ist. Dies gilt nicht, wenn dem schwerwiegende öffentliche oder private Belange entgegenstehen. Diese Voraussetzungen sind in der Regel nicht erfüllt.

  Die Formulierung "darf" in § 4 Abs. 2 Nr. 1 SächsPresseG begründet für den Behördenleiter einen Ermessensspielraum für seine Entscheidung gegenüber dem Pressevertreter; dieser Ermessensspielraum bezieht sich jedoch nicht auf das Verhältnis zwischen Behördenleiter und dem Betroffenen, dessen Daten zur Übermittlung anstehen: Hier gelten die grundrechtlich geprägten speziellen (z. B. § 121 SächsBeamtG) oder

allgemeinen Rechtsvorschriften zur Datenübermittlung (§ 15 SächsDSG), die ihrerseits keine Ermessensspielräume eröffnen, sondern voll nachprüfbare unbestimmte Rechtsbegriffe enthalten.

Als Ergebnis bleibt festzuhalten, daß in den allermeisten Fällen die Übermittlung personenbezogener Informationen aus Gerichtsverfahren nicht auf eine tragfähige Rechtsgrundlage gestützt werden kann.

Diesem Defizit an konkreten gesetzlichen Festlegungen steht eine rasante Entwicklung der Medientechnik und eine verstärkte kommerzielle Nutzung von Pressedatenbanken gegenüber, was zu qualitativ neuen Gefährdungen für das Persönlichkeitsrecht des Einzelnen führt: Durch die Verbreitung von Informationen über Netze und auf elektronischen Datenträgern kann in bisher unbekanntem Maß auf große Informationsbestände durch jedermann zugegriffen werden. Lang zurückliegende Informationen können auf schnellstem Wege recherchiert werden; einmal an die Presse weitergegebene personenbezogene Informationen, die möglicherweise schon im Justizbereich nicht mehr verarbeitet werden dürfen, würden auf diese Weise bei der Presse fortleben. Auch droht das in verschiedenen Rechtsbereichen vorgesehene "Recht auf Vergessen" wirkungslos zu werden, wenn die vom Bundeszentralregister zu beachtenden Löschungsvorschriften durch automatisierte Abrufe aus einer Pressedatenbank unterlaufen werden können.

Bezogen auf den oben angesprochenen Ausgangsfall könnte die Übermittlung der Sitzungslisten bei der Presse zu vollständigen Datensammlungen aller gerichtshängigen Verfahren führen. In bestimmten Gerichtszweigen böte die potentielle Interpretierbarkeit bestimmter Daten weite Auswertungsmöglichkeiten. So könnte das Kündigungsverhalten von Firmen anhand der Zahl ihrer Arbeitsgerichtsprozesse abgelesen werden, über die Prozeßvertretung ließe sich erkennen, ob (und wo) eine Partei gewerkschaftlich organisiert ist, - dies sind nur wenige Beispiele.

In besonderem Maße kann das Recht auf informationelle Selbstbestimmung durch Bekanntgabe von Daten aus Strafermittlungsverfahren beeinträchtigt werden: Dies gilt für Beschuldigte und Angeklagte, für andere Verfahrensbeteiligte (wie z. B. Verwandte, Opfer von Straftaten, Zeugen), in besonderem Maße jedoch für unbeteiligte Personen aus dem sozialen Umfeld der Adressaten des Strafverfahrens.

Nach § 6 Abs. 2 der Verwaltungsvorschrift über das Justizpressewesen soll der Presse die Anklageschrift vor der Hauptverhandlung zur Einsichtnahme zugänglich gemacht werden können, wenn anzunehmen ist, daß das Strafverfahren in der Öffentlichkeit eine "besondere Beachtung finden werde". Abgesehen davon, daß die Verwaltungsvorschrift ohnehin nicht als Rechtsgrundlage für die Datenübermittlung in Betracht kommt, begegnet diese Regelung meiner schärfsten Kritik: Auch wenn sich die Einsichtnahme nicht auf das wesentliche Ergebnis der Ermittlungen erstreckt, erhalten die Presseorgane Kenntnis von äußerst sensiblen personenbezogenen Daten, da die Anklageschrift u. a. sämtliche Angaben zu der zur Last gelegten Tat, zur Person und zum Werdegang des Angeklagten enthält. Damit ist einer möglichen Vorverurteilung des Angeklagten in der Öffentlichkeit Tür und Tor geöffnet. Inwieweit hier noch das rechtsstaatliche Prinzip der Unschuldsvermutung mit Leben erfüllt werden kann, bleibt fraglich. Welchen Beitrag die

Gewährung von Presseeinsicht in nicht abgeschlossene Justizunterlagen leisten kann, dem generalpräventiven Zweck der Vorschrift (§ 1) zu dienen, erschließt sich mir ebenfalls nicht.

Ein Anspruch der Presse auf Vorabübermittlung der Sitzungslisten ergibt sich auch nicht aus § 169 GVG. Nach dieser Vorschrift muß zwar grundsätzlich die Verhandlung vor dem erkennenden Gericht und immer die Verkündung des Urteils öffentlich sein, so daß die öffentliche Kontrolle des Verfahrens und das Informationsinteresse der Allgemeinheit gewahrt wird, die Öffentlichkeitsmaxime gilt jedoch nur für die Hauptverhandlung. Öffentlichkeitserweiterungen über den Gerichtssaal hinaus würden den Angeklagten zum Schauobjekt degradieren. Dies ist mit seiner Menschenwürde unvereinbar. Im Simpson-Prozeß in den USA erleben wir gerade, wie Angeklagter, Opfer, Zeugen, Sachverständige, Ankläger, Verteidiger und Gericht in der Öffentlichkeit "vorgeführt" werden.

Schließlich ist zu bedenken, daß das Strafprozeßrecht zum Schutz des Persönlichkeitsrechts in § 171 b GVG den Ausschuß der Öffentlichkeit regelt. Die Vorschrift trägt dem Umstand Rechnung, daß ein Straf- und Prozeßrecht, das sich immer mehr die Persönlichkeitserforschung zur Aufgabe macht, es erfordert, in der Hauptverhandlung mehr als früher Umstände aus dem persönlichen Lebensbereich, teilweise auch aus dem Intimbereich, sowohl des Angeklagten als auch von Zeugen und insbesondere auch von Tatopfern zu erörtern. Das muß aber nicht vor den Ohren der Öffentlichkeit geschehen. § 171 b GVG erlaubt es daher in Übereinstimmung mit Art. 6 Abs. 1 Satz 2 MRK, das Öffentlichkeitsprinzip hinter dem verfassungsrechtlich geschützten Anspruch auf Achtung der Privatsphäre zurücktreten zu lassen.

Ich erwarte vom SMJus eine gründliche und am Rechtsstaat orientierte Überarbeitung seiner Verwaltungsvorschrift unter meiner Beteiligung.

8.10 Vordrucke der Landesjustizkasse

Der Datenschutzbeauftragte einer sächsischen Großstadt machte mich auf die Praxis der Landesjustizkasse aufmerksam, mittels eines Vordruckes für "Amtshilfeersuchen" in weitem Umfang personenbezogene Daten von Kostenschuldnern bei Stadt- und Gemeindeverwaltungen zu erheben.

Bereits die Bezeichnung "Amtshilfeersuchen" begegnete meiner datenschutzrechtlichen Kritik: Die allgemeine Amtshilfepflicht (Pflicht zum zwischenbehördlichen Beistand) kommt nach dem Volkszählungsurteil des Bundesverfassungsgerichts vom 15. Dezember 1983 (BVerfGE 65, 1 ff.) als Rechtsgrundlage für die Verarbeitung personenbezogener Daten nicht in Betracht. Die Bezeichnung darf daher nicht verwendet werden, wenn Behörden andere öffentliche Stellen um Übermittlung personenbezogener Daten ersuchen. Gerade in der Justiz sollte sich das herumgesprochen haben.

Im Vordruck wurde zum Familienstand gefragt, ob der Betroffene getrennt lebt, bei der Frage nach der ausgeübten Tätigkeit wurde Auskunft darüber verlangt, ob er Angestellter oder Selbstständiger sei.

Ich habe die Landesjustizkasse darauf hingewiesen, daß die bei den Meldebehörden vorliegenden Datenbestände nach § 5 Abs. 1 Nr. 14 SächsMG lediglich den Familienstand, bei Verheirateten zusätzlich den Tag und Ort der Eheschließung umfassen dürfen. Auch wird nach § 5 Abs. 1 Nr. 8 SächsMG nur gespeichert, ob eine Erwerbstätigkeit vorliegt oder nicht. Die Merkmale "Angestellter" oder "Selbstständiger" sind nicht in das Wissen der Meldebehörden gestellt.

Des weiteren war für die Landesjustizkasse offenbar von Interesse, ob Grundbesitz vorhanden sei; wenn ja, sollte die Lage des Grundstücks angegeben werden - Daten, die vom Steuergeheimnis nach § 30 Abs. 1 und Abs. 2 AO geschützt sind und deshalb in diesem Zusammenhang nicht erhoben werden dürfen.

Die Landesjustizkasse kündigte zunächst an, aufgrund meiner Kritik künftig fünf verschiedene Muster zu verwenden, die auf die einzelnen Behörden (Stadt-/Gemeindeverwaltung, zentrale Ausländerbehörde, Arbeitsamt, Gewerbeamt, AOK) zugeschnitten seien; damit würde den datenschutzrechtlichen Anforderungen genügt.

Die Muster machten eine erneute datenschutzrechtliche Stellungnahme notwendig, da Daten an die Landesjustizkasse übermittelt werden sollten, ohne daß dies zu deren Aufgabenerfüllung erforderlich war: Rechtsgrundlage für die Übermittlung der Daten von der Meldebehörde an die Landesjustizkasse ist § 29 Abs. 1 SächsMG. Danach dürfen die Daten “Name, Vorname, Geburtsdatum, Anschrift, verheiratet, geschieden, ledig” übermittelt werden, wenn dies zur Aufgabenerfüllung des Empfängers erforderlich ist. Es ist nicht eindeutig, wozu im Rahmen der Vollstreckung das Datum “geschieden” erforderlich sein soll. Die Mitteilung “verheiratet/nicht verheiratet” würde ausreichen.
Das Datum “getrennt lebend” betrifft nicht den Familienstand, sondern ist Besteuerungsmerkmal (vgl. § 5 Abs. 2 Nr. 2 SächsMG). Da Steuerdaten besonders schutzwürdig sind und die Übermittlung des Datums eine Zweckänderung bedeuten würde (das Datum wird für die Mitwirkung bei der Ausstellung von Lohnsteuerkarten

gespeichert), ist eine besonders restriktive Auslegung des § 29 Abs. 2 SächsMG geboten. Ich habe daher angeregt, dieses Datum vom Vordruck zu streichen.

Die erwünschte Übermittlung der Daten an die Landesjustizkasse durch die Ausländerbehörden ist sogar völlig unzulässig. Ein Vordruck für die Ausländerbehörden darf daher nicht verwendet werden. Zwar läßt § 13 SächsDSG eine Datenübermittlung zwischen öffentlichen Stellen unter bestimmten Voraussetzungen zu, das Sächsische Datenschutzgesetz findet jedoch als sogenanntes "Auffanggesetz" (vgl. § 2 Abs. 4 SächsDSG) keine Anwendung, weil der Bundesgesetzgeber bereichsspezifisch und abschließend die Voraussetzungen einer Datenübermittlung an andere Stellen in § 79 Abs. 1 AuslG geregelt hat. Hiernach dürfen Ausländerbehörden Daten von Ausländern nur an die dort abschließend genannten Behörden übermitteln. Die Landesjustizkasse gehört nicht zu den möglichen Datenempfängern. Sie kann sich im Falle von Ausländern an die jeweilige Meldebehörde wenden.

Soweit die AOK um Übermittlung personenbezogener Daten ersucht wird, gilt folgendes:
Rechtsgrundlage für die Datenübermittlung der AOK an die Landesjustizkasse ist § 284 Abs. 1, 3 SGB V i. V. m. § 68 Abs. 1 SGB X. Der Sozialleistungsträger darf danach Name, Vorname, Geburtsdatum, Geburtsort, derzeitige Anschrift des Betroffenen sowie Name und Anschrift seiner derzeitigen Arbeitgeber übermitteln. Unzulässig auf dem Vordruck ist somit die Frage nach dem Beruf. Die Frage nach dem bekannten letzten Arbeitgeber ist in dieser Form ebenfalls unzulässig. Sie sollte an die gesetzliche Formulierung ("derzeitiger Arbeitgeber") angepaßt werden.
Zusätzlich ist die Übermittlung der Daten nach § 68 Abs. 1 SGB X an bestimmte Voraussetzungen geknüpft.
Erste Voraussetzung für die Übermittlung ist, daß die Anspruchshöhe mindestens 1000,- DM beträgt. Erreicht der Anspruch diese Höhe nicht, ist die Übermittlung der Daten an die Landesjustizkasse unzulässig. Eine andere Übermittlungsbefugnis ist für diese Fälle nicht ersichtlich.

Problematisch ist überdies, daß der Sozialleistungsträger die genannten Angaben nur machen darf, soweit kein Grund zu der Annahme besteht, daß durch die Übermittlung schutzwürdige Interessen des Betroffenen beeinträchtigt werden (vgl. § 68 Abs. 1 Satz 1 SGB X).
Dies bedeutet für die AOK, daß sie eine eigene Abwägung zu treffen hat, ob die verlangten Daten übermittelt werden dürfen oder nicht. Bei der Angabe des Arbeitgebers ist die Gefahr einer solchen Beeinträchtigung sehr hoch, da durch die Vollstreckung der Arbeitgeber von den Problemen seines Mitarbeiters erfährt und daraus möglicherweise Konsequenzen zieht.
Nach § 68 Abs. 1 Satz 2 SGB X ist die ersuchte Stelle auch dann nicht zur Übermittlung verpflichtet, wenn sich die ersuchende Stelle die Angaben auf andere Weise beschaffen könnte. Dadurch soll verhindert werden, daß den Sozialleistungsträgern die Funktion von Ersatzmeldebehörden zukommt. Sinnvoll wäre daher, wenn die Landesjustizkasse zunächst versuchen würde, sich die Anschrift des Schuldners von der Meldebehörde zu verschaffen.

Auf meine Kritik hin wurden die Vordrucke bislang nur teilweise datenschutzgerecht gestaltet. Wenn beim Justizfiskus nicht bald erkannt wird, daß Grundrechte noch

wichtiger sind als das liebe Geld, werde ich wohl um eine Beanstandung nicht herumkommen. Zuvor habe ich ein Gespräch angeregt.

8.11 Ehescheidungsverbundurteile

Sogenannte Ehescheidungsverbundurteile, die neben dem Ausspruch der Scheidung auch gleichzeitig die Entscheidung über Zugewinnausgleich, Unterhalt, Sorgerecht etc. enthalten, müssen geschiedene Eheleute bei zahlreichen Behörden und sonstigen Stellen (Meldebehörde, Standesamt, Finanzamt, Arbeitgeber usw.) vorlegen. Damit erhalten diese Stellen - neben den von ihren benötigten Angaben - zwangsläufig eine Vielzahl von personenbezogenen Informationen, die zu ihrer Aufgabenerfüllung nicht im geringsten benötigt werden: Oft wird es ausreichen, bei Behörden und sonstigen Stellen einen Auszug des Urteilstenors vorzulegen, der ohnehin nach der Hauptsache und den Verbundsachen getrennt gefaßt ist; die genaue Sachverhaltsschilderung und die Entscheidungsgründe interessieren ersichtlich nicht. Selbst im Rahmen der Zwangsvollstreckung dürfte es genügen, wenn der Gerichtsvollzieher eine vollstreckbare Teilausfertigung ohne Tatbestand und Entscheidungsgründe - z. B. nur mit dem Zahlungsausspruch - erhält.

Ein datenschutzrechtliches Problem besteht auch darin, daß die vielfach rechtsunkundige Partei - (der Anwalt hat das Mandat beendet) - nicht weiß, daß sie sich für die verschiedenen Zwecke zur Vorlage bei Behörden Auszüge aus dem Urteilstenor des Verbundurteils anfertigen lassen kann.

Ich habe daher dem SMJus vorgeschlagen, daß die Geschäftsstelle des Familiengerichts bei der Versendung des Urteils an die Parteien in einem beigefügten Merkblatt auf die Möglichkeit hinweist, sich Auszüge aus dem Urteilstenor fertigen zu lassen. Bei der anschließenden Anforderung weiterer Urteilsausfertigungen könnte dann den Wünschen der Parteien und den entsprechenden Verwendungszwecken der Ausfertigungen Rechnung getragen werden. Noch einfacher und bürgerfreundlicher wäre es, eine amtliche Abschrift des Tenors mit dem Aufdruck "zur Vorlage bei Behörden" auszufertigen und mit zuzusenden.

Zu meinem Bedauern sind meine Vorschläge beim SMJus auf "taube Ohren" gestoßen: Ein Merkblatt sei "auch unter dem Gesichtspunkt der Deregulierung kontraproduktiv"; starke Worte zu einem einfachen Vorschlag, der spätere zeitraubende Verwaltungsarbeit, nämlich den Wunsch nach weiteren Ausfertigungen des Urteils, einspart. Hier wird deutlich, daß aus Furcht vor nur vermeintlich höherem Verwaltungsaufwand grundrechtsschützende - und damit zwingend gebotene - bürgernahe Maßnahmen unterbleiben.

Ich werde hier nicht locker lassen.

8.12 Wertanfragen in Testaments- und Nachlaßsachen

Um den Wert eines Nachlasses zu ermitteln, werden die Angehörigen der Verstorbenen vom Nachlaßgericht mit einem Vordruck mit umfangreichen Fragen zur Nachlaßmasse behelligt.

Benötigt werden die erfragten Nachlaßangaben nur für die Berechnung der Gebühren nach der Kostenordnung. Zwar trifft den Kostenschuldner bei der Ermittlung des Nachlaßwertes grundsätzlich eine Mitwirkungspflicht, eine Rechtsvorschrift zur zwangsweisen Datenerhebung existiert jedoch nicht.

Um den datenschutzrechtlichen Anforderungen zu genügen, müssen die Angehörigen daher nach § 11 Abs. 2 Satz 2 SächsDSG auf die Freiwilligkeit ihrer Abgaben zum Nachlaß hingewiesen werden. Diesen Hinweis ließen die in Sachsen verwendeten Formulare bislang vermissen.

Obwohl das SMJus zunächst die geplante Änderung der Kostenordnung abwarten wollte, hat es auf meine Anregung hin die Vordrucke um den Hinweis der Freiwilligkeit der Angaben ergänzt.

Dies begrüße ich, denn das Recht auf informationelle Selbstbestimmung darf nicht hinter vordergründigen verwaltungsökonomischen Gesichtspunkten zurücktreten. Ich erwarte aber auch, daß dieser große Verwaltungsaufwand lediglich zur Gebührenbemessung dadurch unterbleibt, daß der Bund die Kostenvorschriften radikal vereinfacht. Ein großer Nachlaß macht ja nicht mehr Arbeit beim Nachlaßgericht als ein kleiner Nachlaß. Gerechter wäre es, den (Zeit-)Aufwand des Gerichts zu vergüten.

8.13 Sächsische Rechtsanwaltskammer verlangt Offenbarung von Mandantendaten

Wenn im Freistaat Sachsen ein Rechtsanwalt seine Zulassung als Fachanwalt für Steuerrecht beantragt, verlangt die Sächsische Rechtsanwaltskammer von ihm, eine Liste von 50 seiner Mandanten sowie deren Steuernummern vorzulegen.

Diese Praxis ist nicht vom Gesetz über Fachanwaltsbezeichnungen nach der Bundesrechtsanwaltsordnung (RAFachBezG) gedeckt: Nach § 9 Abs. 1 dieses Gesetzes ist der Nachweis besonderer praktischer Erfahrungen auf dem Gebiet des Steuerrechts in der Regel erbracht, wenn der Bewerber 50 Fälle, davon mindestens ein Zehntel gerichtliche Verfahren, als Rechtsanwalt selbständig bearbeitet hat. Zum Modus legt das Gesetz lediglich fest, daß vom Rechtsanwalt "schriftliche Unterlagen" vorzulegen sind (§ 10 Abs. 1 RAFachBezG). Eine konkretere Charakterisierung des Inhalts und des Umfangs der vorzulegenden Schriftstücke nimmt das Gesetz nicht vor.

Somit ist unter dem Gesichtspunkt des verfassungsmäßigen Verhältnismäßigkeitsgebots bei der Ausgestaltung des Verfahrens darauf zu achten, daß Eingriffe in Rechte Dritter (hier: in das Grundrecht auf informationelle Selbstbestimmung der Mandanten und dritter Personen) so gering wie möglich zu halten sind. Der Vorschrift des § 203 Abs. 1 Nr. 3

StGB, die das Rechtsgut des persönlichen Lebens- und Geheimnisbereiches der Mandanten schützt, kommt hierbei zentrale Bedeutung zu. Danach wäre die Offenbarung von Mandantendaten nur dann nicht strafbar, wenn sie auf eine Befugnisnorm gestützt werden könnte. Dies ist vorliegend jedoch nicht der Fall: Das RAFachBezG kommt als Befugnisnorm nicht in Betracht, weil es keine Regelung enthält, die den Umfang des Eingriffs in das informationelle Selbstbestimmungsrecht der Mandanten und Dritter in der vom Bundesverfassungsgericht im Volkszählungsurteil (BVerfGE 65, 1 ff.) geforderten Weise hinreichend präzise umreißt.

Diese Rechtslage habe ich der Sächsischen Rechtsanwaltskammer eingehend dargelegt. Ich habe aufgezeigt, daß nur ein Verfahren zulässig ist, das die Vorlage solcher schriftlicher Unterlagen im Sinne des § 10 RAFachBezG umfaßt, die keine personenbezogenen Daten von Mandanten und dritten Personen mehr enthalten.

Zu meinem Bedauern hat der Präsident der Rechtsanwaltskammer in seinem - etwas oberflächlichen - Antwortschreiben angekündigt, an der bisherigen Praxis festhalten zu wollen. Er vertritt die nicht näher nachvollziehbare Auffassung, Mandantennamen und Aktenzeichen fielen als "öffentliche" Daten nicht unter die anwaltliche Geheimhaltungspflicht. Ich habe mich daher veranlaßt gesehen, über die Rechtslage aufzuklären und sachgerechte Praxisvorschläge zu machen.

Geschütztes Rechtsgut des § 203 StGB ist der persönliche Lebens- und Geheimbereich, der im Individualinteresse des Betroffenen nicht verletzt werden darf. Es geht also nicht um die ungestörte Ausübung der in § 203 Abs. 1 StGB genannten Berufe, sondern um den Schutz des allgemeinen Persönlichkeitsrechts, das auch das verfassungsrechtlich gesicherte Recht einschließt, grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden dürfen. Denn jeder, der sich einem Anwalt anvertraut muß sicher sein, daß sein Fall nicht personenbezogen von einer Anwaltsjury zur Kenntnis genommen wird, also von Anwälten, die er nicht kennt, die womöglich sogar seinen Gegner vertreten. Ich hätte von der Standesvertretung der Anwälte, die jetzt ja auch hierzulande berufen sind, den Rechtsstaat mit zu prägen, ein wenig mehr Fingerspitzengefühl erwartet.

Es ist zwar richtig, daß der Geheimhaltungspflicht nicht unterliegt, was Gegenstand einer öffentlichen Gerichtsverhandlung war; dies trifft jedoch auf die in anwaltlichen Akten enthaltenen personenbezogenen Daten nicht zu: Wenn ein Mandant juristischen Rat bei einem Rechtsanwalt einholt und er dabei persönliche Daten, Tatumstände, Vermögensverhältnisse, personenbezogener Daten Dritter etc. offenbart, werden diese Daten von der Schweigepflicht des Rechtsanwalts erfaßt, weil der Mandant regelmäßig ein schutzwürdiges Interesse an der Geheimhaltung seiner Angaben hat.

Es ist ersichtlich unverhältnismäßig, den gesamten Akteninhalt mit sämtlichen personenbezogenen Daten vorzulegen. Zwar sieht das Gesetz auch die Beurteilung der praktischen Erfahrungen vor, dennoch sprengt die Vorlage der gesamten Akte den Rahmen der Erforderlichkeit. Deshalb sollten nur die Aktenteile vorgelegt werden, die eine Einschätzung der Qualität der anwaltlichen Tätigkeit ermöglichen (z. B. komplizierte Anträge, Rechtsausführungen, anhand der Rechtsprechung gegliederter und abgeschichteter Sachvortrag). Diese Aktenauszüge sind dann vom Rechtsanwalt

entsprechend seiner aus § 203 StGB folgenden Geheimhaltungspflicht zu anonymisieren. Ohne eine zusätzliche anwaltliche Versicherung des Rechtsanwalts, seines Sozius oder des Bürovorstehers, daß der Inhalt der überreichten Unterlagen das geistige Werk des Rechtsanwalts (und nicht eines Sozius, angestellten Rechtsanwalts, Assessors, Referendars oder sonstigen Mitarbeiters) ist, kann die persönliche Leistung des Anwalts ohnehin nicht als gesichert angesehen werden.

Ich habe die Rechtsanwaltskammer um eine Stellungnahme gebeten; eine Beanstandung behalte ich mir vor.

8.14 Ist das Einschalten der Lauthöreinrichtung (Lautsprecher) beim Telefonieren strafbar?

Es ist grundsätzlich unzulässig, die "Lauthöreinrichtung" beim Telefonieren einzuschalten, ohne dies gegenüber dem Gesprächspartner rechtzeitig und eindeutig anzukündigen (vgl. 1. Tätigkeitsbericht Nr. 5.1.3).

Jemand informierte mich darüber, daß eine Staatsanwaltschaft ein Strafverfahren "wegen Verletzung der Vertraulichkeit des Wortes" (§ 201 Abs. 2 StGB) *eingestellt* habe, obwohl feststand, daß ein Gemeindebediensteter - für den Betroffenen nicht erkennbar - beim Telefonieren die Lauthöreinrichtung eingeschaltet hatte.

Ich habe dem Petenten mitgeteilt, daß nicht jeder Rechtsverstoß auch *strafrechtlich relevant ist*:
Eine Bestrafung ist nur dann möglich, wenn dies ausdrücklich in einem Gesetz (z. B. im Strafgesetzbuch) vorgesehen ist. Das ist beim unzulässigen Einschalten der Lauthörvorrichtung nicht der Fall. Die Vorschrift des § 201 Abs. 2 StGB, die als *einzige mögliche Strafvorschrift* in Betracht kommen könnte, verlangt nämlich, daß das nicht öffentlich gesprochene Wort mit einem besonderen *Abhörgerät* abgehört wird. Hierzu zählen beispielsweise versteckt angebrachte Mikrofone oder Vorrichtungen zum unbefugten "Anzapfen" von Telefonleitungen. Das Mithören eines Telefongesprächs mittels eingeschalteter Lauthöreinrichtung sollte hingegen nach dem Willen des Gesetzgebers nicht nach § 201 Abs. 2 StGB strafbar sein (vgl. BVerfG NJW 1982, 1398). Das "Lauthören" ist unverschämt, aber nicht strafbar.

9 Wirtschaft und Arbeit

9.1 Straßenverkehrswesen

9.1.1 Verwertung strafrechtlicher Verurteilungen, die sowohl im Bundeszentralregister als auch im Verkehrszentralregister getilgt sind, durch die Fahrerlaubnisbehörden

Sind Eintragungen über strafrechtliche Verurteilungen im Bundeszentralregister *getilgt*, dürfen die Verurteilungen nicht mehr zum Nachteil des Betroffenen verwertet werden (vgl. § 51 Abs. 1 BZRG). Eine Ausnahme hiervon sieht § 52 Abs. 2 BZRG für Verfahren zur Erteilung oder Entziehung einer Fahrerlaubnis vor, wenn die Verurteilung in das Verkehrszentralregister einzutragen war. Diese Taten können (nach dem Gesetzeswortlaut) zeitlich unbegrenzt zum Nachteil des Betroffenen verwertet werden.

Meine Auffassung, daß es bedenklich sei, wenn einem Führerscheinbewerber im BZR bereits getilgte und mehr als zehn Jahre alte Verurteilungen im Rahmen der *Eignungsprüfung* vorgehalten würden, wird von anderen Datenschutzbeauftragten geteilt. Es stellt sich nämlich die Frage, ob § 52 Abs. 2 BZRG bei der Eignungsprüfung zur Erteilung einer Fahrerlaubnis überhaupt anzuwenden ist. Meine Bedenken beruhen auf folgenden Überlegungen:

Das Verfahren, *wie* die Fahrerlaubnisbehörde ermittelt, ob ein Führerscheinbewerber zum Führen von Kraftfahrzeugen geeignet ist, ergibt sich grundsätzlich *abschließend* aus der Straßenverkehrszulassungsordnung und dem Straßenverkehrsgesetz (z. B. Sehtest gemäß § 9a StVZO; bei Verdacht auf "Neigung zum Trunk" Vorlage eines "MPU"-Gutachtens gemäß § 12 Abs. 1 StVZO etc.).

Zur Ermittlung, ob der Antragsteller "bereits strafrechtlich in Erscheinung getreten" ist, sieht die Straßenverkehrszulassungsordnung zwei Möglichkeiten vor:
Einerseits kann die Fahrerlaubnisbehörde gemäß § 13c StVZO zur Feststellung, ob der Führerscheinbewerber Straftaten oder Ordnungswidrigkeiten *im Zusammenhang mit dem Straßenverkehr* begangen hat, beim Kraftfahrt-Bundesamt Auskunft aus dem VZR verlangen. Das Bundesverwaltungsgericht hat bereits im Jahre 1977 entschieden (NJW 1977, 1075), daß das VZR *die allein maßgebende Erfassungs- und Auskunftsstelle* der für die Belange der Verkehrssicherheit bedeutsamen gerichtlichen und verwaltungsbehördlichen Entscheidungen sein soll. Andererseits kann die Behörde gemäß § 8 Abs. 3 StVZO die Vorlage eines Führungszeugnisses verlangen, in dem auch Straftaten *ohne* Verkehrsbezug vermerkt sind.
Für im VZR gespeicherte Entscheidungen sind die in § 13a StVZO genannten Tilgungsfristen *für die Verwertbarkeit dieser Straftaten* zu beachten. Der Gesetzgeber wollte klarstellen, daß eine strafrechtliche Verurteilung den Betroffenen gerade nicht zeitlich unbegrenzt vorgehalten werden soll (sogenannter "Bewährungsgedanke"). Eine auf § 52 Abs. 2 BZRG gestützte, zeitlich nicht beschränkte Verwertung von Verurteilungen, die beispielsweise aus bei den Behörden geführten Karteien ersichtlich sein können (z. B. Erkenntnisse aus anderen Verfahren), liefe diesem Zweck zuwider.

Daß ein Rückgriff auf im Bundeszentralregister getilgte Verurteilungen bei der Eignungsprüfung nicht stattfinden soll, zeigt sich auch darin, daß der Gesetzgeber in § 8 Abs. 3 StVZO "lediglich" die Vorlage eines *Führungszeugnisses* bei der Fahrerlaubnisbehörde vorgesehen hat. Im BZR getilgte Verurteilungen sind aus Führungszeugnissen nicht mehr ersichtlich. Wenn aber getilgte Verurteilungen im Rahmen der Eignungsprüfung eines Führerscheinbewerbers keine Relevanz haben sollen, würde diese Zielsetzung durch Verwertung von aus anderen Verfahren bekannten, aber tilgungsreifen Verurteilungen unterlaufen.

Da § 52 Abs. 2 BZRG - wie dargelegt - nicht mit den Vorschriften und Zielsetzungen der Straßenverkehrszulassungsordnung in Einklang steht, habe ich angeregt, daß der Bundesbeauftragte für den Datenschutz auf die Streichung der Vorschrift aus dem Bundeszentralregistergesetz hinwirkt.

9.1.2 Dürfen Fahrerlaubnisbehörden bei der Ermittlung von Tatsachen im Rahmen der Eignungsprüfung Anfragen an die Polizei bzw. Staatsanwaltschaft zu laufenden Ermittlungsverfahren richten?

Fahrerlaubnisbehörden haben vor Erteilung einer Fahrerlaubnis umfassend zu prüfen, ob Fahrerlaubnisbewerber zum Führen von Kraftfahrzeugen im Straßenverkehr geeignet sind. Mehrere Fahrerlaubnisbehörden stellten die Frage, ob sie deshalb bei der Staatsanwaltschaft oder der Polizei zu laufenden Ermittlungsverfahren anfragen dürfen:

Anfragen von Fahrerlaubnisbehörden bei Strafverfolgungsbehörden sind im Rahmen der Eignungsprüfung eines Fahrerlaubnisbewerbers weder im Straßenverkehrsgesetz noch in der Straßenverkehrszulassungsordnung vorgesehen. Sie könnten daher allenfalls aufgrund der (*in Ausnahmefällen* für die Ermittlungstätigkeit der Fahrerlaubnisbehörden anwendbaren) allgemeinen polizeilichen Generalklausel zulässig sein. Allerdings ist bei Anfragen *zu laufenden Ermittlungsverfahren* die (auf dem Rechtsstaatprinzip folgende) *Unschuldsvermutung* zu beachten (vgl. BVerfG NJW 1987, 2427 und Art. 6 Abs. 2 Europäische Menschenrechtskonvention). Hiernach gilt jeder Mensch bis zu seiner *rechtskräftigen Verurteilung* als unschuldig. Die Nichteignung eines Fahrerlaubnisbewerbers darf daher nicht ausschließlich auf die Tatsache gestützt werden, daß gegen ihn ein Ermittlungsverfahren läuft. Dieser Rechtslage entsprechen § 13 c StVZO und § 8 Abs. 3 StVZO, wonach ausschließlich *rechtskräftige Strafurteile* (und damit keine Daten aus Ermittlungsverfahren) zur Frage der Eignung von Fahrerlaubnisbewerbern herangezogen werden dürfen.

9.1.3 Zu den Voraussetzungen einer einfachen Auskunft aus dem Fahrzeugregister

Ein Kfz-Halter hat sich darüber beschwert, daß eine Zulassungsstelle seinen Namen und seine Anschrift an einen Dritten auf Anfrage weitergegeben habe, obwohl - wie der Petent sich ausdrückte - "er sich im Straßenverkehr stets vorbildlich verhalten habe". Die Eingabe veranlaßte mich, den Petenten über die Voraussetzungen einer sogenannten "einfachen Registerauskunft" zu unterrichten:

Einfache Auskünfte aus dem Fahrzeugregister sind gemäß § 39 Abs. 1 StVG zulässig, wenn der Antragsteller *darlegt*, daß er die Halterdaten zur Geltendmachung, Sicherung oder Vollstreckung oder zur Abwehr von Rechtsansprüchen im Zusammenhang mit der Teilnahme am Straßenverkehr oder zur Erhebung einer (strafrechtlichen) Privatklage wegen im Straßenverkehr begangener Verstöße benötigt. "Darlegen" bedeutet, daß der Auskunftssuchende schlüssig und widerspruchsfrei einen Sachverhalt schildern muß, aus dem sich die genannten Rechtsfolgen ergeben können. Soweit Schadensersatzansprüche in Betracht kommen, sind möglichst auch Zeitpunkt (Datum und Uhrzeit) und Ort des behaupteten schadensbegründenden Ereignisses anzugeben.

Die Zulassungsstelle hat korrekt gehandelt.

9.1.4 Zu den Anforderungen an ein Aufforderungsschreiben zur Vorlage eines fachärztlichen Gutachtens

Meinen Feststellungen zufolge herrscht unter den sächsischen Fahrerlaubnisbehörden Unsicherheit, wie Anforderungsschreiben zur Vorlage eines fachärztlichen Gutachtens im Rahmen der Eignungsprüfung von Fahrerlaubnisbewerbern zu gestalten sind:

Nach der Rechtsprechung des Bundesverwaltungsgerichts (BVerwGE 34, 248) ist die Aufforderung an den Fahrerlaubnisbewerber, ein fachärztliches Gutachten beizubringen, kein *Verwaltungsakt* gemäß § 35 Abs. 1 VwVfG, sondern eine "unselbständige Maßnahme der Beweiserhebung". Trotzdem muß die Fahrerlaubnisbehörde die Gründe, die aus ihrer Sicht gegen die Eignung des Bewerbers sprechen, in dem Aufforderungsschreiben mitteilen. Nur dann kann der Betroffene den (von ihm gewählten) Gutacher ausreichend informieren und damit erreichen, daß dieser ein *aussagekräftiges* Gutachten erstellen kann.

9.1.5 Unzulässige Weitergabe von Behördenschriftwechsel an den Vorgesetzten eines Antragstellers

Im Zusammenhang mit der Ausstellung eines internationalen Führerscheins führte der Antragsteller, selbst im öffentlichen Dienst beschäftigt, einen umfangreichen Schriftwechsel. Die Führerscheinstelle wußte sich wohl nicht anders gegen die Schreibwut des Betroffenen zu wehren und unterrichtete dessen unmittelbaren Vorgesetzten telefonisch und durch Übersendung des gesamten Schriftwechsels mit dem Hintergedanken, auf diese Weise dem ihr lästigen Verhalten ein Ende zu bereiten.

Das hätte die Behörde nicht tun dürfen. Der Antragsteller hat nämlich als Beteiligter eines Verwaltungsverfahrens (siehe §§ 9 ff. VwVfG) Anspruch auf Geheimhaltung nach § 30 VwVfG. Außerdem verbietet § 6 SächsDSG (Datengeheimnis) die unbefugte Verarbeitung oder sonstige Verwendung personenbezogener Daten.

9.1.6 Gebühren für Registerauskünfte an den Betroffenen?

Bereits im 2. Tätigkeitsbericht (Nr. 9.1.1) habe ich die Schwerpunkte meiner Stellungnahme zum Entwurf zur Änderung des Straßenverkehrsgesetzes dargestellt. Im Berichtszeitraum lagen mir weitere, den ersten Entwurf ergänzende Referentenentwürfe des Bundes zur datenschutzrechtlichen Bewertung vor. Nach einer Vorschrift sollten auch *dem Betroffenen selbst* erteilte Registerauskünfte gebührenpflichtig sein. Das Erheben von Gebühren von dem Betroffenen ist meines Erachtens geeignet, diesen davon abzuhalten, seinen durch das Grundrecht auf informationelle Selbstbestimmung *gewährleisteten* Auskunftanspruch ("Jeder muß wissen können, wer, was, wann über ihn weiß.") geltend zu machen. Ich habe den Bundesbeauftragten für den Datenschutz und das SMWA gebeten, den Verzicht auf eine Gebührenfestsetzung in solchen Fällen zu fordern.

9.1.7 Einholung eines fachärztlichen Gutachtens auf Verlangen der Fahrerlaubnisehörde bei Erteilung einer Fahrerlaubnis zur Fahrgastbeförderung

Nach § 15 e Abs. 1 Nr. 3 c StVZO muß derjenige, der eine Fahrerlaubnis zur Fahrgastbeförderung beantragt, auf Verlangen der Fahrerlaubnisbehörde seine körperliche Eignung durch ein fachärztliches Gutachten nachweisen. Der Datenschutzbeauftragte eines anderen Bundeslandes hat hierzu die Auffassung vertreten, daß es den gesetzlichen Anforderungen genüge, wenn die Fahrerlaubnisbehörden lediglich das *Ergebnis* der ärztlichen Untersuchung im Rahmen der Eignungsprüfung erhielten. Dieser Auffassung vermag ich nicht zu folgen:

Im Gegensatz zu § 9 c Abs. 1 StVZO, der lediglich die *Beibringung* einer ärztlichen *Bescheinigung* für Fahrerlaubnisbewerber der Klasse 2 vorschreibt, verlangt § 15 e Abs. 1 Nr. 3 c StVZO den *Nachweis* der Eignung *durch* ein fachärztliches *Gutachten*. Dies ist ein deutlicher qualitativer Unterschied, den der Gesetzgeber meines Erachtens *bewußt* zum Ausdruck gebracht hat.

Die Formulierung in § 15 e Abs. 1 Nr. 3 c StVZO orientiert sich nämlich an §§ 12 Abs. 1, 15 b Abs. 1 StVZO. Im Anwendungsbereich dieser Vorschriften ist allgemein anerkannt, daß der *Betroffene* den Fahrerlaubnisbehörden das *Gutachten* (und nicht nur das Ergebnis) zur Eignungsprüfung vorzulegen hat. Nur in diesem Fall können die Behörden das ihnen eingeräumte Ermessen zur Frage der Eignung sachgerecht ausüben. Dieser Gedanke trifft auch auf die Eignungsprüfung von Bewerbern zu, die eine Fahrerlaubnis zur Fahrgastbeförderung beantragt haben.

9.1.8 Beibringung eines Gutachtens einer amtlichen anerkannten medizinisch-psychologischen Untersuchungsstelle gemäß § 15 f Abs. 2 Nr. 2 c StVZO

Nach einer Verwaltungsvorschrift des SMWA müssen Inhaber einer Fahrerlaubnis zur Fahrgastbeförderung der Fahrerlaubnisbehörde ab dem 50. Lebensjahr - als ob man dann ein "alter Knacker" sei - ein Gutachten einer amtlichen anerkannten medizinisch-psychologischen Untersuchungsstelle vorlegen. Anderenfalls wird die Fahrerlaubnis nicht verlängert.

Diese Verfahrensweise steht meines Erachtens mit § 15 f Abs. 2 Nr. 2 c StVZO und der neuen Rechtsprechung des Bundesverfassungsgerichts (NJW 1993, 2365) nicht in Einklang:

Gemäß § 15 f Abs. 2 Nr. 2 c StVZO *kann* die Behörde ("auf Verlangen") den Nachweis der Eignung durch Vorlage eines fachärztlichen Gutachtens *oder* eines Gutachtens einer amtlichen anerkannten medizinisch-psychologischen Untersuchungsstelle (MPU-Gutachten) fordern. Die Entscheidung, *ob* sie ein Gutachten und gegebenenfalls *welches* Gutachten (MPU oder fachärztliches) sie verlangt, steht also im *Ermessen* der Behörde. Da es eine *Vermutung* der Nichteignung zur Fahrgastbeförderung ab einem bestimmten Lebensalter, die *nur* durch Vorlage eines MPU-Gutachtens widerlegt werden kann, nicht gibt, würde die Anwendung der Verwaltungsvorschrift zwangsläufig zu einer Ermessensfehlentscheidung der Behörde führen.

Vielmehr ist nach der Rechtsprechung des Bundesverfassungsgerichts (a.a.O.) vor Anforderung eines MPU-Gutachtens stets zu prüfen, ob *tatsächliche Feststellungen* einen Eignungsmangel als naheliegend erscheinen lassen (Einzelfallprüfung) und, ggf., ob Eignungszweifel nicht durch einen "schonenderen" Eingriff in das Persönlichkeitsrecht des Einzelnen (also durch Vorlage eines fachärztlichen Gutachtens) behoben werden können (Grundsatz der Verhältnismäßigkeit).

Meiner Auffassung nach wäre ein der Verwaltungsvorschrift folgendes Handeln nicht von § 15 f Abs. 2 Nr. 2 c StVZO gedeckt und griffe daher mangels gesetzlicher Grundlage (vgl. Art. 33 S. 3 SächsVerf) unzulässig in das Grundrecht der Betroffenen auf informationelle Selbstbestimmung ein.

Beim SMWA habe ich daher die Streichung der Verwaltungsvorschrift angeregt. Das SMWA hat mich daraufhin darüber informiert, daß die Rechtmäßigkeit der inhaltsgleichen bayerischen Verwaltungsvorschrift derzeit vom Bundesverwaltungsgericht geprüft wird. Bis zum Ausgang dieses Verfahrens wird das SMWA nicht auf Einhaltung der Verwaltungsvorschrift "drängen". Hiermit habe ich mich einstweilen einverstanden erklärt.

Vgl. ferner oben Abschnitt 5.11.3.

9.2 Offene Vermögensfragen

Weiterhin kommen mir Fälle zur Kenntnis, in denen der Verdacht einer rechtswidrigen Datenübermittlung aus dem Bereich der Ämter zur Regelung offener Vermögensfragen an private Interessenten, die auf dem Grundstücksmarkt tätig sind, auf der Hand liegt. Es ist aber sehr schwer, die Vorgänge aufzuklären. Manchmal ist auch nicht auszuschließen, daß die ursprüngliche rechtswidrige Übermittlung in den privaten Bereich schon lange zurückliegt, also in die erste Aufbauzeit der Vermögensämter fällt und schon deswegen nicht mehr aufgedeckt werden kann. Dann sind Nachforschungen bei den privaten Dateninhabern der einzige Weg, die Vorgänge doch noch aufzuhellen und etwas zugunsten des Betroffenen zu bewirken. Um so bedauerlicher ist es, wenn die insoweit zuständigen Stellen, also das SMI und das jeweils örtlich zuständige Regierungspräsidium mich - und damit ja vor allem den Betroffenen, und übrigens anders als die betreffenden Vermögensämter - überlang auf die Antwort warten lassen: In einem Fall bin ich gespannt, ob ich nach einem vollen Jahr eine schriftliche Nachricht des SMI erhalten haben werde, die mehr ist als ein ('nicht-qualifiziertes') Vertröstungsschreiben.

10 Soziales und Gesundheit

10.1 Gesundheitswesen

10.1.1 Inkrafttreten des Sächsischen Heilberufekammergesetzes

Im Berichtszeitraum trat das SächsHKaG in Kraft. Über meine Bemühungen zur datenschutzgerechten Gestaltung des berufsgerichtlichen Verfahrens habe ich im 2. Tätigkeitsbericht unter 10.1.9 dargestellt. Das zuständige SMS und der Gesetzgeber haben meine Anregungen aufgegriffen und damit insbesondere im Bereich des Ausschlusses der Öffentlichkeit im berufsgerichtlichen Verfahren (§ 53 Abs. 2 SächsHKaG) und hinsichtlich der anonymisierten Erörterung personenbezogener Daten, die einem Berufsgeheimnis unterliegen, eine vorbildliche Regelung geschaffen.

10.1.2 Krebsregistergesetze

Einigermaßen überraschend haben sich Bundestag und Bundesrat trotz aller Schwierigkeiten doch noch rechtzeitig vor dem Ablauf der Geltungsdauer des *Gesetzes zur Sicherung und vorläufigen Fortführung der Datensammlungen des 'Nationalen Krebsregisters' der ehemaligen Deutschen Demokratischen Republik* (Krebsregistersicherungsgesetz) auf eine neue bundesgesetzliche Regelung einigen können: das *Gesetz über Krebsregister* (Krebsregistergesetz) vom 4. November 1994. Es steckt für die Zeit bis Ende des Jahrzehnts den Rahmen für eine schrittweise Einführung epidemiologischer Krebsregister durch *alle* Bundesländer ab. Vor allem bringt es eine insbesondere in datenschutzrechtlicher Hinsicht verbesserte Regelung, namentlich (vgl. meinen 2. Tätigkeitsbericht unter 10.1.4) die Aufteilung in eine unter ärztlicher Leitung stehende *Vertrauensstelle*, welche, u. a., die ihr gemeldeten Identitäts-Daten des Patienten nach einem sogenannten asymmetrischen Chiffrierverfahren verschlüsselt und an die von ihr abgeschottete *Registerstelle* übermittelt (vgl. §§ 4-7 KRG).

Was die Meldevoraussetzungen (sog. Meldemodus) betrifft, *erlaubt* das Gesetz den Ärzten die Meldung (§ 3 Abs. 1 Satz 1 KRG), verpflichtet sie in den Grenzen des medizinisch Angezeigten zur frühestmöglichen Unterrichtung des Patienten von der erfolgten oder beabsichtigten Meldung (§ 3 Abs. 1 Satz 1 1. Halbs., Satz 3 KRG) und gibt dem Patienten ein Recht, die Beseitigung bzw. Unterlassung der Datenverarbeitung zu verlangen, über das er vom Arzt auch aufgeklärt werden muß (§ 3 Abs. 2 Sätze 2, 4 und 6 KRG).

Das Gesetz sieht die Möglichkeit vor, daß der Meldemodus von den Ländern abweichend geregelt wird: § 1 Abs. 4 i. V. m. § 13 Abs. 5 KRG.

Während in den alten Bundesländern überwiegend insoweit epidemiologischer Nachholbedarf besteht, hat Sachsen, wie die anderen östlichen Bundesländer und im praktischen Verbund mit diesen, bekanntlich auf der Grundlage des erwähnten Krebsregistersicherungsgesetzes und des Sächsischen Krebsregistergesetzes vom 19. Juli 1993 das Krebsregister aus DDR-Zeiten fortgeführt. Eine solche - kostensparende -

gemeinsame Fortsetzung des in Berlin angesiedelten gemeinsamen Krebsregisters haben die östlichen Bundesländer dann mit Wirkung vom 1. Januar 1995 durch ein neues Verwaltungsabkommen geregelt, dessen Ausgestaltung ich sowohl im Verein mit den anderen betroffenen Datenschutzbeauftragten als auch unmittelbar über das SMS zu beeinflussen versucht habe.

Viel wichtiger wird sein, wie der sächsische Gesetzgeber den Spielraum nutzen wird, den das Bundesgesetz bietet. Die Haltung, die ich dazu einnehme, habe ich im 1. und 2. Tätigkeitsbericht ausführlich dargelegt. In meinen Bedenken gegen institutionalisierte Datenverarbeitungen, welche von der öffentlichen Gewalt ('strukturell') durchweg und der Idee nach flächendeckend auf der Grundlage einer beim Betroffenen einzuholenden *Einwilligung* eingerichtet werden (vgl. dazu in meinem 2. Tätigkeitsbericht a. a. O.), sehe ich mich durch Erfahrungen auf anderen Gebieten (nachstehend unter 11.1) bestätigt.

Auch auf die Gefahr hin, daß nicht nur meine Kollegen in anderen Bundesländern mir widersprechen, sondern daß auch Teile der Staatsregierung, die für das Gesundheitswesen keinerlei Verantwortung tragen, auf diesem Gebiet ausnahmsweise den Datenschutz hochhalten und mir erneut die Einwilligungslösung als den einzigen verfassungsmäßigen Weg vorhalten: Ich bin, unverändert, für eine einwilligungsunabhängige Melde*pflicht* der Ärzte. Die Menschenwürde gebietet es, dem - ohnehin schwer betroffenen - Patienten und seinem um möglichst schonende Behandlung ringenden Arzt die schwere Belastung eines Gesprächs darüber zu ersparen, ob der Arzt die Krankheit und ihre Behandlung meldet oder nicht. Das Zauberwort vom "mündigen Patienten" entpuppt sich in dieser Situation als Leerformel. Der Patient ist in erster Linie nicht mündig, sondern krank.

Ich hoffe, daß der Sächsische Gesetzgeber das Feingefühl hat, dies zu erkennen und die generelle Meldepflicht vorsieht. Nur so - und das kommt hinzu - wird ein hoher Meldegrad garantiert, der eine gute wissenschaftlich-epidemiologische Auswertung ermöglicht.

10.1.3 Aufbewahrung von Patientenunterlagen aufgelöster Polikliniken

Anläßlich eines Informations- und Beratungsbesuchs in einem Kreiskrankenhaus machte mich der Hausmeister auf ein Archiv im Keller aufmerksam. In diesem Raum wurden zahlreiche Patientenunterlagen gelagert, insbesondere Röntgenfilme einer nahegelegenen, aber nach der Wende aufgelösten ehemaligen Poliklinischen Abteilung für Lungenkrankheiten und Tuberkulose (PALT). Überdies fand ich noch weitere, bisher unbekannte Patientenunterlagen. Außerdem erfuhr ich, daß die Poliklinik früher 47 Außenstellen unterhielt. Es besteht daher die Gefahr, daß weitere herrenlose Archive seit der Abwicklung bzw. Auflösung der Polikliniken und ihrer Außenstellen existieren.

In solchen Altbeständen von Patientenunterlagen befinden sich häufig Unterlagen, die für eine erfolgreiche Weiterbehandlung der betroffenen Patienten, aber auch für Rentenansprüche, z. B. bei Unfallrenten, entscheidend sind. Wichtig sind sowohl ein schneller Zugriff der Patienten und Sozialleistungsträger als auch die sichere Aufbewahrung.

Die in einer Beratung mit dem SMS und SMI vorgesehene gemeinsame Empfehlung zur Meldung, Aufbewahrung und Nutzung von Patientenunterlagen und Zentralkarteien mit medizinischem Inhalt aus ehemaligen Gesundheitseinrichtungen der DDR und eine entsprechende Informationsschrift für die Bürger (siehe 10.1.3 im 2. Tätigkeitsbericht) sind jedoch noch immer nicht fertiggestellt.

Einige Kommunen haben sich mittlerweile entschlossen, die vorliegenden Patientenunterlagen mit einem (in Berlin schon erprobten) PC-Projekt zu registrieren. Dieses Projekt "Archivierung von Patientenunterlagen aus aufgelösten ambulanten medizinischen Einrichtungen des DDR-Gesundheitswesens im Freistaat Sachsen" erleichtert und beschleunigt die Suche nach dem Fundort der gewünschten Akte. Eingesetzt werden vor allem arbeitslose Frauen, die früher im Gesundheitsbereich tätig waren.

Bei Verwirklichung der von § 9 SächsDSG geforderten Maßnahmen und einer Verpflichtung auf das Datengeheimnis (§ 6 SächsDSG) durch die Kommune oder den Landkreis ist das Projekt zu begrüßen.

Um den Interessenten die Einführung des Projekts zu erleichtern und zugleich eine datenschutzgerechte Verfahrensweise zu sichern, habe ich die Ausarbeitung eines detaillierten Organisationsprojekts, angepaßt an die sächsischen Besonderheiten, angeregt, die auch im Rahmen einer Arbeitsbeschaffungsmaßnahme erfolgen kann.

10.1.4 Übermittlung von Todesbescheinigungen durch das Gesundheitsamt an Berufsgenossenschaften

Todesbescheinigungen enthalten eine Reihe vertraulicher Daten des Verstorbenen. Diese werden zwar nicht mehr vom Recht auf informationelle Selbstbestimmung geschützt - Träger des Grundrechts kann nur ein Lebender sein -, die ärztliche Schweigepflicht (vgl. § 203 Abs. 4 StGB) und der "postmortale Persönlichkeitsschutz" (hergeleitet aus Art. 1 Abs. 1 GG) stellen jedoch auch nach dem Tode eines Menschen sicher, daß dessen Daten nicht unbeschränkt verarbeitet werden dürfen.

Zur Frage, ob und unter welchen Voraussetzungen Daten aus Todesbescheinigungen an Berufsgenossenschaften übermittelt werden dürfen, berichtete mir eine sächsische Stadt: Das städtische Gesundheitsamt verlange von der auskunftsbegehrenden Berufsgenossenschaft vor einer Übermittlung von Todesbescheinigungsdaten unter Hinweis auf § 4 Abs. 1 Nr. 2 SächsDSG (Einwilligung des Betroffenen in die Datenverarbeitung) die Vorlage einer schriftlichen Einwilligungserklärung der Angehörigen des Verstorbenen. In den meisten Fällen werde diese von der Berufsgenossenschaft nicht vorgelegt. Um die Ansprüche der Hinterbliebenen (auf Zahlung einer Rente) nicht auf Monate oder gar Jahre zu blockieren, erteile der Mitarbeiter des Gesundheitsamtes schließlich unter Hinweis auf § 13 Abs. 3 Satz 3 SächsDSG (Einwilligung des Schweigepflichtigen bei Zweckänderung von Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen) seine Einwilligung zur Übermittlung der Daten.

Hierzu habe ich wie folgt Stellung genommen: In Sachsen besteht seit dem 30. Juli 1994 eine gesetzliche Offenbarungsbefugnis für Daten aus Todesbescheinigungen. § 14 Abs. 5 des an diesem Tage in Kraft getretenen Bestattungsgesetzes sieht Einsicht oder Auskunft vor, wenn jemand ein berechtigtes Interesse an der Kenntnis der Todesumstände einer namentlich bestimmten Person glaubhaft macht und kein Grund zur Annahme besteht, daß durch die Offenbarung schutzwürdige Belange des Verstorbenen oder seiner Hinterbliebenen beeinträchtigt werden. Diese Voraussetzungen werden bei der Anfrage einer Berufsgenossenschaft in der Regel erfüllt sein. Berufsgenossenschaften sind Träger der Unfallversicherung (vgl. §§ 646 f. RVO) und damit Sozialleistungsbehörden (§ 1 SGB X). Als Sozialleistungsbehörden sind sie datenschutzrechtlich nicht private, sondern "öffentliche Stellen". Eines Rückgriffs auf den ansonsten durchaus in Betracht kommenden § 13 SächsDSG (Übermittlung an öffentliche Stellen) bedarf es aber wegen des § 14 Abs. 5 Satz 3 Nr. 1 BestG nicht.

Das Gesundheitsamt muß also prüfen, ob im Einzelfall tatsächlich kein Grund zu der Annahme besteht, daß durch die Offenbarung schutzwürdige Belange des Verstorbenen beeinträchtigt werden. Ferner muß das Gesundheitsamt prüfen, ob die Berufsgenossenschaft alle Angaben aus dem vertraulichen Teil der Todesbescheinigung zur Durchführung ihrer Aufgaben benötigt. Zur Feststellung etwa einer Berufskrankheit als Todesursache werden in der Regel Angaben zu den vorhergegangenen Krankheiten und zur unmittelbaren Todesursache erforderlich sein. Die restlichen Angaben, etwa zu den "sicheren Zeichen des Todes", können geschwärzt werden.

Ich werde die weitere Entwicklung auf diesem sensiblen Gebiet im Auge behalten. Dies betrifft vor allem die nach § 24 BestG vorgesehenen Rechtsverordnungen (Abs. 1) und Verwaltungsvorschriften (Abs. 3). So habe ich etwa in guter Zusammenarbeit mit dem SMS einer Regelung zustimmen können, die vorsieht, den Umschlag des bei der Leiche verbleibenden Exemplars der Todesbescheinigung mit dem Namen und dem Sterbedatum des Verstorbenen zu versehen. Das Bestattungsgesetz sah insofern eine Beschriftung des Umschlags des dritten Blattes weder in § 14 (Todesbescheinigung) noch in Anlage 1 zu § 14 Abs. 1 ("Hinweise zur Todesbescheinigung") vor. Eine Kennzeichnung des Umschlages von Blatt 3 der Todesbescheinigung war jedoch dringend geboten, um Verwechslungen von beiden bei der Bestattung auszuschließen. Ich habe mich deshalb mit einer entsprechenden Anwendung der für die Blätter 1 und 2 der Todesbescheinigung vorgesehenen Verfahrensweise einverstanden erklärt.

10.1.5 Meldung eines Erkrankungs- bzw. Todesfalles von humaner spongiformer Enzephalopathie

Die Fälle des "Rinderwahnsinns" und die Möglichkeit der Übertragung ähnlicher Erreger auf den Menschen beschäftigen die Öffentlichkeit seit längerem. Eine Rechtsgrundlage für die Erhebung von Daten über das Auftreten übertragbarer Formen dieser Krankheit beim Menschen ist sicher nötig. Der Bundesgesundheitsminister hat deshalb auf dem Verordnungswege den Katalog der nach dem Bundesseuchengesetz meldepflichtigen Krankheiten erweitert und bestimmte Formblätter für die Meldung vorgeschrieben. Den behandelnden Arzt trifft nunmehr die Pflicht, einen Menschen, der an "Rinderwahnsinn" erkrankt oder gestorben ist, namentlich dem Gesundheitsamt zu melden. Der Arzt benutzt zur Meldung die vorgeschriebenen Formblätter oder meldet mündlich. In diesem Fall werden die Angaben in das vorgeschriebene Formblatt übertragen. Anschließend hat das Gesundheitsamt die Meldung *in anonymisierter Form* über die zuständigen Landesbehörden an das Robert-Koch-Institut, eine Bundeseinrichtung in Berlin, weiterzuleiten.

Die für die Übermittlung in "anonymisierter Form" vorgesehene "Durchschrift (des Meldeformulars) für die zuständige Landesbehörde" stellt jedoch die Anonymität nicht ausreichend sicher. Aus den nicht durch einen Schlüssel vorgegebenen, sondern als Freitext einzutragenden Angaben zum Beruf in Verbindung mit den ersten drei Stellen der Postleitzahl, dem Geburtsmonat und -jahr sowie aus seltenen Staatsangehörigkeiten können sich in Einzelfällen, unter Umständen durch Einbeziehung entsprechenden Zusatzwissens, Hinweise auf bestimmte Personen ergeben.

"Anonymisieren" ist gemäß § 3 Abs. 2 Nr. 4 SächsDSG das Verändern personenbezogener Daten in der Weise, daß sie *nicht mehr* einer bestimmten oder bestimmbaren Person zugeordnet werden können. Ein Re-Identifikations-Risiko muß daher sicher ausgeschlossen werden können. Es besteht vor allem durch die Angabe des Berufs des Erkrankten oder Verstorbenen. Soweit hier der Beruf im Sinne des Wortes nicht allgemein ("Jurist", "Arzt" etc.), sondern mit konkreter Funktionsbezeichnung (z. B. "Landrat", "Amtsarzt" etc.) angegeben wird, ist zusammen mit der dreistelligen Postleitzahl keine Anonymisierung sichergestellt.

Die Gesundheitsämter müssen darüber unterrichtet werden und durch geeignete organisatorische Maßnahmen sicherstellen, daß als Berufsangabe keine Funktionsbezeichnungen verwendet werden. Bereits gespeicherte Funktionsbezeichnungen müssen gelöscht und durch eine Berufsangabe im oben genannten Sinne ersetzt werden. Auch muß die nächste Auflage des Meldebogens entsprechend geändert werden. Dies habe ich dem SMS als zuständiger Landesbehörde mitgeteilt.

10.1.6 Entwurf einer Meldeordnung der Sächsischen Landesärztekammer

Jeder Arzt, der im Freistaat Sachsen seinen Beruf ausübt oder, falls er seinen Beruf nicht ausübt, hier seine Hauptwohnung hat, muß sich gemäß § 3 Abs. 1 SächsHKaG innerhalb eines Monats bei der Sächsischen Landesärztekammer melden. *Diese kann in einer Meldeordnung das Nähere über das Meldeverfahren regeln und die zur Überwachung der*

Berufspflichten erforderlichen Angaben und Nachweise, die Gegenstand der Meldung sein sollen, festlegen (§ 3 Abs. 2 SächsHKaG).

Die sächsische Landesärztekammer hat mir frühzeitig den Entwurf ihrer Meldeordnung zur Stellungnahme übersandt.

Ich habe - ebenso wie gegenüber der Tierärztekammer, in deren Bereich ich mit einem ähnlichen Vorgang befaßt bin (vgl. 10.3.1) - auch gegenüber der Landesärztekammer darauf hingewiesen, daß "erforderlich" im Sinne des § 3 Abs. 2 SächsHKaG nur diejenigen Angaben sind, ohne deren Kenntnis die Erfüllung der Berufspflichten schlechterdings nicht überwacht werden könnte. So hatte ich z. B. zunächst Bedenken gegen die vorgesehene Frage nach der Art der ausgeübten ärztlichen Tätigkeit, insbesondere danach, ob der Arzt niedergelassen, angestellt oder beamtet ist.

Die Landesärztekammer hat mir gegenüber umfassend und in einer für die Belange des Datenschutzes aufgeschlossenen Haltung Stellung genommen. So liegt z. B. der Frage nach dem jeweiligen Status des Arztes eine disziplinarrechtlich unterschiedliche Behandlung von niedergelassenen, angestellten oder beamteten Ärzten im berufsgerichtlichen Verfahren nach § 50 SächsHKaG zugrunde. Darüber hinaus war z. B. diese Frage auch erforderlich, weil bestimmte Regelungen im Sächsischen Heilberufekammergesetz und in der Berufsordnung nur auf den angestellten oder niedergelassenen Arzt anzuwenden sind (z. B. nehmen nur ambulant tätige Ärzte am ärztlichen Notfalldienst teil). Diese Begründung kann ich ebenso wie die übrigen Ausführungen der Landesärztekammer in dieser Angelegenheit nachvollziehen.

Ich freue mich darauf, die auch ansonsten gute und fruchtbare Zusammenarbeit mit der Landesärztekammer in dem datenschutzrechtlich sensiblen Bereich ärztlicher Tätigkeiten fortzuführen.

10.1.7 Vorlage eines "polizeilichen Führungszeugnisses" für die Zulassung als Vertragsarzt bei der Kassenärztlichen Vereinigung

Kassenärztliche Vereinigungen (§ 77 SGB V) sind die Zusammenschlüsse der als Vertragsärzte - früher sprach man von "Kassenärzten" - zugelassenen Ärzte auf Landesebene. Die Voraussetzungen für die Zulassung als Vertragsarzt sind in der Zulassungsverordnung für Vertragsärzte (Ärzte-ZV) vom 1. Juni 1957 geregelt. Danach muß der antragstellende Arzt seinem Zulassungsantrag u. a. ein "polizeiliches Führungszeugnis" (§ 18 Abs. 2 Buchst. b Ärzte-ZV) beifügen.

Tatsächlich lassen sich die Zulassungsausschüsse der Kassenärztlichen Vereinigung Sachsen (KVS) im Rahmen des Zulassungsverfahrens von dem in Berlin angesiedelten Bundeszentralregister ein sogenanntes "Behördenführungszeugnis (Belegart 'O')" direkt übersenden. Diese Verfahrensweise halte ich aus folgenden Gründen mit dem Willen des Verordnungsgebers von 1957 und dem Wortlaut von § 18 Abs. 2 Buchst. b Ärzte-ZV für nicht vereinbar:

"Polizeiliche Führungszeugnisse" (sie enthielten einen beschränkten Auszug aus den ursprünglich von den Ortspolizeibehörden geführten "polizeilichen Listen" und waren zur Vorlage bei privaten Arbeitgebern gedacht) gibt es seit dem Inkrafttreten des BZRG vom 18. März 1971 nicht mehr. Das BZRG kennt nur noch sogenannte Privatführungszeugnisse gemäß § 30 Abs. 1 Satz 1 BZRG, die auf Antrag jeder über 14 Jahre alten Person erteilt werden (Belegart "N") und sogenannte Behördenführungszeugnisse gemäß § 30 Abs. 5 BZRG, die direkt an eine Behörde (Belegart "O") oder - auf Verlangen des Antragstellers - zunächst an ein von ihm benanntes Amtsgericht zur Einsichtnahme durch ihn (Belegart "P") übersandt werden. Der Unterschied zwischen diesen Führungszeugnis-Arten liegt in ihrem Inhalt: In Privatführungszeugnisse werden weniger gerichtliche und verwaltungsbehördliche Entscheidungen aufgenommen als in Behördenführungszeugnisse.

Einem "polizeilichen Führungszeugnis" als einem beschränkten Auszug aus den ursprünglich von der Ortspolizeibehörden geführten polizeilichen Listen entspricht nach Inkrafttreten des BZRG nach Funktion und Verfahrensweise das Privatführungszeugnis Belegart "N" gemäß § 30 Abs. 1 Satz 1 BZRG. Denn der Verordnungsgeber hatte es bei Erlaß der Ärzte-ZV im Jahre 1957 als ausreichend erachtet, daß der Arzt seinem Zulassungsantrag ein "polizeiliches Führungszeugnis" beizufügen hat, in das nicht all das aufgenommen wird, was schon nach damaliger Rechtslage in ein Führungszeugnis zur Vorlage bei einer Behörde aufgenommen werden durfte.

Hinzu kommt: Stellt man auf den in § 18 Abs. 2 Buchst. b Ärzte-ZV verwandten Begriff des "Beifügens" (eines Führungszeugnisses an einen Zulassungsantrag) ab, so scheidet schon begrifflich eine direkte Übersendung eines Führungszeugnisses von dem Bundeszentralregister an die Zulassungsausschüsse aus. "Beigefügt" werden kann einem Antrag nur ein Führungszeugnis, das der Antragsteller - möglicherweise auch nur vorübergehend - in den Händen hielt.

Gemäß § 18 Abs. 2 Buchst. b Ärzte-ZV darf die KVS somit nur die Beifügung eines Privatführungszeugnisses gemäß § 30 Abs. 1 Satz 1 BZRG verlangen. Will sie statt dessen die Übersendung eines Behördenführungszeugnisses, so muß sie auf eine Änderung von § 18 Abs. 2 Buchst. b Ärzte-ZV hinwirken. All dies habe ich der KVS mitgeteilt und um eine Stellungnahme gebeten. Ich werde diese Angelegenheit weiter im Auge behalten.

10.2 Sozialwesen

10.2.1 Zweites Gesetz zur Änderung des Sozialgesetzbuchs

Das Zweite Gesetz zur Änderung des Sozialgesetzbuchs vom 13. Juni 1994 hat den Sozialdatenschutz auf eine neue Grundlage gestellt.

Neu gefaßt wurden die allgemeinen Vorschriften des § 35 SGB I und der §§ 67 bis 85 a SGB X, weiterhin spezielle Regelungen wie die §§ 61 bis 68 SGB VIII.

In Fortbildungsveranstaltungen für behördliche Datenschutzbeauftragte und Mitarbeiter von Sozialleistungsträgern habe ich über diese Regelungen informiert.

Erfreulich ist, daß das Gesetz durch die geänderte Fassung einfacher anzuwenden ist, weil sein Text klarer ist und vor allen Dingen die bisherigen Verweisungen auf das Bundesdatenschutzgesetz im wesentlichen entfallen, der Rechtsanwender also mit einem einheitlichen Gesetz arbeiten kann.

10.2.2 Die Pflegeversicherung unter datenschutzrechtlichen Gesichtspunkten

Der Streit um die Beibehaltung oder Abschaffung des Buß- und Bettages als gesetzlicher Feiertag hat gezeigt, wie umstritten einzelne Auswirkungen der sozialen Pflegeversicherung (SGB XI) sein können. Nur am Rande und unter Fachleuten werden dagegen die mit der Pflegeversicherung verbundenen umfassenden und tiefgreifenden Eingriffe in das Recht auf informationelle Selbstbestimmung des Pflegebedürftigen diskutiert. Ich prüfe derzeit - soweit mein Zuständigkeitsbereich betroffen ist -, ob einzelne der in der Praxis vorgesehenen Verfahrensschritte bei der Feststellung der Pflegebedürftigkeit den gesetzlichen Vorgaben entsprechen.

Das Prinzip der Datenerhebung für die Pflegeversicherung ist leicht beschrieben: Leistungen erhalten Personen, die wegen einer körperlichen, geistigen oder seelischen Krankheit oder Behinderung für die gewöhnlichen und regelmäßig wiederkehrenden Verrichtungen im Ablauf des täglichen Lebens der Hilfe bedürfen (§ 14 SGB XI). Diese Pflegebedürftigen müssen einen Antrag bei ihrer Pflegekasse stellen (§ 33 SGB XI). Die Pflegekasse beauftragt sodann den Medizinischen Dienst der Krankenversicherung (MDK; § 275 f. SGB V), ein "Gutachten" (in Wirklichkeit handelt es sich um eine fachdienstliche Stellungnahme) über den Pflegebedürftigen zu erstellen. Der MDK oder ein von ihm Beauftragter (es kann sich auch um Mitarbeiter eines gewerblichen Pflegedienstes handeln, die ein wirtschaftliches Interesse an der Feststellung und Aufrechterhaltung der Pflegebedürftigkeit haben) untersucht den Pflegebedürftigen daraufhin in der Regel in häuslicher Umgebung. Ausnahmsweise kann sich auch aufgrund der Aktenlage eindeutig ergeben, in welche der drei Pflegestufen der Pflegebedürftige eingeordnet werden soll (§ 18 Abs. 2 SGB XI).

Wie aber stellt der MDK die Pflegestufe in der Praxis fest? Hierzu haben die Pflegekassen unter Beteiligung des MDK Richtlinien gemäß § 17 SGB XI *über die Abgrenzung der Merkmale der Pflegebedürftigkeit und der Pflegestufen sowie zum Verfahren der Feststellung der Pflegebedürftigkeit* beschlossen und einen *fünfseitigen Gutachtenvordruck* entwickelt, auf dem der MDK sein Gutachten gegenüber der Pflegekasse abgeben soll. Er umfaßt Fragen zu nahezu sämtlichen Lebensbereichen, die für einen pflegebedürftigen Menschen (noch) von Interesse sind. So will der MDK im Rahmen der Untersuchung z. B. die Namen aller Pflegepersonen (mit deren Pflegestundenzahl pro Woche), ggf. Angaben zur medikamentösen Behandlung und zur Teilnahme an der Krankengymnastik sowie generell zur Krankenvorgeschichte erfahren; ferner müssen u. a. "pflegerelevante Aspekte der Wohnsituation", der Grad der Desorientierung und der Bewußtseinslage und die "Fähigkeiten im Bezug auf die Aktivitäten des täglichen Lebens" angegeben werden. Zur Bestimmung des Grades der

Pflegebedürftigkeit wird gefragt, ob die Körperpflege (z. B. "rasieren" oder "duschen"), die Ernährung (mundgerecht?), die Mobilität (an- und auskleiden?) und vieles mehr noch vom Pflegebedürftigen selbst gemeistert werden kann. Bei dieser Untersuchung soll der Pflegebedürftige auch gleich in die Offenbarung seiner Vorerkrankungen durch seine vorbehandelnden (Haus-) Ärzte einwilligen (§ 18 Abs. 3 SGB XI). Tut er dies nicht und lassen sich deshalb nach Ansicht des MDK die Voraussetzungen der Pflegeleistung nicht bestimmen, lehnt die Pflegekasse eine Leistung ab. Schließlich faßt der MDK das Ergebnis seiner "Begutachtung" auf den letzten eineinhalb Seiten des Gutachtenvordrucks zusammen. Das gesamte Gutachtenformular wird sodann der Pflegekasse zur Kenntnis gegeben.

Problematisch erscheint mir darin u. a. folgendes: Das Gesetz erlaubt es den Kassen, mit Hilfe *ihres* Medizinischen Dienstes - letztlich ein inkorporierter Teil der Kassen - über die Gewährung von Pflegeleistungen zu entscheiden und hierzu einen tiefen Einblick in die Lebensverhältnisse des Pflegebedürftigen (und die Arbeitsweise seiner Ärzte!) zu nehmen - eine im Grundsatz problematische Konstruktion, insbesondere auch hinsichtlich des nicht genau bestimmten Umfangs der Einwilligung des Pflegebedürftigen in die Offenbarung aller seiner Krankendaten bei sämtlichen seiner vorbehandelnden (Haus-)Ärzte. Hier muß im Text der Einwilligungserklärung genau bestimmt werden, daß nur die zur Bestimmung der Pflegestufe erforderlichen Auskünfte bei den vorbehandelnden Ärzten eingeholt werden dürfen.

Ich halte es für unwürdig - jawohl, hier stoßen wir an die Menschenwürde des Art. 1 Abs. 1 GG, hier tasten wir sie an - Einzelheiten der körperlichen und seelischen Verfassung eines Pflegebedürftigen in dem oben beschriebenen, bisher nicht gekannten Umfang offenbaren zu müssen, damit daraufhin er selbst oder die Pflegeperson in den Genuß einer Versicherungsleistung kommt. Mit dem "freiwilligen" Herauslösen fast aller Krankheitsdaten aus dem als geistesgeschichtliche Tradition (dazu OVG Berlin NJW 1980, 2485) bestehenden, auf dem besonderen Vertrauen in die Verschwiegenheit des Arztes beruhenden Arzt-Patienten-Verhältnis kommt der Einzelne seiner Degradierung zum Objekt eines Sozialleistungsverfahrens gefährlich nahe, zumal die Daten nicht bei dem Arzt des Medizinischen Dienstes verbleiben, sondern dem Gesamtapparat der Versicherungsunternehmen zur Verfügung gestellt werden.

Das SMS habe ich in der oben gestellten Frage um eine Stellungnahme gebeten. Ich werde den gesamten Komplex der Datenverarbeitung in der Pflegeversicherung - auch hinsichtlich weiterer, hier nicht erwähnter Probleme - wegen seiner gesamtgesellschaftlichen Bedeutung aufmerksam und genau beobachten.

10.2.3 Datenschutzrechtliche Anforderungen an das Sozialgesetzbuch VII

Im Zusammenhang mit Unfällen werden durch die Träger der gesetzlichen Unfallversicherung häufig Daten von Versicherten erhoben und weitergegeben, ohne daß diese davon Kenntnis erhalten. Nach meiner Auffassung ist dies mit dem Recht auf informationelle Selbstbestimmung, insbesondere hinsichtlich der Transparenz der einzelnen Verfahrensschritte, nicht vereinbar.

Auch der vorliegende Referentenentwurf des Bundesministers für Arbeit und Sozialordnung zum Unfallversicherungs-Einordnungsgesetz - SGB VII enthält dazu keine Verbesserungen.

Die 49. Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat daher in ihrer Entschließung zum Sozialgesetzbuch VII Anforderungen an einen verfassungsgemäßen Datenschutz für Unfallversicherte formuliert. Die Anforderungen beziehen sich z. B. auf die Auskunftspflicht behandelnder Ärzte, die Datenerhebung, -verarbeitung und -nutzung durch Durchgangsärzte, auf Formulare zur Anzeige eines Unfalls und eine eindeutige Regelung der Akteneinsicht der Versicherten (siehe 16.2.10).

10.2.4 Grundsatzproblem: Datenschutzwidrige Bundesauftragsverwaltung

Im Zusammenhang mit den Datenschutzproblemen in dem Vordruck B zur Überprüfung des Kindergeldanspruchs nach dem 1. SKBPG ab 1. Januar 1994 bin ich auf folgende Grundsatzfrage gestoßen:

Führen Länder Bundesgesetze, wie das novellierte Bundeskindergeldgesetz aus, so unterstehen sie der Weisung der obersten Bundesbehörden (Art. 85 Abs. 3 GG). Die entsprechenden Weisungen zur Anwendung des Fragebogens B gingen an das SMF. Die darin verlangte Ausforschung eines Adoptionsverhältnisses war rechtswidrig (siehe 10.2.7). Ist das SMF verpflichtet, solche rechtswidrigen Anweisungen der obersten Bundesbehörde auszuführen, und welche Möglichkeiten habe ich, mich dagegen zu wenden?

Das SMF ist zwar an Weisung des Bundes gebunden. Es ist jedoch verpflichtet, gegenüber dem Bundesministerium Einwände gegen ein rechtswidriges Verfahren geltend zu machen und Gegenvorstellungen im Sinne eines rechtskonformen Gesetzesvollzugs zu äußern.

Sofern die angewiesene oberste Landesbehörde nichts unternimmt, sondern einfach - ohne eigene Prüfung, ob sie rechtmäßig handelt - tätig wird und der rechtswidrigen oder undurchdachten Weisung "aus Bonn" oder "aus Berlin" folgt, besteht für mich das Recht zur Beanstandung nach § 26 Abs. 1 SächsDSG. Beanstanden kann ich diese Untätigkeit, aber auch den bloßen objektiv rechtswidrigen Handlungsablauf. Indirekt kann ich dadurch die datenschutzwidrige Weisung der obersten Bundesbehörde kritisieren. Gegen die Rechtswidrigkeit dieser Weisung vermag sich also nicht nur der für die Bundesbehörden zuständige Bundesbeauftragte für den Datenschutz mit Erfolg zu wenden.

10.2.5 Aufklärungs- und Hinweispflichten bei Datenerhebungen durch den Sozialleistungsträger gemäß § 67 a SGB X

Wenn der Sozialleistungsträger Sozialdaten erhebt, muß er gemäß § 67 a Abs. 3 SGB X dem Betroffenen den Erhebungszweck angeben. Wenn die Datenerhebung aufgrund einer Rechtsvorschrift erfolgt, die zur Auskunft verpflichtet, hat er diese Rechtsvorschrift zu nennen, ferner auf die Auskunftspflicht hinzuweisen und die Folgen einer Verweigerung mitzuteilen.

Nach anderen Rechtsvorschriften ist der Betroffene zwar häufig nicht verpflichtet, eine Auskunft zu erteilen. Er erhält jedoch eine Leistung oder einen anderen Vorteil nur, wenn er die gewünschten Angaben macht. Der Sozialleistungsträger muß ihn auf die Vorschrift hinweisen und deutlich machen, welche Folgen die Verweigerung der Auskunft hat.

Wenn der Betroffene darum gebeten wird, freiwillig Angaben zu machen, dürfen ihm keine Nachteile entstehen; der Sozialleistungsträger muß ihn dann auf die Freiwilligkeit hinweisen.

Beispiel: Ein Rentenversicherungsträger hatte eine 53 Jahre alte Versicherte gebeten, den Ausweis für Arbeit und Sozialordnung oder beglaubigte Kopien von Auszügen vorzulegen. Damit sollte eine frühzeitige Speicherung der für die Feststellung des Rentenverlaufs und die spätere Rentenberechnung erforderlichen Daten ermöglicht werden.

Die Angaben waren freiwillig. Bei einer Verweigerung besteht jedoch die Gefahr, daß bei der späteren Rentenberechnung Nachweise fehlen. Darüber hat das Anschreiben nicht ausreichend informiert. Die Versicherte äußerte ihr Unverständnis darüber, daß sie sieben Jahre vor der Rente und obwohl sie keinen Rentenantrag gestellt hatte, um die Unterlagen gebeten wurde.

Der Rentenversicherungsträger änderte das Anschreiben in guter Zusammenarbeit mit mir, so daß diese Irritationen in Zukunft nicht mehr auftreten dürften. Ein (möglicher) geringer Mehraufwand bei der Formulierung solcher Anforderungsschreiben kann also zu einer Vermeidung langwieriger Auseinandersetzungen und einem guten Einvernehmen zwischen dem Sozialleistungsträger und dem Empfänger dieser Leistungen beitragen.

10.2.6 Sozialhilfestatistik

Seit dem 1.1.1994 wird eine Sozialhilfestatistik auf der Grundlage der novellierten §§ 127 ff. BSHG durchgeführt.

Die Sozialhilfestatistik ist eine Sekundärstatistik. Es werden also für sie nicht Daten vom Betroffenen erhoben, sondern die bei der Gewährung der Sozialhilfe bereits verarbeiteten Daten genutzt.

Fraglich ist allerdings, ob die in § 128 BSHG festgelegten Statistikdaten den Daten entsprechen, die für die Gewährung von Sozialhilfe tatsächlich erforderlich sind. Diese Zweifel beziehen sich insbesondere auf die Angaben zum höchsten Schulabschluß an allgemeinbildenden Schulen und zum höchsten Berufsabschluß (beschränkt auf Leistungsempfänger zwischen 15 und 64 Jahren), weiterhin Angaben zu besonderen sozialen Situationen (darunter verstehen Statistische Landesämter äußerst sensible Daten wie Drogensucht, Freiheitsentzug und Trennung/Scheidung!).

Das Bundesministerium für Familie und Senioren hat die Auffassung vertreten, diese Daten seien für die Hilfegewährung erforderlich, etwa die Angabe zum höchsten Berufsabschluß für die berufliche Wiedereingliederung (Schreiben vom 22. August 1994 an die Geschäftsstelle der Konferenz der obersten Landessozialbehörden).

Landessozialbehörden, die solche Daten hingegen für die Sozialhilfebearbeitung nicht für erforderlich halten, führen eine Nacherhebung der Daten für die Statistik nur auf freiwilliger Grundlage durch.

Auch ich bezweifle, daß alle in § 128 BSHG aufgeführten Erhebungsmerkmale in jedem einzelnen Falle für die Hilfegewährung benötigt werden. Gemäß § 67 a Abs. 1 BSHG ist das Erheben von Sozialdaten nur zulässig, wenn ihre Kenntnis zur Erfüllung einer Aufgabe der erhebenden Stelle nach diesem Gesetzbuch erforderlich ist. So werden etwa Angaben über den höchsten Berufsabschluß bei einer alleinerziehenden Mutter kleiner Kinder auf absehbare Zeit nicht für die Prüfung einer beruflichen Wiedereingliederung gebraucht. Das Datum wird also in einem solchen Fall - unzulässigerweise - nur für statistische Zwecke erhoben.

Offensichtlich lagen die in § 128 BSHG aufgeführten Daten in der Vergangenheit häufig nicht vor (was dafür spricht, daß sie auch nicht benötigt wurden). Daher fanden in verschiedenen Bundesländern umfangreiche Nacherhebungsaktionen statt. Den Hilfeempfängern wurden Fragebögen vorgelegt und Nachteile angedroht, falls sie diese nicht ausfüllten.

Ein solches Vorgehen ist rechtswidrig. Eine Pflicht, zur Durchführung der Statistik Auskunft zu erteilen, besteht nämlich nur für die Sozialämter, nicht für den Hilfeempfänger. Dieser ist nur auskunftspflichtig gemäß § 60 Abs. 1 Nr. 1 SGB I, soweit die Angaben für die Hilfeleistung, also nicht für die Statistik, erforderlich sind, was jedoch, wie ausgeführt, häufig nicht der Fall ist.

Eine umfassende schriftliche Nacherhebung durch Fragebögen allein aus Statistikgründen ist auch nach Auffassung des Bundesministeriums nicht zulässig. Es schlägt vor, bei der nächsten Vorsprache des Hilfeempfängers im Sozialamt die Daten nachzuerheben. Im Einzelfall könne auch eine besondere Vorsprache zu diesem Zweck geboten sein.

Dies ist allerdings nur zulässig, wenn man, wie das Bundesministerium, die Erforderlichkeit der Erhebungsmerkmale in § 128 BSHG auch für die Leistungsgewährung bejaht. Andernfalls darf auch eine solche "Einzelnacherhebung" nicht mit der Androhung von Zwang verbunden werden. In Betracht kommen allenfalls freiwillige Angaben des Hilfeempfängers. Die Zulässigkeit einer solchen Nacherhebung

für eine Sekundärstatistik ist jedoch umstritten. Zudem ist zu berücksichtigen, daß gerade im Bereich der Sozialhilfe, auf die der Empfänger existentiell angewiesen ist, wenig Raum für eine wirklich freiwillige Entscheidung bleibt. Ich werde gemeinsam mit dem von mir um Stellungnahme gebetenen SMS nach einer Klärung dieser Probleme suchen und an meiner Auffassung festhalten, daß die Datenerhebung rechtswidrig ist.

10.2.7 Verletzung des Adoptionsgeheimnisses bei der Überprüfung des Kindergeldanspruchs

Ein Formular des Bundesministeriums für Familie und Senioren, das (mit Modifikationen) bundes- und landesweit zur Überprüfung des Kindergeldanspruchs verwendet wurde, veranlaßte auch in Sachsen Anfragen und Eingaben.

In einem Vordruck zur Überprüfung des Kindergeldes für öffentlich Bedienstete wird nach dem Kindschaftsverhältnis zum Kindergeldbezieher oder seinem Ehegatten gefragt, und zwar unterschieden nach: "leibliches Kind", "Adoptivkind" und "Pflegekind". Die Rechtsgrundlage, die zur Beantwortung dieser Frage verpflichtet, war nicht präzise angegeben.

Alle Datenschutzbeauftragten haben nachdrücklich Bedenken gegen die Frage nach einer Adoption geäußert, weil damit das von § 1758 BGB geschützte Adoptionsgeheimnis ausgeforscht wird. Die Frage war zudem überflüssig, weil das Kindergeld von ihrer Beantwortung nicht abhängt.

Personenbezogene Sozialdaten sind zu löschen, wenn ihre Speicherung unzulässig ist (§ 84 Abs. 2 SGB X). Meine Hinweise auf eine Löschung des unzulässig erfaßten Adoptivkindschaftsverhältnisses an das Landesamt für Finanzen und das SMF blieben zunächst ohne Ergebnis, da "erst eine entsprechende Weisung in einem gemeinsamen Rundschreiben des Bundesministeriums für Familie, Senioren, Frauen und Jugend und des Bundesministeriums des Innern abgewartet" werden sollte.

Nach langer Zeit ordnete dann ein gemeinsames Rundschreiben vom 16. Dezember 1994 an, daß die Information über ein unzulässig offenbartes Adoptivkindschaftsverhältnis spätestens bei der nächsten Fallbearbeitung zu löschen ist.

In vielen Fällen wird im Jahre 1995 eine Fallbearbeitung und damit auch eine Löschung erfolgen. Falls jedoch vereinzelt eine Fallbearbeitung für den Kindergeldbezieher erst nach Jahren oder vielleicht überhaupt nicht mehr erfolgt, so tritt ein unerträglicher Zustand ein: Einige unzulässig erfaßte Daten sind gelöscht, andere später oder überhaupt nicht. Dieser Umgang mit den Folgen eines Fehlers ist nach meiner Auffassung nicht hinnehmbar.

Alle Fragebögen müssen geprüft und alle unzulässig erfaßten Daten müssen spätestens zu einem absehbaren Termin gelöscht sein. Ich habe dem SMF eine entsprechende Anregung gegeben und den für die Bundesbehörden zuständigen Bundesbeauftragten für den Datenschutz informiert.

Bei Redaktionsschluß dieses Tätigkeitsberichtes teilte mir das SMF - nach seiner Abstimmung mit dem Landesamt für Finanzen - mit, daß es 1995 eine gesonderte Überprüfungsaktion anweisen wird. Damit sollen tatsächlich alle Kindergeldzahlfälle erfaßt werden, die den bemängelten Vordruck B erhalten haben. Aus Gründen der Verwaltungsökonomie wird diese Überprüfung der ca. 65000 Zahlakten mit einer ohnehin anstehenden kindergeldrechtlichen Überprüfung verknüpft. Ein Abschluß wird unmehr für das dritte Quartal 95 ins Auge gefaßt. Ich begrüße diese Entscheidung des SMF.

Eltern, die ein Adoptivkindschaftsverhältnis im Vordruck B offengelegt haben, erhalten vom Landesamt für Finanzen einen berichtigten Vordruck und ein Anschreiben mit der Bitte, diesen neuen Vordruck auszufüllen (ohne die Angabe über das Kindschaftsverhältnis). Sobald dieser berichtigte Vordruck beim Landesamt für Finanzen eintrifft, wird der bisherige alte Vordruck in den Akten vernichtet. Ich wurde auch darüber unterrichtet, daß auch sämtlicher mit dieser Korrektur verbundener Schriftwechsel vernichtet wird. Es ist demnach aus der Akte nichts mehr ersichtlich als der neue Erhebungsbogen.

10.3 Lebensmittelüberwachung und Veterinärwesen

10.3.1 Meldepflichten der Tierärzte gegenüber der Sächsischen Landestierärztekammer

Die Sächsische Landestierärztekammer ist die Selbstverwaltungseinrichtung der etwa 1200 Tierärzte im Freistaat. Begründet ein Tierarzt seine Hauptwohnung in Sachsen oder übt er hier seine Tätigkeit aus, muß er sich bei der Kammer in Dresden melden. Diese übersendet ihm sodann zwei Fragebögen, mit deren datenschutzgerechterer Gestaltung ich im Berichtszeitraum mehrmals befaßt war.

Die Fragebögen (ein "Tierärztekammermeldebogen" und ein Fragebogen zur "Art der Tätigkeit") sahen eine ganze Reihe von Angaben vor, für deren Erhebung sich im Sächsischen Heilberufekammergesetz nicht die erforderliche Grundlage findet. So sollte der Tierarzt in dem "Tierärztekammermeldebogen" unter anderem seine Staatsangehörigkeit, gegebenenfalls seinen Geburtsnamen, den Kreis und Regierungsbezirk seines Geburtsortes sowie Privat-, Praxis- und Korrespondenz-Anschriften angeben müssen. Sehr umfangreich war der Katalog von Fragen zur Art der Tätigkeit des Tierarztes: Hier waren insgesamt 52 (!) Antwortmöglichkeiten vorgesehen. So sollte der Tierarzt unter anderem angeben, ob er niedergelassen, angestellt oder beamtet, als Praxisassistent oder Industrietierarzt, ausschließlich oder teilbeschäftigt in der Fleischuntersuchung, im Schlachthof oder bei einer Versandschlachterei, im Außendienst in der Pharmazeutischen Industrie oder bei der Bundeswehr beschäftigt ist und welche Nebentätigkeit er gegebenenfalls dabei ausübt oder ob er derzeit seinen Beruf nicht oder als Doktorand ohne weitere Tätigkeit ausübt!

Ich habe wie folgt Stellung genommen: Datenerhebungen im Meldeverfahren der Tierärztekammer bedürfen wie jeder Eingriff in das Grundrecht auf informationelle Selbstbestimmung einer gesetzlichen Grundlage. § 3 Abs. 1 SächsHKaG bestimmt lediglich, daß sich der Tierarzt innerhalb eines Monats nach Beginn der

Pflichtmitgliedschaft bei der Kammer zu melden hat. Das Nähere über das Meldeverfahren und die zur Überwachung (der Erfüllung) der Berufspflichten erforderlichen Angaben und Nachweise darf die Kammer in einer Meldeordnung regeln (§ 3 Abs. 2 SächsHKaG), was bisher nicht geschehen ist. In jedem Fall ist Voraussetzung, daß alle zu erhebenden Daten zur Aufgabenerfüllung der Tierärztekammer erforderlich sein müssen. Dies ist insbesondere bei den Fragen zur Art der Tätigkeit nicht der Fall. Zwar mögen einige der ins Detail gehenden Fragen insbesondere auf dem Fragebogen "Art der Tätigkeit" noch für die Berechnung des Kammerbeitrages erforderlich sein. Die meisten Fragen konnte ich jedoch *keiner* Aufgabe der Kammer zuordnen.

Hierauf und auf die Erforderlichkeit einer Meldeordnung gemäß § 3 Abs. 2 SächsHKaG habe ich die Tierärztekammer schriftlich und in mehreren Besprechungen hingewiesen, und ich habe dabei deutlich "schlankere" Meldebögen gefordert. Mittlerweile liegt mir ein Entwurf einer Meldeordnung vor, der das *vollständige* Ausfüllen der Meldebögen zu einer Berufspflicht des Tierarztes erklärt. Damit kann ich aus oben genannten Gründen nur einverstanden sein, wenn sich die Meldebögen auf das zur Aufgabenerfüllung der Kammer erforderliche Maß beschränken. Da mir bisher jedoch noch keine in diesem Sinne überarbeiteten Muster von Erhebungsbögen vorliegen, werde ich die Angelegenheit weiter beratend und kontrollierend begleiten.

10.3.2 Übermittlung von Tierhalterdaten an einen Doktoranden?

Die sächsischen Rinderhalter konnten im Jahre 1993 freiwillig Blutproben, die ihren Tieren pflichtweise entnommen wurden, zusätzlich auch auf das Vorkommen von Antikörpern gegen einen bestimmten Virus untersuchen lassen.

Durchgeführt wurden diese Untersuchungen bei der *Landesuntersuchungsanstalt für das Gesundheits- und Veterinärwesen* (§ 3 SächsGDG), die auch die Ergebnisse gespeichert hat, und zwar überwiegend zugeordnet den einzelnen rinderhaltenden Betrieben, aus denen die Proben angeliefert worden waren. Finanziert worden waren die Untersuchungen durch die Sächsische Tierseuchenkasse (§§ 5 ff. SächsAGTierSG) aufgrund ihrer Leistungssatzung.

Ein Doktorand wollte die Durchseuchung der sächsischen Rinder mit besagtem Virus erforschen. Geplant waren zu diesem Zwecke zweierlei Zugriffe auf personenbezogene Daten: Zum einen sollte der Doktorand aus den bei der Landesuntersuchungsanstalt in maschinenlesbarer Form vorhandenen Daten sich bezüglich aller rinderhaltenden Betriebe in Sachsen folgenden Datensatz heraussuchen: Inhaber und Anschrift des Betriebes, Anzahl der auf den Virus untersuchten Proben sowie Anzahl der Proben *mit Befund*. Hinsichtlich der auf diese Weise ermittelten Betriebe sollte der Doktorand dann außerdem aus der Gesamt-Tierhalter-Liste der Tierseuchenkasse oder doch jedenfalls aus einem Ausdruck aus den Daten der Tierseuchenkasse, der sämtliche rinderhaltendenen Betriebe mitsamt der Zahl der gemeldeten Rinder aufführte, die Anzahl der im jeweiligen Betrieb gehaltenen Rinder herausfinden. Daten der Landestierseuchenkasse aus Meldungen über die Teilnahme an einem den Virus betreffenden freiwilligen besonderen Bekämpfungsprogramm sollten noch hinzukommen.

Aus den Daten sollten für die Dissertation folgende Werte gewonnen werden: Der durchschnittliche Durchseuchungsgrad der Rinderbestände derjenigen Betriebe, die an der freiwilligen Untersuchung teilgenommen hatten (und zusätzlich derjenige der Betriebe, die am Bekämpfungsprogramm teilgenommen hatten), und zwar jeweils bezogen auf die Kreise des Freistaats.

Die datenschutzrechtliche Überprüfung des Dissertationsvorhabens ergab dann folgendes:
Die geplante Datenübermittlung durch die Landesuntersuchungsanstalt wäre nach § 6 Abs. 1 Satz 3 (Offenbarungsverbot) sowie Satz 4 (persönliche Geheimhaltungspflichten der Amtsangehörigen, die unberührt bleiben) SächsGDG *verboten* gewesen. Im Sinne des § 6 SächsGDG ist die Landesuntersuchungsanstalt nämlich eine "Behörde des öffentlichen Gesundheitsdienstes", trotz der Entgegensetzung zwischen Landesuntersuchungsanstalt und den "für den Vollzug gesundheitsrechtlicher Vorschriften für Mensch und Tier ... zuständigen Behörden" in § 3 Abs. 2 SächsGDG. Denn sonst wäre der durch § 6 SächsGDG bezweckte Schutz äußerst lückenhaft: Die strengen Regeln dieser Vorschrift gälten für die Landesuntersuchungsanstalt, bei der besonders schutzbedürftige Daten anfallen, gerade nicht. Nur so läßt sich das Gesetz meiner Auffassung nach in diesem Punkt *verfassungskonform* auslegen. Da es sich um Daten handelte, die bei einer *freiwilligen Untersuchung bekanntgeworden sind,* wäre die Übermittlung personenbezogener Daten durch die Landesuntersuchungsanstalt an den Doktoranden oder auch an dessen Universität nach § 6 Abs. 1 Satz 1, 2. Fall in Verbindung mit Satz 3 SächsGDG rechtswidrig gewesen.

Letztlich kam es auf diese Auslegungsfrage jedoch nicht an:
Auch wenn man die Landesuntersuchungsanstalt wegen der genannten Entgegensetzung in § 3 Abs. 2 SächsGDG und auch deswegen, weil sie in § 2 SächsGDG nicht erwähnt ist, *nicht* im Sinne der §§ 6 und 7 SächsGDG als "Behörde des öffentlichen Gesundheitsdienstes" ansehen will, ist das Ergebnis kein anderes. In diesem Falle beurteilt sich die Zulässigkeit mangels bereichsspezifischer Regelung nach dem Sächsischen Datenschutzgesetz, dessen allgemeine Übermittlungsregelung für die Übermittlung personenbezogener Daten durch die *Landestierseuchenkasse* ohnehin maßgeblich ist.

Die Übermittlungs-Erlaubnis des § 15 Abs. 1 Nr. 1 SächsDSG setzt voraus, daß die Übermittlung der personenbezogenen Daten zur Erfüllung der Aufgaben der übermittelnden Stelle *erforderlich* ist. An dieser Erforderlichkeit fehlte es jedoch. Für den Erkenntnis-Gegenstand der Dissertation hätte es genügt, wenn von der Landesuntersuchungsanstalt bzw. der Tierseuchenkasse *kreisweise aggregierte* Daten übermittelt worden wären. Genauso hätte es genügt, wenn man dem Doktoranden hinreichend anonymisierte Betriebs-Daten übermittelt hätte, was nach einer vorübergehenden Zusammenführung noch personenbezogener Daten zwischen Landesuntersuchungsanstalt und Tierseuchenkasse, also auf einem privilegierten Übermittlungsweg (vgl. § 23 Abs. 3 SächsAGTierSG), möglich gewesen wäre.

Die Landestierseuchenkasse hatte erklärt, an der Durchführung des Dissertationsvorhabens interessiert zu sein, sich jedoch, genauso wie die Landesuntersuchungsanstalt, nicht in der Lage gesehen, selbst die für eine Anonymisierung der Daten nötige Arbeit zu leisten.

Letztlich lief das Dissertationsvorhaben darauf hinaus, die mit der Anonymisierung bzw. Aggregierung der Daten verbundene Arbeit aus dem Bereich der öffentlichen Stellen nach außerhalb auf einen Doktoranden zu übertragen, weil die beteiligten öffentlichen Stellen auf die Angelegenheit doch nicht so viel Wert legten, daß sie eigene Kapazitäten für diese Arbeit (die bezeichnenderweise keinerlei veterinärmedizinischen Kenntnisse erfordert hätte) einsetzen wollten.

Es versteht sich nahezu von selbst, daß sich auch über § 15 Abs. 1 Nr. 2 (mit Abs. 3) SächsDSG keine Erlaubnis der Datenübermittlung ergab: Die Inhaber der betroffenen rinderhaltenden Betriebe, insbesondere derjenigen mit positivem Befund, hatten wegen der möglichen Wirkungen auf die Verkäuflichkeit ihrer Rinder ein Interesse am Unterbleiben der Übermittlung, und dieses Interesse war, da es im Hinblick auf die betreffende Erkrankung keine Untersuchungs- beziehungweise Meldepflicht gibt, auch schutzwürdig, weil der Verdacht einer Gefährdung der menschlichen Gesundheit nicht besteht.

Den Doktoranden habe ich auf die Möglichkeit aufmerksam gemacht, seine Untersuchung in Form einer hinreichend anonymisierten *Experten-Befragung* durchzuführen, also als Befragung niedergelassener Tierärzte zu deren persönlicher Einschätzung im Hinblick auf die Verbreitung des Virus in den Rinderbeständen ihrer Region (*nicht* in den von ihnen betreuten Rinderbeständen - was nicht hinreichend anonymisiert durchführbar wäre).

10.3.3 Datenverarbeitung der Lebensmittelüberwachungsbehörden

Lebensmittelüberwachungsbehörden sind in Sachsen die Lebensmittelüberwachungs- und Veterinärämter (LÜVÄ), die Regierungspräsidien und das SMS. Praktisch wird die Lebensmittelüberwachung vor allem durch Entnahme und Untersuchung von Lebensmittelproben in lebensmittelverarbeitenden Betrieben durchgeführt. An der naturwissenschaftlichen Untersuchung der Proben ist die Landesuntersuchungsanstalt (LUA) beteiligt. Bei diesen Überwachungsmaßnahmen werden eine Vielzahl personenbezogener Daten erhoben, z. B. wie oft der Betriebsinhaber gegen Vorschriften des Lebensmittelrechts verstoßen hat und welche Verstöße im einzelnen vorliegen (z. B. überlagerte Lebensmittel, Zustand der Sanitäranlagen, fehlende Desinfektionsmittel, Schmutz auf Gegenständen, etc.). § 12 SächsAGLMBG sieht insofern vor, daß die Lebensmittelüberwachungsbehörden Daten verarbeiten und sich und der Landesuntersuchungsanstalt *"alle Daten, die zur wirkungsvollen Lebensmittelüberwachung erforderlich sind"*, übermitteln dürfen.

Diese Regelung ist nicht unproblematisch: Die Befugnis zur Datenübermittlung besteht nur unter den in § 40 Abs. 3 Nr. 2 LMBG genannten Voraussetzungen, also bei Zuwiderhandlungen und beim Verdacht auf Zuwiderhandlungen gegen Vorschriften des Lebensmittelrechts. Das (Bundes-)LMBG gibt insofern den Rahmen für die landesrechtliche Regelung im SächsAGLMBG, über den eine landesrechtliche Ermächtigung zur Datenverarbeitung nicht hinausgehen darf. Die in § 12 Abs. 2 SächsAGLBMG verwandte Formulierung, wonach "alle" Daten übermittelt werden dürfen, ist insofern nicht eindeutig. Bis zu einer Änderung dieser Vorschrift muß sie, damit sie nicht gegen das höherrangige Bundesrecht (Art. 31 GG) verstößt und damit

verfassungswidrig (und deswegen nichtig) ist, verfassungskonform einschränkend so ausgelegt werden, daß nur die Daten übermittelt werden, die in einem direkten Zusammenhang mit Zuwiderhandlungen oder einem (durch Tatsachen begründeten) Verdacht auf Zuwiderhandlungen stehen.

Das SMS hat auf meinen Hinweis die nachgeordneten Behörden und die LUA in diesem Sinne unterrichtet.

In der technischen Durchführung bedienen sich die Lebensmittelüberwachungsbehörden des in Sachsen entwickelten "Verbraucherschutz- und Gesundheitsinformations-Systems der Behörden" (VEGIS/B); seine Übernahme ist auch in anderen Bundesländern geplant. Den Anwendungsbereich hatte das SMS bereits auf der Grundlage des SächsGDG durch eine Verwaltungsvorschrift geregelt. Diese sieht unter anderem vor, daß geringfügige Mängel, wie z. B. ungeputzte Fenster oder nicht sauber gewischte Fußböden, deren Behebung die Prüfer formlos anmahnen (was nicht als förmliche Anordnung, also nicht als Verwaltungsakt anzusehen ist), nicht als Verstöße zu erfassen sind, sondern in einem von VEGIS/B vorgesehenen "Memofeld" stichwortartig erfaßt werden.

Hier hatte ich zunächst Bedenken, daß die Vollzugsbehörde zeitlich und sachlich nahezu unbegrenzt Daten der zu überwachenden Personen und Betriebe speichern könne, auch wenn dies im Einzelfall zur Aufgabenerfüllung nicht mehr erforderlich ist. Meine Bedenken waren jedoch unbegründet. Das SMS hatte bereits 1992 angeordnet, welche Feststellungen im einzelnen in dem Memory-Feld verwendet werden dürfen und daß die Anwender von VEGIS/B auf diese Einschränkungen schriftlich zu verpflichten sind.

Bei dem LÜVA einer sächsischen Großstadt, also der für die Lebensmittelüberwachung an Ort und Stelle verantwortlichen Behörde, habe ich mir den Betrieb von VEGIS/B vorführen und erläutern lassen. Ich habe bei der Einsichtnahme in die dort gespeicherten Daten eines zufällig ausgewählten lebensmittelverarbeitenden Betriebes keine Daten feststellen können, die nicht zur Aufgabenerfüllung erforderlich gewesen wären. Bei der Prüfung des weiteren Verfahrens ist mir jedoch aufgefallen, daß der LUA auf dem Probenahmeschein gemäß § 42 LMBG weit mehr Daten übermittelt werden, als es zur naturwissenschaftlichen Untersuchung der Lebensmittelprobe erforderlich scheint. So wird insbesondere auch der Name des kontrollierten Betriebes mit übermittelt. Die LUA erhält damit einen Überblick über alle in Sachsen kontrollierten lebensmittelverarbeitenden Betriebe und gegebenenfalls deren Verstöße gegen das Lebensmittelrecht, obwohl sie meiner Meinung nach ihre Untersuchungsaufgabe in gleicher Weise mit einem anonymisierten Probenahmeschein erfüllen könnte. Daher habe ich das SMS gebeten, mir ein Verfahren vorzuschlagen, durch das sichergestellt wird, daß der LUA keine anderen als zur Aufgabenerfüllung erforderlichen Daten übermittelt werden. Der letzte Stand ist, daß das SMS die Erforderlichkeit zur Zeit noch anders beurteilt als ich. Die Fragen werden daher im einzelnen genauer untersucht werden müssen.

10.4 Rehabilitierungsgesetze

Seit Ende 1992 gibt es, als Bestandteil des Ersten SED-Unrechtsbereinigungsgesetzes, das *Strafrechtliche Rehabilitierungsgesetz*. Im wesentlichen regelt es, unter welchen Voraussetzungen strafrechtliche Entscheidungen, die ein deutsches Gericht im Beitrittsgebiet zwischen dem 8. Mai 1945 und dem 2. Oktober 1990 gefällt hat, wegen Verstoßes gegen wesentliche Grundsätze einer freiheitlichen rechtsstaatlichen Ordnung aufzuheben und inwieweit den von solchen Entscheidungen Betroffenen Ausgleichsleistungen zu gewähren sind. Mehr als einhunderttausend Rehabilitierungsanträge sind auf dieser Grundlage bereits beschieden worden.

Seit Mitte 1994 sind mit dem Zweiten SED-Unrechtsbereinigungsgesetz das *Berufliche* sowie das *Verwaltungsrechtliche Rehabilitierungsgesetz* hinzugekommen. Jenes soll in besonders krassen Fällen beruflicher Benachteiligung bis heute fortdauernde Folgen ausgleichen oder doch mildern; dieses soll in sonstigen Fällen grob rechtsstaatswidriger Verwaltungsmaßnahmen der DDR ausnahmsweise eine Überprüfung ermöglichen (vgl. auch Art. 19 EVertr) und bis heute nachwirkende Folgen durch Ausgleichsleistungen mildern. Zuständig für Leistungen nach dem Strafrechtlichen Rehabilitierungsgesetz ist in Sachsen die Staatsanwaltschaft bei dem Oberlandesgericht Dresden; als Rehabilitierungsbehörde nach dem Verwaltungsrechtlichen und nach dem Beruflichen Rehabilitierungsgesetz fungiert das *Landesamt für Familie und Soziales*.

Die Ausführung der drei Rehabilitierungsgesetze wirft schwierige datenschutzrechtliche Fragen auf.

Eine davon ergibt sich aus folgendem: Alle drei Gesetze erklären Ansprüche auf Ausgleichsleistungen (§ 16 Abs. 2 StrRehaG) bzw. Folgeansprüche (§ 2 Abs. 2 VwRehaG) bzw. Leistungen nach dem Beruflichen Rehabilitierungsgesetz (§ 4 BerRehaG) für ausgeschlossen, wenn der Berechtigte (Verfolgte) selbst gegen die Grundsätze der Menschlichkeit oder Rechtsstaatlichkeit verstoßen oder aber eine Machtstellung schwerwiegend zum eigenen Vorteil oder zum Nachteil eines anderen mißbraucht hat (wofür auch die Zeit *vor* dem 8. Mai 1945 in Frage kommt).

Auch das Vorliegen solcher Ausschlußgründe hat die Rehabilitierungsbehörde von Amts wegen zu prüfen.

Eine durch den BStU Ende 1993/Anfang 1994 untersuchte Stichprobe hat ergeben, daß ein weit höherer Prozentsatz als erwartet, nämlich 9 v. H. der Antragsteller nach dem Strafrechtlichen Rehabilitierungsgesetz aktenkundig für das MfS tätig gewesen ist. Aufgrund dieser Erkenntnisse hat man für die Rehabilitierungsbehörden Fragebögen entworfen, in denen die Antragsteller von der Behörde - unter Hinweis auf die Freiwilligkeit der Beantwortung - nach Umständen gefragt werden, die einen *Anfangsverdacht* begründen, daß der eine oder der andere der beiden genannten Ausschlußtatbestände erfüllt ist.

So wird nach einer etwaigen Rückwanderung aus Westdeutschland in die DDR, nach dem beruflichen Werdegang (der trotz einer politisch bedingten Verurteilung möglicherweise systemnah verlaufen sein könnte), nach der Ausübung bestimmter Funktionen im SED-

oder NS-Staat, nach Tätigkeit für das MfS oder die Abteilung K 1 der Volkspolizei gefragt.

An der Ausgestaltung dieser (überwiegend ländereinheitlich verwendeten) Fragebögen bin ich vom SMJus und vom SMS rechtzeitig beteiligt worden. Wie auch der BfD habe ich mich den Erfordernissen, die sich bei der Ausführung dieser Gesetze ergeben, nicht verschließen können. Meine Bedenken gegen die rechtliche Gründung dieser Datenerhebung auf *die Einwilligung* des Antragstellers habe ich zurückgestellt.

Rechtlich noch schwierigere Fragen hat dann das Landesamt für Familie und Soziales aufgeworfen, als es anfragte, ob es die Namen derjenigen in einer gesonderten Datei speichern darf, die ein Antragsteller zur Begründung eines Antrages gegenüber der Rehabilitierungsbehörde als "Werkzeuge des SED-Unrechtsregimes" genannt hat. Mittels dieser Datei möchte die Behörde für jeden Antragsteller prüfen können, ob er von einem anderen Antragsteller der Behörde gegenüber in einer Weise genannt worden ist, die einen Anfangsverdacht begründet, daß einer der Ausschlußtatbestände erfüllt sein könnte.

Aus Gründen, die hier im einzelnen darzulegen zu weit führen müßte, habe ich der Einrichtung und Benutzung dieser Datei zugestimmt.

11 Landwirtschaft, Ernährung und Forsten

11.1 Die sogenannten Pachtausschüsse

Bekanntlich verpachtet die inzwischen in "Bundesanstalt für vereinigungsbedingte Sonderaufgaben (BVS)" umbenannte Treuhandanstalt (THA) die landwirtschaftlich genutzten Grundstücke, die früher in Volkseigentum standen (unmittelbares THA-Eigentum auf der Grundlage der 3. DVO zum Treuhandgesetz). Gesetzliche Vorgabe dabei ist § 1 Abs. 6 TreuhG sowie das sogenannte Eigentumsübertragungsgesetz vom 22. Juli 1990.

Die Treuhandanstalt hat mit der Durchführung (vertraglich) eine ihrer 'funktionalen Beteiligungsgesellschaften' beauftragt, die auch nach der Umstrukturierung der THA/BVS unverändert bestehende Bodenverwertungs- und -verwaltungs GmbH (BVVG). Diese hat sich dabei nach einer "Richtlinie" der THA/BVS zu richten, die unter anderem vorschreibt, nach welchen Gesichtspunkten unter mehreren in Frage kommenden Pacht-Bewerbern auszuwählen ist. Als Verfahrensweise ist der BVVG dabei vorgeschrieben, einer zuständigen Landesbehörde die ihr vorliegenden Pacht-'Anträge' mitsamt einer ersten Bewertung vorzulegen, damit diese dann, unter Einhaltung der in der Richtlinie vorgegebenen materiellen Auswahlregeln, der BVVG eine fachliche Stellungnahme mitsamt Entscheidungsvorschlag unterbreitet; von diesem darf die BVVG nur nach Rücksprache mit dem jeweiligen Landwirtschaftsministerium abweichen.

In Sachsen sind die ÄfL die von der BVVG einzuschaltende Behörde.

Durch einen von einer Landtagsfraktion eingebrachten Antrag und dessen Beantwortung durch die Staatsregierung erfuhr ich nun davon, daß - wie sich herausstellte übrigens ähnlich wie in den anderen neuen Bundesländern - in Sachsen "bei" den staatlichen Ämtern für Landwirtschaft sogenannte "Pachtausschüsse" gebildet worden sind, in denen mit "Vertretern der berufsständischen Interessenvertretungen" der Landwirte (landwirtschaftlichen Unternehmer) die zunächst von den ÄfL im Hinblick auf die jeweiligen Vorlagen der BVVG erarbeiteten (Empfehlungs-)Vorschläge beraten werden.

Eine solche Beratung und Entscheidung kann selbstverständlich nicht stattfinden, ohne daß nähere Angaben über Person oder Betrieb der Pachtbewerber geprüft werden: Betriebskonzept sowie kraft Eigentums oder Pachtvertrages schon zur Verfügung stehende Betriebsflächen spielen eine maßgebende Rolle. Es werden also personenbezogene Daten weitergegeben. Und zwar von einer Behörde an Privatleute:
Die von keinem Gesetz und keiner Rechtsverordnung vorgesehenen "Pachtausschüsse" beziehungsweise die ihnen angehörenden Vertreter der bäuerlichen Standesorganisationen sind rechtlich gesehen ausschließlich als Privatpersonen tätig. Die Übermittlung personenbezogener Daten durch öffentliche Stellen an solche Privatpersonen erlaubt § 15 Abs. 1 SächsDSG auf zwei verschiedenen juristischen Wegen. Der erste, § 15 Abs. 1 Nr. 1 SächsDSG, setzt voraus, daß die Übermittlung zur Erfüllung der Aufgaben erforderlich ist, die der öffentliche Stelle (sc. kraft Gesetzes) zukommen. Schon daran fehlt es: Das zuständige AfL wird in der Regel über die zur fachlichen Stellungnahme erforderlichen Kenntnisse selbst verfügen. Verfügt die Verwaltungsbehörde, hier das AfL,

ausnahmsweise nicht über die erforderliche Sachkenntnis, so hat sie sich diese im Wege eigener Ermittlungen, durch unabhängige Gutachter oder durch Amtshilfe anderer Behörden zu beschaffen. Die Einbindung Privater in die Entscheidungsfindung widerspricht dagegen dem *Grundsatz der Eigenverantwortlichkeit der Verwaltung.*

Der andere Weg ist durch § 15 Abs. 1 Nr. 2 SächsDSG dann eröffnet, wenn der Empfänger der zu übermittelnden Daten ein berechtigtes Interesse an deren Kenntnis hat oder doch zumindest glaubhaft darlegt *und* der Betroffene kein schutzwürdiges Interesse am Unterbleiben der Übermittlung hat. Ich kann mir kaum vorstellen, daß diese Voraussetzungen im Fall der Pachtausschüsse je erfüllt sein könnten: Entweder gehen die Privatperson, die das Pachtausschußmitglied nun einmal darstellt, die betrieblichen Verhältnisse der Pachtbewerber gar nichts an, oder sie ist persönlich sogar auf dem Markt für landwirtschaftliche Erzeugnisse selbst Wettbewerber des einen oder anderen Pachtbewerbers oder doch solchen Wettbewerbern irgendwie verbunden.
(Eine Beurteilung der Datenübermittlung nach § *13* SächsDSG führte zu keinem anderen Ergebnis!)

Mag der Zuschlag der Pachtfläche auch ein örtliches Politikum sein; die Verantwortung dafür, aus dem Kreis der Pachtbewerber den Richtigen auszuwählen, trägt die BVVG (und das genehmigende AfL). Die Abwälzung dieser Verantwortung auf einen "Ausschuß", der die Daten der Bewerber angeblich fachbezogen, häufig aber parteiisch, nach irgendeinem Proporz ("keine Wessis, abwechselnd LPG-Nachfolger, Nebenerwerbler und Wiedereinrichter") oder gar aus Konkurrenzneid auswerten und jedenfalls ohne rechtliche Bindung entscheiden könnte, kommt aus datenschutzrechtlichen Gründen nicht in Betracht.

Ich habe das SML daher aufgefordert, entweder von den landwirtschaftlichen Pachtausschüssen Abschied zu nehmen oder sie auf eine hinreichend bestimmte gesetzliche Grundlage zu stellen.

Nach Verabschiedung des Entschädigungs- und Ausgleichsleistungsgesetzes (EALG) habe ich zusätzlich darauf hingewiesen, daß die rechtlich einwandfreie Gestaltung des Zustandekommens der Pachtverträge mit der THA/BVS nunmehr noch größerer Sorgfalt bedürfe, weil durch die später gegebenen erleichterten Eigentumserwerbsmöglichkeiten für die Pachtbewerber noch mehr als bisher auf dem Spiele steht (vgl. § 3 EALG).

Darüber hinaus habe ich auch auf das Problem des Verhältnisses zum Verwaltungsverfahren nach dem Landpachtverkehrsgesetz hingewiesen: Nicht nur, daß § 4 LPachtVG schon eine ausreichende Rechtsgrundlage für eine zweckentsprechende Überprüfung der von der BVVG abgeschlossenen Landpachtverträge darstellt - vor allem geht es nicht an, daß der jeweilige Vertreter des Amtes für Landwirtschaft im unzuständigen Pachtausschuß eine Empfehlung abgibt und dann anschließend, nunmehr in der Tat zuständig, den von ihm empfohlenen Landpachtvertrag im Rahmen des Verwaltungsverfahrens nach dem Landpachtvertragsgesetz (Beanstandungsverfahren nach § 7) zu prüfen und faktisch zu genehmigen hat.

Das SML hat eingewandt, diese Praxis könne rechtmäßig doch auf der Grundlage einer Einwilligung der Pachtbewerber in die Bekanntgabe ihrer Daten an die Mitglieder der Pachtausschüsse durchgeführt werden. Dem mußte ich zweierlei entgegenhalten.
Zunächst: Die nach § 4 Abs. 2 Satz 2, § 11 Abs. 2 Satz 2 SächsDSG erforderliche Freiwilligkeit einer wirksamen Einwilligung - und dies Freiwilligkeitserfordernis für eine wirksame Einwilligung gilt in allen Rechtsgebieten - ließe sich nur gewährleisten, wenn Pachtbewerbern, die einer Bekanntgabe an den Pachtausschuß nicht zustimmten, dieselben Erfolgsaussichten eingeräumt würden wie solchen, die die Einwilligung nicht verweigerten. Das aber bedeutet: Das Verfahren auf die Grundlage der Freiwilligkeit zu stellen hieße es abzuschaffen, sobald auch nur der erste Bewerber von der Möglichkeit Gebrauch machte, seine Einwilligung zu verweigern. Dementsprechend hat das SML mir gegenüber auch nie eindeutig und konkret behauptet, rechtsgültige Einwilligungen der Pachtbewerber lägen vor.

Zum anderen habe ich dem SML im einzelnen dargelegt, daß es der öffentlichen Verwaltung aus Gründen ihrer *Gesetzesbindung* und des sogenannten *Vorbehaltes des Gesetzes (Wesentlichkeitsdoktrin* des Bundesverfassungsgerichts) verwehrt ist, ein Verwaltungsverfahren einzurichten, das strukturell den durchgängigen Verzicht der verfahrensbeteiligten Privaten auf eines ihrer Grundrechte - hier dasjenige auf informationelle Selbstbestimmung - zur Voraussetzung hat.

Nach langer Zeit, in der man in Zeitungen einiges lesen konnte, wonach es bei der Umgestaltung der Landwirtschaft in den neuen Bundesländern und namentlich bei der Verpachtung vielfach nicht mit rechten Dingen zugeht ("Bauern, Bonzen und Betrüger"), hat mir das SML dann im Februar 1995 mitgeteilt, es werde die Pachtausschüsse die schon laufenden Verfahren noch zu Ende führen lassen und sie dann auflösen.

Ich werde das überprüfen.

11.2 Verdacht einer strafbaren Datenübermittlung aus dem SML an einen privaten Dritten

Im Berichtszeitraum wurde ich mit einer mutmaßlichen rechtswidrigen Übermittlung in amtlicher Eigenschaft erhobener personenbezogener Daten durch einen Bediensteten des SML an eine private Stelle befaßt, wobei es sich möglicherweise sogar um eine gemäß § 203 Abs. 2 StGB (unbefugtes Offenbaren von Privatgeheimnissen durch Amtsträger und gewisse amtsnahe Personen) strafbare Übermittlung handelt.

Nachdem Betroffene sich beschwert hatten und diese Beschwerden vom Ministerium zweimal schriftlich zurückgewiesen worden waren, hatten sie Strafantrag gestellt. Die Staatsanwaltschaft hatte das Ermittlungsverfahren jedoch eingestellt und die Sache im Hinblick auf § 32 Abs. 1 Nr. 1 Buchst. a, Abs. 3 SächsDSG an das zuständige Regierungspräsidium als die insoweit zur Verfolgung von Ordnungswidrigkeiten zuständige Behörde abgegeben.
Nachdem ich auf den Vorgang aufmerksam gemacht worden war, habe ich eigene datenschutzrechtliche Ermittlungen aufgenommen, die noch nicht abgeschlossen sind. Die

von mir gemäß § 25 Satz 2 Nr. 1 SächsDSG angeforderte Stellungnahme des SML läßt zur Zeit unangemessen lange auf sich warten.

11.3 Forstaufsicht und Forstförderung

Zu Beginn des Berichtszeitraums übersandte mir das SML den Entwurf eines "Organisationserlasses über die Einrichtung der organisatorischen Einheit 'Forstaufsicht' in den Forstdirektionen Bautzen und Chemnitz" sowie Entwürfe verschiedener Antragsvordrucke aus dem Bereich der Forstförderung, nachdem ich seit längerem hierum gebeten hatte.

Der Entwurf des Organisationserlasses sah unter anderem vor, die (staatliche) Forstaufsicht über den Wald der Gemeinden und den Privatwald (§ 40 Abs. 1 SächsWaldG) in den beiden sächsischen Forstdirektionen Bautzen und Chemnitz von dem "Sachgebiet Recht" wahrnehmen zu lassen. Gegenüber dem SML habe ich darauf hingewiesen, daß diese Organisationsregelung mit § 37 Abs. 2 Sätze 2 und 3 SächsWaldG unvereinbar ist. Danach wird sowohl die Aufgabe der Forstaufsicht als auch die der Durchführung forstlicher Förderungsmaßnahmen von *je einer organisatorischen Einheit der höheren Forstbehörde wahrgenommen; diese Einheiten dürfen jeweils keine anderen Aufgaben erfüllen*. Mit dieser Vorschrift soll verhindert werden, daß der Staat als Waldbesitzer und Marktbeherrscher solche Daten, die er in seiner Eigenschaft als Aufsichtsführender erhoben hat, zu Konkurrenzzwecken mißbraucht. Zu diesem Zwecke müssen die Aufgaben der Forstförderung, bei der der Staat Subventionen an kommunale und private Waldbesitzer zahlt, von den übrigen Aufgaben der Forstbehörden getrennt werden. Außerdem müssen beide Aufgaben von der Forstdirektion und nicht von dem örtlich zuständigen Forstamt wahrgenommen werden (§ 37 Abs. 2 Satz 2 SächsWaldG).

Von der Praxis der Forstaufsicht und -förderung habe ich mich an Ort und Stelle bei einer Forstdirektion ein ungefähres Bild verschafft. Ich habe mich davon überzeugt, daß der dort für die Forstaufsicht zuständige Jurist zwar Querschnittsaufgaben wahrnimmt, aber wohl keine Forstbetriebsdaten des Privat- oder Körperschaftswaldes verarbeitet.

Die mir neben dem "Organisationserlaß" gleichfalls zur Prüfung übersandten "Verfahrensbestimmungen für die forstliche Förderung" und die einzelnen Antragsformulare waren in zweierlei Hinsicht problematisch: Zum einen enthielten die Förderantragsformulare einige Fragen, die ich als zur Aufgabenerfüllung der Forstbehörden insoweit nicht erforderlich angesehen habe. Zum anderen war vorgesehen, daß praktisch alle Anträge auf Forstförderung bei dem zuständigen Forstamt, also einer unteren Forstbehörde, abgegeben, dort mit einer forstfachlichen Stellungnahme versehen und sodann an die zuständige Forstdirektion weitergeleitet werden sollten. Hier habe ich auf folgendes hingewiesen: Bewilligungsbehörden für die Forstförderung sind ausschließlich die Forstdirektionen, nicht die Forstämter. Dies ergibt sich zwingend aus § 37 Abs. 2 Satz 2 SächsWaldG. Das Forstamt kann allenfalls als "Postbote" fungieren und darf die Daten des Antrages nicht zur Kenntnis nehmen. Ich weiß, was die Forstpraktiker denken und sagen, wenn ich dies fordere. Dennoch: Vielleicht lohnt es sich, über Grundrechte und ihre ganz praktische Umsetzung im Alltag nachzudenken. Schon der Anschein, das Forstamt sei allzuständig, allwissend und allmächtig, ist ein Greuel für

jeden, der sich der Ordnungspolitik einer freiheitlichen Wirtschaftsordnung verpflichtet weiß. Die Regelung, wonach Anträge auf Forstförderung auch beim Forstamt gestellt werden können und dort vorab mit einer Stellungnahme des Forstamtsleiters versehen werden, ist rechtswidrig und der abgesegnete Versuch einer Gesetzesumgehung. Die Entgegennahme der Förderanträge durch Forstämter, häufig verbunden mit einer Erstbearbeitung durch eine forstfachliche Stellungnahme, würde den Forstämtern in der Praxis eine Verfahrensstellung zuwachsen lassen, die ihnen gesetzlich nicht zukommt. 'Herrin des Verfahrens' ist gemäß § 37 Abs. 2 Satz 2 SächsWaldG vielmehr ausschließlich die Forstdirektion. Es ist allenfalls zulässig, daß im Einzelfall forstfachliche Stellungnahmen durch die Forstämter erstellt werden. Dabei muß sichergestellt sein, daß die Forstämter nur die zur Erfüllung dieser Aufgabe erforderlichen Daten des Waldbesitzers erhalten.

Das SML hat mir zugesichert, die Antragsformulare für die Forstförderung und die Verfahrensbestimmungen in diesem Sinne neu zu fassen und mir zu übersenden. Diese Zusage, die aus der Mitte des Berichtszeitraums stammt, ist bis heute nicht erfüllt worden, ohne daß mir eine Erklärung dafür mitgeteilt worden wäre.

11.4 Überwachung der Betriebe des ökologischen Landbaus

Im Berichtszeitraum habe ich zu dem Entwurf einer Verwaltungsvorschrift des SML für das Zulassungs- und Kontrollverfahren nach der EG-Verordnung Nr. 2092/91 über den ökologischen Landbau und seine Erzeugnisse Stellung genommen. Aufgrund der genannten EG-Verordnung können in Sachsen ökologisch wirtschaftende landwirtschaftliche Unternehmen auch von privaten Kontrollstellen kontrolliert werden. Die privaten Kontrollstellen werden durch die Sächsische Landesanstalt für Landwirtschaft als solche zugelassen. Sie führen bei den Öko-Bauern die Kontrolle als beliehene Unternehmen und damit als öffentliche Stellen im Sinne des § 2 Abs. 1 SächsDSG (vgl. hierzu Abschnitt 13 meiner Bekanntmachung zur Datenverarbeitung im Auftrag [§ 7 SächsDSG] und zur Rechtsstellung des beauftragten Unternehmens [§ 2 Abs. 2 SächsDSG] SächsAbl. 1993, S. 1304) durch. Ich habe deshalb darauf hingewiesen, daß die Mitarbeiter der privaten Kontrollstellen nach dem Gesetz über die förmliche Verpflichtung nichtbeamteter Personen zu verpflichten sind.

Die Verwaltungsvorschrift enthielt ein Muster der Meldung, die die Öko-Landwirte der Landesanstalt für Landwirtschaft machen müssen. Während gemäß Anhang IV zur EG-Verordnung Nr. 2092/91 lediglich Angaben über die "Lage der Betriebe und gegebenenfalls der Parzellen (Katasterangaben)" vorgeschrieben sind, forderte das Musterformular die Beifügung von Katasterauszügen bzw. Kopien des neuesten Flächen- und Nutzungsnachweises zum Antrag auf Agrarförderung. Ich habe darauf gedrungen, daß klargestellt wird, daß die formlose Angabe der Katasterdaten im Sinne eines hinreichend genauen und verständlichen Planes (Lage, Flurstücknummer) ausreicht und die Vorlage von Katasterauszügen oder Kopien des neuesten Flächen- und Nutzungsnachweises nicht nötig ist. Ich habe ferner den Text der formularmäßig vorgesehenen Verpflichtung, "bei Betriebskontrollen alle erforderlichen Auskünfte zu erteilen ..." als zu unbestimmt bemängelt und einen Text vorgeschlagen, aus dem sich unter Bezugnahme auf die entsprechende Vorschrift der EG-Verordnung ergibt, daß nur

die zur Durchführung der darin vorgeschriebenen Kontrollen erforderlichen Auskünfte zu erteilen sind und insoweit Einsicht in Geschäftsunterlagen zu gewähren ist.

Das SML hat mir mitgeteilt, daß alle meine Anregungen in der überarbeiteten Fassung der Verwaltungsvorschrift berücksichtigt worden seien. Warum mir das SML trotz wiederholter Bitten kein Exemplar der überarbeiteten Verwaltungsvorschrift hat zukommen lassen, kann ich mir nicht erklären.

12 Umwelt und Landesentwicklung

12.1 Das Umweltinformationsgesetz

Seit dem 16. Juli 1994 ist das *Gesetz zur Umsetzung der Richtlinie 90/313/EWG des Rates vom 7. Juni 1990 über den freien Zugang zu Informationen über die Umwelt* vom 8. Juli 1994 (BGBl. I 1490) in Kraft, das im wesentlichen aus dem *Umweltinformationsgesetz* (UIG) besteht. Die im 2. Tätigkeitsbericht (Kapitel 12) erörterten Fragen der unmittelbaren Anwendung der genannten Richtlinie stellen sich damit nicht mehr, oder doch jedenfalls nicht mehr ohne weiteres.

Diese Einschränkung muß man deswegen machen, weil die vorliegende gesetzliche Regelung keineswegs über jeden verfassungsrechtlichen Zweifel erhaben ist.

Das Gesetz verschafft jedermann einen Anspruch auf freien Zugang zu Informationen über die Umwelt, die bei einer Behörde oder bei einer privaten Stelle vorhanden sind, die für Behörden öffentlich-rechtliche Aufgaben im Bereich des Umweltschutzes wahrnimmt (§ 4 Abs. 1 Satz 1 UIG). Den gebotenen Schutz des Grundrechts auf informationelle Selbstbestimmung versucht das Gesetz dadurch zu gewährleisten, daß es in § 8 Abs. 1 Satz 1 Nr. 1 den Anspruch aus § 4 Abs. 1 Satz 1 insoweit ausschließt, als *durch das Bekanntwerden der Informationen personenbezogene Daten offenbart und dadurch schutzwürdige Interessen der Betroffenen beeinträchtigt würden*.

Unverändert stehe ich dem Anspruch auf freien Zugang zu behördlichen Informationen über die Umwelt, soweit es um personenbezogene Daten geht, skeptischer gegenüber als die meisten meiner Kollegen. Daher habe ich auch keinerlei Schwierigkeiten, nachzuvollziehen, wenn ein ausgewiesener Kenner der Materie die Regelung des Anspruchsausschlusses in § 8 Abs. 1 Satz 1 Nr. 1 für *verfassungswidrig* hält; und zwar für verfassungswidrig wegen Verstoßes gegen das rechtsstaatliche Bestimmtheitsgebot des Grundgesetzes, das bekanntlich (vornehmlich unter der Bezeichnung "Gebot der Normenklarheit") gerade beim Grundrecht auf informationelle Selbstbestimmung eine besondere Rolle spielt (Einzelheiten bei Scherzberg, Das neue Umweltinformationsgesetz, DVBl. 1994, 733, 740/741). Der Gesetzgeber des UIG hat sich nämlich darauf beschränkt, die von Verfassungs wegen ohnehin bestehende Abwägungsaufgabe zu formulieren, ohne die Abwägung in ihren Grundzügen selbst vorzunehmen, obwohl er das, anders als im allgemeinen Datenschutzrecht, durchaus hätte tun können. Denn der besondere Verwendungszusammenhang der Daten und das öffentliche Interesse an ihrer Übermittlung steht, eben anders als im allgemeinen Datenschutzrecht, für den Anwendungsbereich der Übermittlungserlaubnis (§ 4 Abs. 1 Satz 1 UIG) bzw. des Abwägungsgebotes (insoweit § 8 Abs. 1 Satz 1 Nr. 1 UIG) - bereichsspezifisch - von vornherein fest. Der Gesetzgeber hat mithin eine nur formell bereichsspezifische Regelung der Datenübermittlung geschaffen. Den eigentlichen Zweck bereichsspezifischer Regelungen (die ja kein Selbstzweck sind!), nämlich größere inhaltliche Bestimmtheit zu ermöglichen, hat er aber gerade *verfehlt*.

Eine ganz ähnliche mangelnde Bestimmtheit weist wohl auch § 8 Abs. 1 Satz 2 UIG auf (vgl. Scherzberg a.a.O. S. 743, sowie Fluck, Der Schutz von Unternehmensdaten im Umweltinformationsgesetz, NVwZ 1994, 1048, 1055).

Solche "salvatorischen Klauseln" sind beim Gesetzgeber (und beim Entwurfsverfasser) immer dann beliebt, wenn Zielkonflikte zwar erkannt, aber aus Faulheit (sic!) oder politischer Opportunität nicht gelöst werden; man überläßt die Arbeit dann lieber den Gerichten ...

In Gestalt der in § 4 Abs. 1 Satz 1 UIG ausgesprochenen Verpflichtung der Behörde zur Datenübermittlung an den Anspruchsinhaber *ermächtigt* das Gesetz zugleich zum Eingriff in das Grundrecht auf informationelle Selbstbestimmung. Der Umfang dieser Ermächtigung wird inhaltlich begrenzt durch den Anspruchsausschluß in § 8 Abs. 1 Satz 1 Nr. 1 UIG. Beide Rechtssätze *zusammen* enthalten die gesetzliche Bestimmung der Voraussetzungen des Grundrechtseingriffs. (Von anderen, weniger wichtigen Rechtssätzen, die § 4 Abs. 1 Satz 1 ergänzen, kann in diesem Zusammenhang abgesehen werden.) Ist nun dieser Anspruchsausschluß infolge mangelnder Bestimmtheit verfassungswidrig, so überträgt sich entweder die Unbestimmtheit auf die Anspruchs-Norm des § 4 Abs. 1 Satz 1 UIG, oder aber diese Vorschrift ist, mangels jeglicher rechtswirksamer Einschränkung zugunsten des Grundrechts auf informationelle Selbstbestimmung eine mangels Verhältnismäßigkeit grundrechtswidrige Eingriffsermächtigung. Die zum Grundrechtseingriff ermächtigende Vorschrift müßte daher *nichtig sein*, ein Anspruch auf Übermittlung *personenbezogener* Daten bestünde demnach *nicht.*

Ich bin gespannt, wie die weitere Diskussion dieser Fragen verlaufen wird und wie vor allem die Gerichte entscheiden werden.

12.2 Erfassung der individuell verursachten Abfallmengen

Gemäß § 1 Abs. 1 Satz 1 EGAB hat die Abfallwirtschaft in Sachsen *vorrangig zum Ziel, die Abfallmenge und den Schadstoffgehalt in Abfällen so gering wie möglich zu halten (Abfallvermeidung)*. Zu diesem Zweck haben gemäß § 3 Abs. 2 Satz 5 EGAB die Landkreise und kreisfreien Städte als die entsorgungspflichtigen Körperschaften *durch die Gebührengestaltung nachhaltige Anreize zur Vermeidung und Verwertung von Abfällen zu schaffen*. Die Landkreise und kreisfreien Städte sind danach verpflichtet, Abfallgebührenberechnungssysteme, die keinen Bezug zur individuell verursachten Abfallmenge aufweisen, abzuschaffen und durch Gebührensysteme zu ersetzen, die den Einzelnen um so stärker belasten, je mehr Abfall er verursacht. Die bisher übliche pauschale Belastung des einzelnen Haushalts mit einer der Höhe nach im voraus festgelegten Abfallgebühr soll also entfallen und durch eine Gebühr auf der Grundlage der individuell erzeugten Abfallmenge ersetzt werden.

In Sachsen hat derzeit, soweit mir bekannt, allein die Stadt Dresden ein Abfallmengen-erfassungssystem eingeführt, bei dem die Abfallbehälter mit Chips ausgerüstet wurden, so daß sie bei der Leerung einem bestimmten Haushalt zugeordnet werden können. Den privaten Entwickler des Systems habe ich beraten. Einige weitere Städte (z. B. Hoyerswerda) bereiten derzeit die Erprobung unterschiedlicher anderer Abfallmengenberechnungssysteme vor.

Aus Datenschutzgründen sind Systeme, bei denen personenbezogene Daten verarbeitet werden müssen, nach Möglichkeit zu vermeiden - zugunsten einfacherer Systeme, die z. B. mit einer münzähnlichen Marke (Jeton) oder einer Guthabenspeicherkarte (ähnlich einer Telefonkarte) betrieben werden, also eine Erfassung personenbezogener Daten entbehrlich machen, und übrigens auch kostengünstiger sind.

Wegen dieser Erprobungen stehe ich in Kontakt mit dem SMU und dem Landesamt für Umwelt und Geologie. Beide Behörden zeigen sich dabei dem Anliegen einer datenschutzgerechten - und einfachen - Gestaltung der Abfallgebührenberechnung aufgeschlossen. Wenn erste Erfahrungen mit automatisierten Abrechnungssystemen vorliegen, werde ich mich an Ort und Stelle im einzelnen kundig machen.

13 Wissenschaft und Kunst

13.1 Schulforschung: Befragung an Mittelschulen

Die Tendenz zu mehr Befragungen stellte ich auch im Bereich der Bildungs- und Schulforschung fest.

Das SMK bat mich um Beratung zu einer wissenschaftlichen Untersuchung über die Situation von Schülerinnen und Schülern an den sächsischen Mittelschulen, ihrer Eltern und der Lehrer -leider erst kurz vor Drucklegung der Fragebögen.

Das SMK befragt durch eine Universität Schüler der 6. und 9. Klasse an ausgewählten Mittelschulen und zum Vergleich an Gymnasien, z. B. wie es ihnen an der Schule gefällt, wie sie die Schule und das Verhältnis zu den Eltern beurteilen, welche Pläne sie für die Zukunft haben. Auf einem 21seitigen Fragebogen werden außerdem die Mittelschüler der 9. Klasse befragt. Ein Fragebogen richtet sich an die Lehrerinnen und Lehrer, ein anderer an die Eltern der Mittelschüler.

Meine zahlreichen datenschutzrechtlichen Hinweise zur Gestaltung der Anschreiben und der Befragung wurden von den Forschern in das Projekt eingearbeitet. Die Eltern der Schüler der 6. Klasse werden zwei Wochen vor der eigentlichen Befragung ihrer Kinder informiert, um Einverständnis zu dieser Befragung gebeten und ausdrücklich auf die Freiwilligkeit hingewiesen. Sie werden ferner darüber informiert, daß die Befragung ohne Namensangabe erfolgt, die Fragebögen nach der Auswertung vernichtet werden und nur Forscher Einblick in die Unterlagen nehmen, die zur absoluten Vertraulichkeit verpflichtet sind.

Die Einhaltung von § 9 SächsDSG ist im Projekt gewährleistet. Das betrifft u. a. Einzelheiten des Ablaufs der Befragung, die Aufbewahrung und Auswertung der Daten mit Computerprogrammen und die Löschung personenbezogener Daten aus dem Forschungsprojekt. Z. B.: Die Briefumschläge der ausgefüllten Elternfragebögen werden sofort nach ihrem Posteingang vernichtet. Das Forschungsteam übernimmt die Fragebögen ohne Umschläge. Die ausgefüllten Fragebögen werden gesichert transportiert. Nach der Dateneingabe in den Rechner kommen die Fragebögen in den Reißwolf.

Es besteht Einigkeit, daß eine Kontaktaufnahme mit dem Sächsischen Datenschutzbeauftragten schon in der Planungsphase solcher Befragungen zweckmäßig ist. In einem frühen Projektstadium im Sinne eines vorbeugenden Datenschutzes zu wirken ist besser als später Korrekturen an einem schon laufenden Projekt zu versuchen. "Prophylaktischer Datenschutz ist besser als therapeutischer Datenschutz."

13.2 Befragung chronisch mehrfach geschädigter Abhängigkeitskranker

Immer häufiger erreichen mich auch Anfragen zu Forschungsvorhaben im Sozialbereich. Zuweilen wird den Forschern erst kurz vor Beginn einer Befragung bewußt, daß Untersuchungen zur sozialen Situation in der Regel mit Datenschutzproblemen verbunden

sind. Problematisch sind die für eine wirksame Einwilligung der Befragten entscheidenden ausreichenden und für sie verständlichen Informationen, die Gestaltung der benutzten, möglichst anonymen Fragebögen, ein datenschutzgerechter Verfahrensablauf der Befragung, die Auswertung und Vernichtung der Klardaten und schließlich die Weitergabe der anonymisierten Ergebnisse und deren Nutzung.

Über Anzahl und Situation mehrfach geschädigter "Suchtkranker", insbesondere aus dem Kreis der Obdachlosen, gibt es in Sachsen keine ausreichenden empirischen Erkenntnisse, um damit die erforderliche Hilfe und psychiatrische Betreuung planen zu können. Im Rahmen einer Pilotstudie sollten von einer Universität entsprechende Befragungen und Datenerhebungen in den Suchtberatungsstellen einer Großstadt durchgeführt werden. Die Studenten sollten Befragungen und Datensammlungen in einem Forschungspraktikum durchführen.

Die Befragung betraf einen Gesundheits- und Sozialbereich, der besonders strengen Schweigepflichten unterliegt (z. B. ärztliche Schweigepflicht nach § 203 StGB, Sozialdatengeheimnis nach § 35 SGB I, § 67 ff. SGB X). Eine Einwilligungslösung war vorgesehen. Die Verhaltensspezifik und die besonderen sozialen Situationen mehrfach geschädigter Abhängigkeitskranker mußten dabei berücksichtigt werden.

In intensiver Zusammenarbeit mit dem Leiter des Forschungsprojekts und dem Geschäftsführer eines Vereins zur sozialen Rehabilitation haben wir eine Lösung gefunden, die folgenden datenschutzrechtlichen Anforderungen genügt:

1. Ausreichende schriftliche Information der Probanden (vor ihrer Einwilligung zur Befragung) und verständliche Aufklärung über den gewünschten Zweck der Untersuchung, über die Anonymität der Auswertungsergebnisse und die Adressaten der Ergebnisse. Enthalten ist der Hinweis auf die Möglichkeit, sich bei Fragen an die Mitglieder der Forschungsgruppe zu wenden. Die Teilnahme an der Befragung ist freiwillig, aus der Nichtteilnahme entstehen den Angesprochenen keinerlei Rechtsnachteile. Jeglicher Druck auf die möglichen Probanden, an der Befragung teilzunehmen, soll ausgeschlossen werden. Dies garantiert im übrigen wahrheitsgemäße Mitarbeit. Die Informationsschreiben wurden durch die Beratungsstellen versandt.
2. Der Befragungsbogen ist so gestaltet, daß er - soweit es der Forschungszweck gestattet - keine personenbezogenen oder personenbeziehbaren Daten enthält. Eine Deanonymisierung mittels Detailangaben über die Probanden wird durch den Verzicht auf direkt personenbeziehbare Angaben erschwert (z. B. statt der Angabe des Geburtsortes die Verwendung eines Gruppenmerkmals wie "Ländliche Gemeinde", "Kleinstadt" oder "Großstadt").
3. Der Umgang mit den personenbezogenen Daten insbesondere bei Erhebung, Speicherung, Transport, Auswertung und Löschung ist präzis festgelegt.
   Alle Teilnehmer am Projekt unterschreiben eine Verschwiegenheitserklärung. Identifizierende Merkmale wie z. B. die Initialen der Probandennamen, die benötigt werden, um störende Mehrfacherfassungen auszuschließen, werden nach Vergabe einer Fallnummer vom Fragebogen getrennt und auch getrennt gespeichert. Ein Zugriff ist nur dem Projektleiter mit Paßwort möglich. Nach Abschluß der Auswertung werden diese Daten gelöscht.

Dieses Beispiel zeigt, daß ich prinzipiell personenbezogene Forschungsarbeiten nicht verhindern, sondern vernünftig fördern will. Ich versuche, auf derartige Forschungsprojekte so Einfluß zu nehmen, daß sie in ihren Details datenschutzgerecht ausgestaltet werden und die unabdingbaren Rechte der Probanden geschützt bleiben. Dies garantiert den Erfolg.

14 Technischer und organisatorischer Datenschutz

14.1 Sicherheit in Netzen / Client-Server-Prinzip

14.1.1 Allgemeines

Personalcomputer (PC) werden in allen Bereichen der öffentlichen Verwaltung eingesetzt und vernetzt. Damit mehrfachgenutzte Datenbestände nur einmal zentral gespeichert und bei Bedarf auch nur ein Mal geändert werden müssen, werden PCs zu sogenannten lokalen Netzen (LAN, Local Area Network) zusammengeschlossen. Bei der lokalen Vernetzung in einem örtlich begrenzten Bereich, z. B. in einer Abteilung oder einem Bürogebäude, hat sich im Gegensatz zum Zentralrechner-Terminal-Prinzip das Client-Server-Prinzip durchgesetzt. Die PCs (Clients) werden dabei an einen zentralen Rechner (File-Server) angeschlossen, der die Programme und Datenbestände verwaltet, die im Netz zur Verfügung stehen sollen. Die eigentliche Programmverarbeitung geschieht im Client, der aber auch netzunabhängig arbeiten kann. Zur Verwaltung der Druckaufträge können außerdem Print-Server und für die Kommunikation mit anderen Netzwerken Kommunikations-Server angeschlossen werden.

14.1.2 Datensicherheitsprobleme lokaler Netze

Übermittlung

Durch die Vernetzung entstehen gegenüber den Einzel-PCs neue Risiken. Augenfällig ist, daß personenbezogene Daten abgehört werden können, sofern sie unverschlüsselt übertragen werden. Das Abhörrisiko kann sowohl von der physikalischen Netzstruktur als auch von der Wahl des Übertragungsmediums beeinflußt werden.

Es wird zwischen vier Grundformen der Netzstruktur unterschieden: Stern, Baum, Bus und Ring.

Bei einem *Sternnetz* sind alle Teilnehmer einer Zentrale zugeordnet und über eine eigene Leitung mit dieser verbunden. Dadurch erfolgt der Datenverkehr nur auf der "eigenen" Leitung und nur diese könnte abgehört werden. Nachteilig wäre der Ausfall der Zentrale, da sämtliche Übertragungswege unterbrochen wären.

Bei einem *Baumnetz* sind die Teilnehmer gruppenweise Netzknoten in Sternform zugeordnet und angeschlossen. Die Netzknoten sind wiederum sternförmig an eine Zentrale angeschlossen, das heißt, zwischen Zentrale und Netzknoten existiert nur eine Leitung und alle Informationen der am Netzknoten angeschlossenen Teilnehmer könnten abgehört werden.

Bei einem *Busnetz* sind alle Teilnehmer an einer gemeinsamen Leitung angeschlossen. Alle teilnehmenden Stationen besitzen eine eigene Netzadresse. Die (adressierten) Datenpakete werden an alle Netzteilnehmer rundgeschickt (Broadcastprinzip). Die Adresse des Datenpaketes wird von den Stationen gelesen. Bei Gleichheit der Adresse mit

der eigenen Netzadresse empfängt die Station die an sie gerichteten Informationen. Da aber alle Informationen über *eine* Leitung laufen, ist das Abhörrisiko groß.

Ein *Ringnetz* ist ein mit beiden Enden verbundener Bus. Der Datenaustausch erfolgt also prinzipiell genauso wie beim Bus. Vorteil dieser Anordnung ist, daß bei Leitungsunterbrechung die Datenübertragung von beiden Seiten bis zur Bruchstelle stattfinden kann. Wie beim Busnetz ist das Abhörrisiko hoch.

Neben der Struktur des Netzes beeinflußt das Übertragungsmedium die Datensicherheit eines lokalen Netzes. Als Übertragungsmedien können Kupferkabel (Twisted-Pair-Kabel), Koaxialkabel und Lichtwellenleiter eingesetzt werden. Kupferkabel kann leicht abgehört werden, indem die Ummantelung aufgetrennt oder unterbrochen und die Abstrahlung aufgefangen wird. Bei Koaxialkabeln ist der Aufwand höher. Die Ummantelung und die Abschirmung des Innenleiters muß mit Spezialwerkzeugen angebohrt und angezapft werden. Beim Lichtwellenleiter ist ein Abhören nur mit hohem technischem Aufwand durch Auftrennen und Zusammenfügen mit besonders aufwendigen Spezialwerkzeugen möglich.

Ein Beispiel für eine Gefährdung beim Anmelden am Netz ist das Abhören des Paßwortes. Wird das Paßwort unverschlüsselt im Netz übertragen, könnte das Paßwort abgehört und mit seiner Hilfe unerlaubter Zugriff auf Daten bzw. Programme erschlichen werden. Deshalb sollte das Paßwort im Netz nur verschlüsselt übertragen werden.

Server- und Clientbetrieb

Wegen der zentralen Speicherung der Benutzerprogramme und -daten auf dem Server konzentriert sich die Gefährdung unmittelbar auf den Server, die Infrastruktur und seine Verwaltung.

Ein Administrator legt üblicherweise die Zugriffsrechte der Benutzer auf Ressourcen, directories, Programme, Daten und periphere Geräte fest. Sie müssen differenziert und aufgabenbezogen vergeben werden. Dadurch können einzelne Datenbestände voneinander abgeschottet und schutzwürdige Belange der Betroffenen berücksichtigt werden.

Der Systemverwalter hat auf sämtliche Dateien des File-Servers fast unbegrenzten Zugriff und dies häufig ohne ausreichende Protokollierung. Deshalb muß der Systemverwalter besonders sorgfältig ausgewählt werden. Nimmt nur *eine* Person die Administration und Systemverwaltung wahr, so besteht eine Aufgabenzentralisierung und damit ein besonders hohes Mißbrauchspotential. Um das Risiko einzuschränken, sollte unbedingt eine Funktionstrennung zwischen Systemverwalter und Administrator erfolgen. In größeren Netzwerken sollte zusätzlich das Vier-Augen-Prinzip, z. B. durch ein geteiltes Paßwort, beachtet werden.

Das Risiko in einem Netz kann aber auch vom berechtigten Benutzer, der nur auf zuvor festgelegte Ressourcen zugreifen kann, ausgehen. Er kann netzweit anderen (unberechtigten) Benutzern seine Ressourcen zur Verfügung stellen.

Ein weiteres Problem kann durch die unzureichende Trennung von Netzbetrieb und Einzelplatz-Betrieb beim PC-Client auftreten. Wird beispielsweise eine Datei mit sensiblen Informationen vom Server auf die Festplatte eines PC kopiert, besteht keinerlei Zugriffsschutz mehr. Jeder Nutzer des PC kann den Inhalt der Festplatte sehen, manipulieren oder löschen. Die Diskettenlaufwerke können beliebig zur Ein- oder Ausgabe von Dateien und Programmen genutzt werden. Auch bei PCs ohne Diskettenlaufwerk könnten über eine ungesicherte serielle oder parallele Schnittstelle ungehindert die Daten übertragen werden, so daß der Zugriff nicht mehr dem festgelegten Zugriffsschutz des Netzes unterliegt (siehe auch 2. Tätigkeitsbericht S.149).

In einigen Netzstrukturen (z. B. Bus, Ring) werden die Adressen von Informationen überprüft, mit der eigenen Netzadresse verglichen und bei Gleichheit wird die gesendete Information vom Teilnehmer empfangen. Durch Manipulationen an der eigenen Netzadresse könnten Zugriffsrechte erschlichen werden. Dadurch wäre es möglich, personenbezogene Daten zu lesen, die für einen anderen Teilnehmer bestimmt waren.

Weitere Probleme können sich durch den Einsatz unterschiedlicher Netzbetriebssysteme (z. B. Novell-Netz, LAN-Manager) ergeben.

14.1.3 Anforderungen an ein lokales Netz

Wichtigster Grundsatz ist, daß eine Vernetzung nur dann zulässig ist, wenn dies der Aufgabe angemessen ist und schutzwürdige Belange der Betroffenen berücksichtigt werden.
Nachfolgend werden Maßnahmen vorgestellt, die der Sicherheit im Client-Server-Netz dienen:

- Identifizierung/Authentifizierung (Benutzerkennung, Paßwort, Chipkarte usw.),
- Benutzer- und Zugriffsrechte festlegen und revisionsfähig aufbewahren,
- Zugriffsberechtigung an bestimmten PC binden,
- Zahl der Anmeldefehlversuche begrenzen,
- keinen Zugriff auf Betriebssystem des PCs - Menüsteuerung,
- Einsatz von PCs ohne Diskettenlaufwerk, Verschluß der Diskettenlaufwerksschächte,
- Bildschirmverdunkelung bei Arbeitsunterbrechung, vor Weiterarbeit Paßworteingabe,

- Server in besonders gesichertem Raum,
  - Zugang nur mit Systempaßwort,
  - Einsatz eines Virensuchprogramms,
  - Gehäuseschloß,
  - USV (unterbrechungsfreie Stromversorgung),
  - regelmäßige Sicherungen (täglich, wöchentlich),
  - Gefahrenmeldeanlage installieren,

- sichere Aufbewahrung der Backup-Datenträger,

- sporadische Überprüfung der Sicherungsdatenträger auf Wiederherstellung,

- Regelungen für Wartungs- und Reparaturarbeiten,

- Schutz der Leitungen (Kabel) in gesicherten Kabelschächten (evtl. Doppelverkabelung),

- Verschlüsselung der Kommunikation für besonders sensible Bereiche vor der Übertragung (und im Netzrechner),

- Dokumentation der Netzwerkstruktur,

- Festlegen der Berechtigten zum Druck der Standardlisten und eigenen Listen,

- Auswahl der Topographie (möglichst sternförmige Verkabelung),

- Auswahl abhörsicherer Übertragungsmedien (Koaxialkabel, Lichtwellenleiter),

- Verwendung abgeschirmter Kabel,

- Schutz der Netzbetriebssystemsoftware gegen Manipulation,

- Zuweisen, Einrichten, Überwachung und Protokollierung von Netzzugangsrechten,

- Protokollierung sämtlicher wichtiger Aktivitäten einschließlich versuchter Zugriffe,

- Auswertung der Protokolle (möglichst automatisiert),

- nicht benutzte Anschlußdosen sind physikalisch abzukoppeln,

Wird netzübergreifend gearbeitet, sollten weitere Maßnahmen beachtet werden.:

- Zutrittsschutz für Kopplungstechnik (Brücken, Router, Gateway),

- Filterung der Informationsströme in der Kopplungstechnik (z. B. nach Quelladresse, Zieladresse, Protokolltyp, Masken),

- bei Wählverbindungen (Modem mit Rückruf, Modem mit Schalter),

- Einrichtung geschlossener Benutzergruppen,

- Einrichtung von Teilnetzen,

- Festlegen berechtigter Personen für den Dateitransfer.

14.2 Protokollierung

14.2.1 Ausgangslage

Die Spannbreite der in der öffentlichen Verwaltung eingesetzten EDV-Technik und ihrer Möglichkeiten ist groß. Dies gilt auch für eine der wichtigsten Sicherheitsmaßnahmen, die Protokollierung. Der einfache MS-DOS-PC auf dem Platz des Sachbearbeiters gewährleistet nicht einmal die primitivsten Sicherheitsanforderungen, geschweige denn Protokollierung; die Großrechneranlage ermöglicht Bewegungsprofile ihrer Nutzer. Häufig bestehen auch bei den Anwendern Unklarheiten und Unkenntnis darüber, ob und wie weit Protokollierung notwendig und möglich ist. Hat der Anwender allerdings die Notwendigkeit der Protokollierung erkannt und will diese bei seiner Datenverarbeitung einsetzen, so steht er bei den Angeboten vor einer verwirrenden Vielfalt von Möglichkeiten. Dies führt dazu, daß Überflüssiges gespeichert, Sinnvolles nicht genutzt, Notwendiges vergessen wird. Um dem abzuhelfen, hat der Arbeitskreis Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder eine Arbeitshilfe zur Protokollierung entwickelt, die - angepaßt an die sächsischen Verhältnisse - die Grundlage der folgenden Ausführungen ist.

14.2.2 Begriffe

Protokollierung beim Betrieb von IT-Systemen ist die Erstellung von manuellen oder automatisierten Aufzeichnungen

- über die tatsächlichen Veränderungen an Hardwarekomponenten (z. B. vorübergehendes Entfernen von Sicherheitselementen wie Diskettenschachtverriegelungen oder ähnlichem) und an der Software (Betriebssystem, systemnahe Software, Anwendungssoftware) sowie
- über die Verarbeitung (Erhebung, Speicherung, Veränderung, Löschung, Sperrung, Übermittlung und sonstige Nutzung) von personenbezogenen Daten.

Elemente einer Protokollierung sind:
- Art des Vorganges,
- Zeitpunkt der Aktivität,
- Merkmale der Maßnahme (z. B. Eingabewerte),
- ausführende Person oder Stelle.

Aus den Protokollen müssen sich folgende Fragen beantworten lassen:

- Wer hat wann mit welchen Mitteln was veranlaßt beziehungsweise worauf zugegriffen?
- Wer hatte von wann bis wann welche Zugriffsrechte?

14.2.3 gesetzliche Regelungen

Nur wenige gesetzliche Bestimmungen enthalten explizite Protokollierungsverpflichtungen wie z. B. in Nr. 7 der Anlage zu § 9 BDSG. Die meisten Regelungen bedingen (lediglich) eine Protokollierung, um die jeweils geforderte Maßnahme realisieren zu können (vgl. z. B. bezüglich der Speicherkontrolle und der automatischen Abrufverfahren Nr. 3 der Anlage zu § 9 BDSG, § 10 Abs. 2 BDSG, § 9 SächsDSG).

Für eine Reihe von Verwaltungsverfahren gelten zudem bereichsspezifische, vom Datenschutzrecht des Bundes beziehungsweise Sachsens abweichende Protokollierungsvorschriften. Als Beispiel hierfür kann die ausführliche Regelung für die Führung des "elektronischen Grundbuches" im Registerverfahrensbeschleunigungsgesetz (RegVBG) gelten (siehe Kapitel 8.8).

Bevor Art und Umfang von Protokollierungen festgelegt werden, haben die datenverarbeitenden Stellen deshalb zu ermitteln, welche gesetzlichen Regelungen für ihren Zuständigkeitsbereich welche Rahmenbedingungen definieren. Der Komplex "Protokollierung" stellt sich so nicht als eine Maßnahme im Rahmen des Ermessens dar, sondern als eine Folge aus den jeweils gültigen gesetzlichen Bestimmungen.

Die nachfolgenden Hinweise können daher nur unter diesem Vorbehalt den Charakter von Mindestanforderungen erfüllen.

14.2.4 Arten der Protokollierung

Beim Betrieb von IT-Systemen sollte zwischen den Funktionen der Administration und der Benutzung unterschieden werden.

Als "Administration" sind die Maßnahmen zur Installation, Modifikation und Konfiguration von Hard- und Software einschließlich der Abarbeitung von Systemnachrichten zu verstehen. Es handelt sich hierbei im wesentlichen um Basisfunktionen, die die fortdauernde Benutzung des Systems überhaupt erst ermöglichen.

Unter "Benutzung" ist die Inanspruchnahme der von der Administration bereitgestellten Ressourcen anzusehen. In der Praxis stellt sich dies als der Aufruf von Software dar, die entsprechend den in einem Benutzerprofil festgelegten Zugriffsrechten (in der Regel in einem Menü) zur Verfügung gestellt wird.

Die Protokollierung der Administrationsaktivitäten hat daher den Charakter einer Systemüberwachung, während die Protokollierung der Benutzeraktivitäten im wesentlichen der Verfahrensüberwachung dient. Dementsprechend finden sich die Anforderungen an die Art und den Umfang der systemorientierten Protokollierung überwiegend in dem "allgemeinen" Datenschutzrecht, während die verfahrensorientierte Protokollierung weitgehend nach bereichsspezifischen Regelungen richtet.

14.2.5 Administrationsprotokollierung

Folgende Aktivitäten sollten *vollständig* protokolliert werden:

- *Systemgenerierung und Modifikation von Systemparametern*
  Da auf dieser Ebene in der Regel keine systemgesteuerten Protokolle erzeugt werden, bedarf es entsprechender detaillierter manueller Aufzeichnungen, die mit der Systemdokumentation korrespondieren sollten.

- *Einrichtung von Benutzern*
  Wem von wann bis wann das Recht eingeräumt worden ist, das betreffende IT-System zu benutzen, ist vollständig zu protokollieren. Dies ergibt sich auch aus der Eingabekontrolle. Für diese Protokolle sollten längerfristige Aufbewahrungszeiträume vorgesehen werden, da sie Grundlage praktisch jeder Revisionsmaßnahme sind.

- *Verwaltung von Befugnistabellen*
  Im Rahmen der Protokollierung von Befugniszuweisungen muß insbesondere auch aufgezeichnet werden, wer die Erteilung einer bestimmten Befugnis angewiesen hat.

- *Einspielen und Änderung von Anwendungssoftware*
  Die Protokolle repräsentieren das Ergebnis der Programm- und Verfahrensfreigaben.

- *Änderungen an der Dateiorganisation*
  Im Hinblick auf die vielfältigen Manipulationsmöglichkeiten, die sich bereits bei Benutzung der "Standard-Dateiverwaltungssysteme" ergeben, kommt einer vollständigen Protokollierung eine besondere Bedeutung zu (vgl. z. B. Datenbankmanagement).

- *Durchführung von Back-up- und Datensicherungsmaßnahmen*
  Da derartige Maßnahmen mit der Anfertigung von Kopien bzw. dem Überschreiben von Datenbeständen verbunden sind und häufig in "Ausnahmesituationen" durchgeführt werden, ist ihre Protokollierung besonders wichtig.

- *Sonstiger Aufruf von Administrations-Tools*
  Für praktisch alle IT-Systeme gibt es Tools (nutzbare Zusatzfunktionen wie Datenwiederherstellung), die nur in "Ausnahmesituationen" Anwendung finden sollten. Deshalb sollte ihr Einsatz besonders protokolliert werden.

14.2.6 Benutzungsprotokollierung

Folgende Aktivitäten sollten in Abhängigkeit von der Schutzwürdigkeit der verarbeiteten Daten vollständig oder selektiv protokolliert werden (zur Schutzwürdigkeit von Daten vergleiche meine Bekanntmachung zu den Maßnahmen zur Gewährleistung des Datenschutzes (§ 9 SächsDSG) vom 30. Juni 1994, SächsABl. S. 979):

- *Versuche unbefugten Einloggens und Überschreitung von Befugnissen*
  Geht man von einer wirksamen Authentifizierungsprozedur und sachgerechten Befugniszuweisungen aus, kommt der vollständigen Protokollierung aller "auffälligen Abnormalitäten" beim Einloggen und bei der Benutzung zu. Benutzer in diesem Sinne ist auch der Systemadministrator.

- *Eingabe von Daten*
  Die sogenannte Eingabekontrolle erfolgt grundsätzlich verfahrensorientiert (z. B. Protokollierung in Akten, soweit vorhanden, Protokollierung direkt im Datenbestand, sofern keine Akten geführt werden). Auch wenn man davon ausgeht, daß Befugnisüberschreitungen anderweitig protokolliert werden, dürfte eine vollständige Protokollierung von Dateneingaben als Regelfall angesehen werden müssen.

- *Datenübermittlungen*
  Nur soweit nicht gesetzlich eine vollständige Protokollierung vorgeschrieben ist, kann eine selektive Protokollierung als ausreichend angesehen werden. In diesem Zusammenhang ist auch die Anfertigung von Dateikopien, Hardcopies und ähnlichem relevant. Dabei ist zu beachten, daß der Benutzer die grundsätzliche Befugnis haben muß, derartige Datenübermittlungen zu veranlassen, anderenfalls würde es sich um die Überschreitung von Befugnissen handeln.

- *Benutzung von automatisierten Abrufverfahren*
  In der Regel ist eine vollständige Protokollierung der Abrufe empfehlenswert, damit aufgedeckt werden kann, ob der Abrufende im Rahmen der grundsätzlich eingeräumten Zugriffsrechte unberechtigt auf Daten zugegriffen hat. § 8 Abs.2 SächsDSG verlangt zumindestens eine stichprobenweise Protokollierung

- *Löschen von Daten*
  Eine vollständige Protokollierung ist insbesondere erforderlich, wenn die Daten ausschließlich in automatisierten Dateien gespeichert sind. In Abhängigkeit vom Gegenstand der Datenverarbeitung ist eine Protokollierung der gelöschten Daten oder lediglich die Tatsache der Löschung angezeigt. Ersteres scheidet aus, wenn Löschungsansprüche der Betroffenen erfüllt werden.

- *Aufruf von Programmen*
  Dies kann erforderlich sein bei besonders "sensiblen" Programmen, die z. B. nur zu bestimmten Zeiten oder Anlässen benutzt werden dürfen. Deshalb ist in diesen Fällen eine vollständige Protokollierung angezeigt. Die Protokollierung dient auch der Entlastung der befugten Benutzer (Nachweis des ausschließlich befugten Aufrufs der Programme).

14.2.7 Personenbezug von Protokolldaten

Protokolle, die aus den oben genannten Gründen erzeugt werden, stellen faktisch alle personenbezogene Dateien dar. In erster Linie besteht ein Personenbezug zu den veranlassenden Personen oder Stellen. In vielen Fällen lassen Protokolle außerdem Rückschlüsse auf Daten von Betroffenen zu. Soweit nicht Ausnahmeregelungen gelten (vgl. z. B. § 1 Abs. 3 Nr. 1 BDSG), sind diese Protokolle wie "normale" Dateien zu behandeln.

14.2.8 Zweckbindung von Protokolldaten

Protokolldaten unterliegen aufgrund der nahezu übereinstimmenden Regelung im Datenschutzrecht des Bundes und der Länder einer besonders engen Zweckbindung (z. B. § 14 Abs.4 BDSG, § 31 Abs. 5, 7 SächsDSG). Sie dürfen nur zu den Zwecken genutzt werden, die Anlaß für ihre Speicherung waren.

Dies sind in der Regel die in einem Sicherheitskonzept festgelegten allgemeinen Kontrollen, die in den meisten Datenschutzgesetzen geforderte "Überwachung der ordnungsgemäßen Anwendung der Datenverarbeitungsprogramme, mit denen personenbezogene Daten verarbeitet werden" (vgl. § 18 Abs. 2 BDSG, § 9 Abs. 1 SächsDSG) und die Kontrolle durch interne oder externe Datenschutzbeauftragte.

14.2.9 Aufbewahrungsdauer für Protokolle

Die Aufbewahrungsdauer der Protokolle richtet sich, da es sich um personenbezogene Daten handelt, nach den allgemeinen Löschungsregeln der Datenschutzgesetze. Maßstab ist die "Erforderlichkeit zur Aufgabenerfüllung". Gibt es keinen zwingenden Grund für das weitere Aufbewahren von Protokolldateien, besteht eine Löschungspflicht (vgl. z. B. § 20 Abs. 2 BDSG, § 19 Abs.2 Nr.1 SächsDSG).

Eine exakte Bestimmung des Zeitraums für Protokolle, deren Auswertung zeitlich nicht konkretisiert ist (vergleiche z. B. die Protokolle im Zusammenhang mit der Administration,), ist nicht möglich. Als Anhaltspunkte können dienen

- die Wahrscheinlichkeit, daß Unregelmäßigkeiten (noch) offenbart werden können und
- die Möglichkeit, die Gründe von Unregelmäßigkeiten anhand der Protokolle und anderer Unterlagen aufdecken zu können.

Erfahrungsgemäß sollte eine Frist von einem Jahr nicht unterschritten werden.

Werden Protokolle zum Zwecke gezielter Kontrollen angefertigt, kommen kürzere Speicherungsfristen in Betracht. In der Regel reicht eine Aufbewahrung bis zur tatsächlichen Kontrolle.

Eine Begrenzung der Speicherungsdauer von Protokolldaten kann auch dadurch erreicht werden, daß durch eine "Ringspeicherung" nur eine maximale Anzahl von Protokolldatensätzen für die Kontrolle vorgehalten wird (z. B. die jeweils letzten Sätze). Andere Möglichkeiten der Reduzierung der Datenmengen bestehen darin, Protokolldatensätze nach einem Zufallsprinzip (feste Prozentsätze oder ähnliches) zu erzeugen oder die Erstellung durch den Kontrolleur zu veranlassen.

14.2.10 Technische und organisatorische Rahmenbedingungen

Die Effektivität der Protokollierung und ihre Auswertung im Rahmen von Kontrollen hängt im entscheidenden Maße von den technischen und organisatorischen Rahmenbedingungen ab. In diesem Zusammenhang sollten folgende Aspekte Berücksichtigung finden:

- Es sollte ein Revisionskonzept erstellt werden, das die Zielrichtung der Protokolle und der Kontrolle sowie Schutzmechanismen für die Rechte der Mitarbeiter und der sonstigen betroffenen Personen klar definiert.
- Die Zwangsläufigkeit und damit die Vollständigkeit der Protokolle muß gewährleistet werden.
- Das gleiche gilt für die Manipulationssicherheit der Einträge in Protokolldateien.
- Entsprechend der Zweckbindung der Datenbestände müssen wirksame Zugriffsbeschränkungen realisiert werden.
- Die Protokolle müssen so gestaltet sein, daß seitens der Kontrolleure/Revisoren eine effektive Überprüfung möglich ist.
- Die Auswertungsmöglichkeiten sollten vorab mit den Kontrolleuren abgestimmt und festgelegt sein.
- Soweit möglich, sollten Kontrollen nach dem 4-Augen-Prinzip erfolgen.
- Es sollte vorab definiert werden, welche Konsequenzen sich aus Verstößen ergeben, die durch die Kontrolle von Protokollen aufgedeckt werden.
- Personalräte sollten bei der Erarbeitung des Revisionskonzeptes und bei der Auswertung der Protokolle beteiligt werden.

14.3 Abfragesprachen für Datenbanken

In einigen Datenbanksystemen kann der Benutzer leicht von seiner Datenstation (Terminal, PC) aus mit allgemeinverständlichen "Abfragesprachen" eigene Abfragen von Datenbankinhalten formulieren. Unabhängig vom Anwendungsprogramm können damit Verknüpfungen, Abfragen und Auswertungen der vom Datenbanksystem verwalteten Datenbestände durchgeführt werden.

Im Anwendungsprogramm sind in der Regel Zugriffsregelungen festgelegt, für welchen Zweck auf bestimmte personenbezogene Daten zugegriffen werden kann und welche Auswertungen erstellt werden sollen. Dadurch ist gesichert, daß die Auswertungen erforderlich sind und datenschutzrechtliche Forderungen erfüllt werden.

Dagegen kann der Benutzer beim Einsatz von Abfragesprachen von seiner Datenstation aus spontan Abfragen auf alle Felder aller vom Datenbanksystem verwalteten personenbezogenen Daten richten, ohne an Restriktionen des Anwendungsprogramms gebunden zu sein.

Deshalb sollte entweder ganz auf den Einsatz frei formulierbarer Abfragesprachen verzichtet, oder zumindestens sollten die Zugriffsbefugnisse durch besondere Maßnahmen eingeschränkt und kontrolliert werden, z. B.:
- Restriktive Zugriffsberechtigungen für Nutzer (z. B. für weniger sensitive Datenfelder),
- Genehmigung der Abfrage durch eine autorisierte Person (Formular, Dokumentation),
- Protokollierung der Abfragekriterien (Wer hat wann welche Abfrage getätigt?),
- Kontrolle der Protokollierung auf unzulässige Abfragen.

Werden nur anonymisierte Auswertungen mit Hilfe der Abfragesprache erstellt, gibt es keine datenschutzrechtlichen Bedenken.

14.4 Datenautobahn / Multimedia

Zukünftig soll eine "Globale Informations-Infrastruktur" entstehen, die ein die ganze Welt umfassendes Leitungsnetz (Datenautobahn) für superschnelle und massenhafte Übertragung von Text, Graphik, graphische Animation, Einzelbildern, Video und Sprache bereitstellt. Damit diese "Multimedia-Autobahnen" tatsächlich weltweit funktionieren können, müssen einheitliche technische, organisatorische und juristische Regeln geschaffen werden. Dazu wurden von den drei weltgrößten IT-Verbänden in Tokio Anforderungen formuliert, die auch auf den Schutz der Privatsphäre und die Datensicherheit eingehen.

14.4.1 Multimedia-Pilotprojekt in Deutschland

Zur Zeit startet die Telekom Multimedia-Pilotprojekte für neue Dienste in sechs bundesdeutschen Städten (Hamburg, Berlin, Leipzig, Nürnberg, Stuttgart, Köln/Bonn). Voraussetzungen für die Teilnahme am Pilotprojekt sind ein Kabelanschluß (Breitband-Kabelnetz für Kabelfernsehen) als Übertragungsmedium und ein modernes Farbfernsehgerät.
Außerdem muß ein digitaler Decoder (Set-Top-Box) gekauft oder gemietet werden, der zwischen Kabelanschluß und Fernsehgerät geschaltet wird. Eine Chipkarte (Smartcard) aktiviert die Set-Top-Box und ermöglicht so den Zugang zu den neuen Diensten. Folgende Dienste stehen den Teilnehmern am Pilotprojekt zur Verfügung:

- *Pay per channel*
  Der Fernsehteilnehmer zahlt für die Nutzung des gesamten Programmangebotes, wie z. B. beim TV-Sender "Premiere".
- *Pay per view*
  Der Zuschauer zahlt nur für einzelne gesehene Sendungen.
- *Near video on demand*

Jeder Film läuft in mehreren Kopien zeitversetzt. Der Zuschauer kann selbst entscheiden, welche Filme er wann (im Zeitraster) entgeltpflichtig einschaltet.

- *Video on demand*
  Der Fernsehteilnehmer entscheidet, wann er welchen Film entgeltpflichtig abruft. Er kann im Handlungsverlauf "vor- und zurückspulen" oder den Film kurzfristig anhalten.
- *Videogames*
  Der Teilnehmer zahlt für die Zuspielung (Downloading) der Software für Computerspiele. Er kann mit anderen Spielern oder allein spielen.
- *Service on demand*
  Der Fernsehteilnehmer kann das sogenannte Homeshopping in Anspruch nehmen (z. B. Angebote der Versandhäuser, Banken und Reiseveranstalter nutzen). Der Anbieter legt Inhalt und Umfang fest, während der Fernsehteilnehmer Waren beziehungsweise Dienstleistungen auswählt und bestellt oder Informationen kostenpflichtig abruft.

Außerdem könnte Fernunterricht sowie Zugang zu Katalogen von Bibliotheken angeboten werden.

14.4.2 Funktionsbeschreibung

Bisher wurden Fernsehprogramme im Breitbandkabelnetz nur *analog* übertragen. Die Nutzung neuer Dienste, die individuelles Fernsehen ermöglichen, setzt eine *digitale Übertragung* (höhere Übertragungsqualität, höherer Bedienkomfort) voraus. Außerdem ermöglicht die digitale Übertragung eine Datenkompression, die die zu übertragende Datenmenge reduziert und somit eine Voraussetzung für die schnelle Übertragung großer Datenmengen schafft.

Während bisher allen Empfängern das gleiche Fernsehangebot übertragen wurde, müssen jetzt Vermittlungscomputer den Empfänger auswählen, damit nur der den gewählten Dienst erhält, der ihn auch bestellt hat. Dies setzt voraus, daß der Empfänger zuvor über den sogenannten Rückkanal den entsprechenden Dienst angefordert hat. Bevor der Teilnehmer jedoch einen Dienst anfordern kann, muß er sein Zugriffsrecht durch eine gültige Chipkarte, die in die Set-Top-Box eingeführt wird, nachweisen. Außerdem werden in der Set-Top-Box digitale in analoge Signale und umgekehrt umgewandelt, denn Fernsehgeräte können zur Zeit nur analoge Signale empfangen.

14.4.3 Datenschutzrechtliche Gesichtspunkte

Für den Abruf der Dienste werden Teilnehmerdaten und Verbindungsdaten vom Diensteanbieter (hier TELEKOM) zur Abrechnung der Entgelte erhoben, gespeichert und verarbeitet. Da registriert wird, wer wann was gesehen oder bestellt hat und worüber Informationen eingeholt wurden, entstehen sehr sensible Datensammlungen. Es könnten somit umfassende Persönlichkeitsprofile erstellt werden. Derartige Datensammlungen sind aus datenschutzrechtlicher Sicht nicht hinnehmbar. Deshalb muß hier eine gesetzliche Regelung für die Verarbeitung der anfallenden personenbezogenen Daten geschaffen werden, die auch folgende Forderungen erfüllt:

- Abrechnungsdaten sind so zu speichern, daß sie Zeitpunkt, Dauer, Art, Inhalt und Häufigkeit der Dienste nicht erkennen lassen, es sei denn, der Teilnehmer beantragt einen Einzelnachweis.
- Nicht mehr für Abrechnungszwecke benötigte Daten sind sofort zu löschen. Eine strikte Zweckbindung ist vorzuschreiben.
- Sofern personenbezogene Daten erhoben werden müssen, dürfen unberechtigte Dritte nicht darauf zugreifen können.
- Die Daten müssen eindeutig dem richtigen Teilnehmer/Empfänger zugeordnet werden können.
- Das gesamte Verfahren muß so gestaltet werden, daß es auch für den Teilnehmer durchschaubar ist.

Da im Rahmen des Pilotprojektes die Akzeptanz der neuen Dienste getestet werden soll, bedarf es in dieser Phase einer umfangreicheren Datenerfassung. Damit können die oben genannten Forderungen nicht im vollen Umfang durchgesetzt werden. Gerade deshalb müssen aber die Teilnehmer zuvor umfassend darüber informiert werden, was mit ihren Daten geschieht.

14.5 IT-Grundschutzhandbuch

Oft begegnet mir in den Behörden Ratlosigkeit, wenn es um Fragen der Sicherheit bei der EDV-Technik geht. Selbst den verantwortlichen technischen Mitarbeitern sind viele Gefährdungslagen und daraus resultierende Anforderungen nicht bekannt. Eine erste Hilfe soll auf diesem Gebiet das IT-Grundschutzhandbuch, eine Veröffentlichung des Bundesamtes für Sicherheit in der Informationstechnik (BSI), bieten. Ausgehend von einem mittleren Schutzbedarf kann der Nutzer ohne eine detaillierte Risikoanalyse Maßnahmen bestimmen, die die IT-Sicherheit gewährleisten können. Für Einzel-PCs, lokal vernetzte Systeme (LAN) und Telekommunikationsanlagen sind Gefährdungen und Maßnahmeempfehlungen beschrieben, die sowohl die Technik wie auch die Infrastruktur (z. B. Gebäude, Verkabelung, Datenträgerarchiv) umfassen. Auch wenn das Grundschutzhandbuch nicht die in bestimmten Fällen (z. B. bei besonders geschützten persönlichen Daten) notwendige detaillierte Risikoanalyse ersetzt, so würde seine Beachtung doch einer Reihe von Mißständen in den Behörden abhelfen, denen ich immer wieder begegne.

Das Buch erscheint nach der nunmehr abgeschlossenen Erprobungsphase ab Mai im Bundesanzeigerverlag, PF 100 534, 50445 Köln, ISBN 3-88784-604-4. Abonnenten des Bundesanzeigers erhalten bei Anforderung ein kostenloses Exemplar.

14.6 Entsorgung von Datenträgern - Karbonfarbbänder

In Schreibmaschinen werden neben den gebräuchlichen Nylonbändern auch Karbonbänder eingesetzt. Karbonbänder können ähnlich dem Kohlepapier nur einmal in der Schreibmaschine zum Schreiben eingesetzt werden, da der Farbstoff vom Karbonband auf das Papier übertragen wird. Dadurch läßt sich der geschriebene Text auf dem Karbonband leicht lesen. Die Bänder müssen deshalb unbedingt datenschutzgerecht entsorgt werden.

Die Vernichtung kann sowohl zentral als auch dezentral erfolgen. Die Art des Datenträgers, die Menge und der zeitliche Anfall der zu vernichtenden Datenträger bestimmen die individuelle Lösung. Die sicherste Lösung ist die sofortige Vernichtung an Ort und Stelle.

Karbonfarbbänder können in einem Shreddergerät zerkleinert werden. Geeignete Datenshredder zerkleinern nicht nur Akten beziehungsweise Papier, sondern auch andere Datenträger wie Karbonbänder, Disketten, Scheck- und sonstige Plastikkarten sowie Mikrofilme und Mikrofiches. Werden die jeweiligen Datenträger getrennt voneinander zerkleinert, kann das zerkleinerte Material recycelt werden.

Jede öffentliche Stelle ist bis zur abgeschlossenen Vernichtung für ihre zu vernichtenden Datenträger verantwortlich, das heißt, bis die personenbezogenen Daten als gelöscht gelten können. Dies gilt auch bei Entsorgung der nicht mehr genutzten Karbonbänder durch einen Auftragnehmer. Die auftraggebende Stelle ist nach § 7 SächsDSG verpflichtet, den Auftragnehmer unter besonderer Berücksichtigung der Eignung der von ihm getroffenen personellen, technischen und organisatorischen Maßnahmen zur Datensicherheit sorgfältig auszuwählen (siehe dazu Bekanntmachung des Sächsischen Datenschutzbeauftragten zur Datenverarbeitung im Auftrag [§ 7 SächsDSG] und zur Rechtsstellung des beauftragten Unternehmers [§ 2 Abs. 2 SächsDSG] vom 3. November 1993, SächsABl. S. 1304).

14.7 Datenverarbeitung im Auftrag - Abwasserzweckverband

Zahlreiche Gemeinden und Gemeindeverbände, insbesondere die Wasser-/Abwasserzweckverbände, schließen mit privaten Unternehmen "Beratungsverträge" ab, um die eigentliche Aufgabe der Gemeinde bzw. des Zweckverbandes "außer Hauses" erledigen zu lassen. Danach übernehmen Beratungsunternehmen gegen eine pauschale Vergütung pro beitragspflichtiger Grundstückseinheit verschiedene Arbeiten, die zur Beitragserhebung nach §§ 17 ff. SächsKAG und den entsprechenden Trinkwasser-/Abwassersatzungen notwendig sind.

So erledigte ein privates Unternehmen im Auftrag eines Zweckverbandes für Kommunale Wasserversorgung und Abwasserbehandlung folgende Arbeiten automatisiert:
Ermittlung der Global- und Beitragsberechnung für das gesamte Verbandsgebiet (Wasserversorgung)
Ausfertigung der Beitragsbescheide.

Nach § 7 Abs.2 SächsDSG hat der Auftraggeber den Auftragnehmer unter besonderer Berücksichtigung der Eignung der von diesem getroffenen personellen, technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. Gegenstand und Umfang der Datenverarbeitung sowie die notwendigen personellen, technischen und organisatorischen Maßnahmen sind schriftlich im Vertrag festzulegen.

Durch die Kontrolle beim Auftragnehmer, dem privaten Unternehmer, an der der Auftraggeber, vertreten durch den Geschäftsführer des Zweckverbandes für Kommunale Wasserversorgung und Abwasserbehandlung, teilnahm, habe ich folgende Mängel festgestellt:

1. Der PC-Raum ist nur unzureichend gegen unbefugtes Eindringen, Diebstahl und Zerstörung gesichert.
2. Für die Vernichtung von Datenträgern gibt es kein geeignetes Gerät.
3. Die PCs sind nicht in ausreichendem Maße gegen Mißbrauch geschützt.
4. Die Sicherungskopien werden nicht brandgeschützt aufbewahrt.
5. Das Dateien- und Geräteverzeichnis gemäß § 10 SächsDSG wird nicht geführt.

Im einzelnen wurde dazu folgendes festgestellt:

Zu 1: Während der Arbeitszeit wird der Zugang zum Gebäude durch Pförtner, außerhalb der Arbeitszeit durch Einbruchsmeldeanlagen, die in den Gängen installiert sind, überwacht. Der jetzige Standort ist zur Aufstellung der PCs nicht geeignet. Der Raum befindet sich im Erdgeschoß und ist von der Straße gut einsehbar. Die ungesicherten Fenster bieten wenig Schutz gegen Eindringen. Die PCs sollten deshalb an einem anderen Ort (z. B. in einer höhere Etage) aufgestellt werden.

Zu 2: Datenträger (z. B. Disketten, Ausdrucke und so weiter), die nicht mehr gebraucht werden oder aufgrund eines Defektes ausgesondert werden sollen, sind so zu entsorgen, daß keine Rückschlüsse auf vorher gespeicherte Daten möglich sind. Bei funktionierenden elektronischen Datenträgern kann dies durch Löschen (vollständiges Überschreiben oder Formatieren) der Daten vorgenommen werden. Bei Ausdrucken oder nicht mehr funktionierenden elektronischen Datenträgern kann dies durch physikalisches Zerstören erreicht werden. Für eine datenschutzgerechte Vernichtung von Datenträgern ist ein Datenshredder oder Aktenvernichter aufzustellen.

Zu 3: PCs ohne zusätzliche Sicherheitsvorkehrungen sind für die Verarbeitung personenbezogener Daten nicht geeignet, da z. B. Benutzerkontrolle, Zugriffsschutz und Protokollierung nicht möglich sind. Jeder Benutzer hat Zugriff auf alle Dateien; der Diskettenbetrieb ist unkontrollierbar. Der Einsatz des BIOS-Paßwortes allein bietet keinen ausreichenden Schutz der Daten vor unbefugtem Zugriff. Um

unberechtigtes Booten oder Kopieren zu verhindern, sollten vorläufig die Laufwerke durch Diskettenschlösser gesperrt werden.
Erst mit zusätzlicher Hard- und Software kann jedoch ein Sicherheitsstandard erreicht werden, der für die Verarbeitung personenbezogener Daten auf einem MS-DOS-PC ausreichend ist. Dazu wird 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 Benutzerkennung und Paßwort (vereinzelt auch mit Chipkarte) den Zugang zur Festplatte schützen. Damit auch hier die Benutzeranmeldung nicht umgangen werden kann, muß der Systemstart über das Diskettenlaufwerk durch zusätzliche Bootschutzeinrichtungen verhindert werden.

Zu 4: Die Datenträger werden in einem verschließbaren Schrank im Zimmer des Geschäftsführers (Sicherheitsstufe 1- besonders gegen Einbruch gesichert) aufbewahrt. Wegen der Brandgefahr sollten sie jedoch in einem Data-Safe diebstahl- und feuersicher aufbewahrt werden.

Zu 5: Der Auftraggeber muß den Auftragnehmer vertraglich verpflichten, ein Verzeichnis der Dateien des Auftraggebers und der eingesetzten Datenverarbeitungsanlagen nach § 10 SächsDSG zu führen. Dieses hat der Auftragnehmer auf Anforderung nach § 28 Abs. 1 dem Sächsischen Datenschutzbeauftragten zuzuleiten.

Die Auftragsdatenverarbeitung in dem Unternehmen sowie die vertraglichen Regelungen entsprachen zwar nicht in allen Punkten den Anforderungen des § 7 SächsDSG, jedoch zeigte der Kontrollbesuch die Bereitschaft des Geschäftsführers des Unternehmens, die vorgeschlagenen Verbesserungen zur technisch-organisatorischen Sicherheit in die Wege zu leiten.

Ich habe den kommunalen Zweckverband aufgefordert, die oben genannten Mängel unverzüglich zu beseitigen. Außerdem war der Vertrag mit dem privaten Unternehmen um datenschutzrechtliche Regelungen zu ergänzen (siehe 5.5.2).

14.8 Adressierung von Behördenbriefen und Postverteilung in Behörden

Zu diesem Thema habe ich gegenüber einem Landratsamt Stellung genommen.
In diesem Landratsamt wurde die Postverteilung folgendermaßen geregelt:

Die hier besonders interessierenden Ämter für Gesundheitswesen, Jugend und Soziales sind zu einem Dezernat zusammengefaßt, in dem die Postverteilung für die Ämter erfolgt. Nur als "Vertraulich, persönlich" gekennzeichnete Post wird ungeöffnet weitergeleitet. Die Mitarbeiter sind entsprechend belehrt.

Diese bisher praktizierte Postverteilung ist problematisch.

Neben der allgemeinen Pflicht zur Amtsverschwiegenheit gelten die besonderen Verschwiegenheitspflichten wie z. B. das Arzt- oder das Sozialgeheimnis. Diese

besonderen Verschwiegenheitspflichten sind auch im Postverkehr mit anderen Ämtern der gleichen Organisationseinheit, hier des Dezernats oder des gesamten Landratsamts, zu beachten: funktionaler Stellenbegriff. Dieser Begriff wurde in § 67 Abs. 9 Satz 3 SGB X für die Sozialleistungsträger, also z. B. Sozialamt, Jugendamt, mit folgendem Wortlaut erläutert: "Ist der Leistungsträger eine Gebietskörperschaft, so sind eine speichernde Stelle die Organisationseinheiten, die eine Aufgabe nach einem der besonderen Teile dieses Gesetzbuchs funktional durchführen". Das bedeutet, daß beispielsweise das Sozialamt, welches Aufgaben nach dem Bundessozialhilfegesetz wahrnimmt, eine eigene speichernde Stelle gegenüber der Wohngeldstelle, die Aufgaben nach dem Wohngeldgesetz bzw. dem Wohngeldsondergesetz wahrnimmt, darstellt. Die Stellen sind untereinander organisatorisch so abzuschotten, daß keine allgemeine Datenübermittlung vorkommt und jede Stelle ihre "eigenen" Daten zur Kenntnis nimmt.

Ich habe dem Landratsamt folgende Empfehlungen zu einer datenschutzgerechteren Organisation der Postverteilung gegeben, die auch auf die anderen Dezernate des Landratsamtes anwendbar sind:

a) Behandlung des Posteingangs
Post, die erkennbar an das jeweilige Amt (z. B. "Arztpost") oder direkt (z. B. "Sozialamt") adressiert ist, sollte erst im jeweiligen Amt geöffnet werden. Die im Dezernat eingehende Post ist also ungeöffnet weiterzuleiten. Post, die mit dem Zusatz "persönlich", "vertraulich" oder ähnliches versehen ist, ist der betreffenden Person ungeöffnet auszuhändigen.

Es ist nicht zu verkennen, daß ein Spannungsverhältnis zwischen der Dienstpflicht des Dezernatsleiters zur Kontrolle der Amtsleiter und dem Schutz der personenbezogenen Daten besteht. Deshalb muß der Amtsleiter im Einzelfall entscheiden, inwieweit der Dezernatsleiter von Einzelfällen unterrichtet wird. Jedes Amt sollte deshalb "Poststelle" sein. Die dort geöffneten Postsendungen sind mit dem Eingangsstempel zu versehen. Bei ungeöffnet weiterzuleitenden Sendungen ist der Eingangsstempel auf die Briefhülle zu setzen (die dann zu den Akten gehört).

Ist die Postsendung nur "an das Landratsamt" gerichtet, so ist sie durch bestimmte Mitarbeiter der zentralen Poststelle zu öffnen. Sie sind über die bei ihrer Tätigkeit zu beachtenden Vorschriften zu unterrichten und auf deren Einhaltung schriftlich zu verpflichten (§ 6 Abs. 2 SächsDSG).

Sogenannte "Irrläufer" sollten direkt zwischen den Ämtern und nicht erst über die Dezernatsebene weitergeleitet werden.

b) Behandlung des Postausgangs
Die zu versendenden Schriftstücke sind von den Schreibkräften oder der Poststelle des jeweiligen Amtes in einem verschlossenen Umschlag weiterzuleiten.

Schriftstücke mit besonders zu schützenden Daten (z. B.Gesundheits- und Sozialdaten) sind grundsätzlich auch innerhalb der Landkreisverwaltung in einem Umschlag zu übermitteln.

Schreiben der Behörden sollten also so gestaltet werden, daß der Empfänger seine Antwort im Sinne des oben dargestellten Verfahrens unmittelbar an das zuständige Amt richten kann. Diese genaue Bezeichnung sollte allerdings nur auf dem Briefbogen, nicht auf dem Briefumschlag erfolgen, weil vielen Menschen Post z. B. vom Sozialamt oder Jugendamt unangenehm ist. Der Briefumschlag oder das Fenster im Briefumschlag sollte so neutral wie möglich gehalten werden, also z. B. "Stadtverwaltung ...", "Landratsamt ..."

15 Vortrags- und Schulungstätigkeit

Auf Seminaren, Fortbildungsveranstaltungen, Tagungen und mit Vorträgen waren die Angehörigen der Dienststelle und ich trotz hoher Arbeitsbelastung verstärkt bemüht, den Datenschutzgedanken zu verbreiten. Zielgruppen waren beispielsweise: Studenten, Polizeibeamte, Sozialarbeiter, Lehrer, Bedienstete sächsischer Ministerien sowie in den Bereichen Personalwesen, Datensicherheit und Meldewesen tätige Mitarbeiter der Kommunen und Landkreise.

Nach wie vor besteht reges Interesse an meiner - diesmal im September 1994 in Dresden abgehaltenen - zentralen Fortbildungsveranstaltung für die Datenschutzbeauftragten sächsischer öffentlicher Stellen.

16 Materialien

16.1 Bekanntmachungen

16.1.1 (SächsABl. S. 976)

Bekanntmachung
des Sächsischen Datenschutzbeauftragten
zur Zulässigkeit automatisierter Abrufverfahren (§ 8 SächsDSG)
Vom 29. Juni 1994

Immer wiederkehrende Fragen und Probleme im Zusammenhang mit der Zulässigkeit **automatisierter Abrufverfahren** und damit zugleich auch mit der Anwendung des § 8 des Gesetzes zum Schutz der informationellen Selbstbestimmung im Freistaat Sachsen (Sächsisches Datenschutzgesetz - SächsDSG) vom 11. Dezember 1991 (SächsGVBl. S. 401) veranlassen den Sächsischen Datenschutzbeauftragten, folgende Hinweise zu geben:

1. § 8 SächsDSG gilt nur für automatisierte Abrufverfahren zwischen sächsischen öffentlichen Stellen.

2. Ein **automatisiertes Abrufverfahren** ist ein von mindestens zwei datenverarbeitenden Stellen gemeinsam eingerichtetes und betriebenes Verfahren, durch das die **abrufende Stelle** personenbezogene Daten aus einer von der **bereithaltenden Stelle** eingerichteten Datei abrufen kann. Die abrufende Stelle (Datenempfänger) bestimmt **allein** darüber, ob und wann sie welche Daten (innerhalb eines vorgegebenen Rahmens) abruft.

3. Der automatisierte Abruf ist seitens der abrufenden Stelle eine **Datenerhebung** (§ 3 Abs. 2 Nr. 1 SächsDSG) und seitens der bereithaltenden Stelle eine **Datenübermittlung** (§ 3 Abs. 2 Nr. 5 Buchst. b SächsDSG).

4. Da die bereithaltende (=übermittelnde) Stelle als "Herrin der Daten" ihrer Verantwortung für die Zulässigkeit der Übermittlung (§ 13 Abs. 2 Satz 3 SächsDSG) nicht vor den Abrufen nachkommen kann, sind Einrichtung und Betrieb automatisierter Abrufverfahren nur unter den besonderen Voraussetzungen des § 8 SächsDSG (vgl. Nr. 7 ff.) zulässig. **Daneben** müssen die für **jede Datenerhebung und -übermittlung geltenden Voraussetzungen** erfüllt sein:

   - eine Erhebungsbefugnis seitens der abrufenden Stelle;

   - eine Übermittlungsbefugnis seitens der bereithaltenden Stelle.
   Falls bereichsspezifische Erlaubnisnormen nicht bestehen, sind § 11 bzw. § 13 SächsDSG heranzuziehen.

5. § 8 SächsDSG unterscheidet hinsichtlich der Anforderungen an ein automatisiertes Abrufverfahren nach den organisatorischen Beziehungen zwischen den am Abrufverfahren beteiligten Stellen. Falls Abrufe zwischen Stellen im funktionalen

Sinn (z. B. Einwohnermeldeamt, Wohnungsamt) stattfinden sollen, die zu **einer** Stelle im organisatorischen Sinn (z. B. Stadtverwaltung, Landratsamt) gehören, gelten die in § 8 **Abs. 2** SächsDSG aufgeführten Zulässigkeitsvoraussetzungen (vgl. Nr. 8 und Nr. 9). Falls am Abrufverfahren **verschiedene** Behörden (Stellen im organisatorischen Sinn) beteiligt sind, gelten die Voraussetzungen des § 8 **Abs. 1** SächsDSG: Das Abrufverfahren muß dann ausdrücklich durch ein Gesetz (vgl. Nr. 7) zugelassen sein (z. B. § 36 Straßenverkehrsgesetz, § 17 Abs. 1 Satz 2 Paßgesetz).

Nicht unwesentlich würde das noch ausstehende Gesetz über Aufbau, räumliche Gliederung und Zuständigkeiten der Landesverwaltung (Art. 83 Abs. 1 Satz 1 SächsVerf) zur Rechtssicherheit in der Frage beitragen, ob automatisierte Abrufverfahren nach § 8 Abs. 1 SächsDSG oder nach § 8 Abs. 2 SächsDSG zu beurteilen sind.
Ohne dieses Gesetz sind nämlich Fälle denkbar, daß eine bislang selbständige öffentliche Stelle im organisatorischen Sinn durch bloßen Erlaß der Staatsregierung in eine andere Behörde einbezogen wird. Ein zwischen diesen Stellen bestehendes automatisiertes Abrufverfahren wäre vorher an § 8 Abs. 1 SächsDSG (Gesetzesvorbehalt) zu messen gewesen, wohingegen nach dem Zusammenschluß das Verfahren nur noch an die Voraussetzungen des § 8 Abs. 2 SächsDSG gebunden sein würde. Dies bedeutete eine Einschränkung des Schutzniveaus für das Recht der Betroffenen auf informationelle Selbstbestimmung.
*Der Erlaß einer eindeutigen und **abschließenden** gesetzlichen Regelung über die Organisation der Landesverwaltung ist daher auch im Interesse des Datenschutzes dringend geboten.*

6. § 8 SächsDSG findet keine Anwendung auf bereits **vor** Inkrafttreten des Sächsischen Datenschutzgesetzes (14. Dezember 1991) eingerichtete Verfahren. Für diese Verfahren gilt die Übergangsregelung des § 34 SächsDSG. Nach § 34 Abs. 1 Nr. 2 i. V. m. § 8 Abs. 3 SächsDSG hätte der Sächsische Datenschutzbeauftragte über bereits eingerichtete Verfahren bis zum **31. März 1992** unterrichtet werden müssen (vgl. Nr. 13). Im übrigen hätten vorhandene automatisierte Verfahren gemäß § 34 Abs. 2 SächsDSG bis spätestens zum **31.12.1992** den Vorschriften des Sächsischen Datenschutzgesetzes angepaßt werden müssen. Sollte die Unterrichtung des Datenschutzbeauftragten oder die Anpassung bis heute nicht erfolgt sein, ist dies unverzüglich nachzuholen. Bei seinen datenschutzrechtlichen Kontrollen wird der Datenschutzbeauftragte sein besonderes Augenmerk auf den ordnungsgemäßen Vollzug dieser Vorschrift richten und ggf. Verstöße gemäß § 26 SächsDSG beanstanden.

7. Die Einrichtung eines automatisierten Abrufverfahrens zwischen verschiedenen Stellen im organisatorischen Sinn ist gemäß **§ 8 Abs. 1 SächsDSG** nur zulässig, soweit ein **Gesetz** dies ausdrücklich **erlaubt**. Anders als der weitergehende Begriff "Rechtsvorschrift" (vgl. § 4 Abs. 1 Nr. 1 SächsDSG) sind mit "Gesetz" hier ausschließlich **formelle Bundes- oder Landesgesetze** gemeint. Allerdings können durch Rechtsverordnung oder Satzung die näheren Einzelheiten des Verfahrens geregelt werden. Um einen umfassenden Schutz des Rechts auf informationelle Selbstbestimmung (Art. 33 Sächsische Verfassung) zu gewährleisten, muß der Gesetzgeber nach Art. 75 Abs. 1 S. 2 Sächsische Verfassung Inhalt, Zweck und

Ausmaß der Ermächtigung bestimmen; der Gesetz-, Rechtsverordnungs- oder Satzungsgeber sollte **mindestens** den Anlaß und den Zweck des Abrufverfahrens, die bereithaltende und abrufende Stelle, den abrufbaren Datenumfang sowie das Nähere über das Verfahren festlegen. Außerdem sind hinreichende personelle, technische und organisatorische Sicherheitsregelungen i. S. v. § 9 SächsDSG zum Schutz des Rechts auf informationelle Selbstbestimmung zu treffen. Insbesondere ist die Abrufkontrolle (Protokollierung der Abrufe) zu gewährleisten (vgl. Nr. 9 und 10).

8. Vor der Prüfung, ob das beabsichtigte Verfahren den Voraussetzungen des § 8 Abs. 2 SächsDSG entspricht, ist **zunächst** zu prüfen, ob die Anwendung dieser Vorschrift nicht durch **besondere** und **abschließende** Rechtsvorschriften des Landes oder des Bundes **ausgeschlossen** ist (vgl. § 2 Abs. 4 SächsDSG). Beispielsweise läßt die abschließende Regelung in § 36 Straßenverkehrsgesetz kein automatisiertes Abrufverfahren zwischen Kfz-Zulassungstelle und anderen Ämtern der gleichen Verwaltung (z. B. kommunale Verkehrsüberwachung) zu. Weiterhin gelten z. B. für Sozialleistungsträger (vgl. § 35 SGB I) die besonderen Vorschriften der §§ 79 SGB X, 10 BDSG und die übrigen Regelungen des Sozialgesetzbuchs (Zehntes Buch) über die Erhebung und Offenbarung von Sozialdaten.

   Nach **§ 8 Abs. 2 S. 1 SächsDSG** ist die Einrichtung eines automatisierten Abrufverfahrens innerhalb einer Behörde, also zwischen Stellen im funktionalen Sinn, die zu **einer** Stelle im organisatorischen Sinn gehören, nur zulässig, wenn das Verfahren unter Berücksichtigung der schutzwürdigen Interessen der Betroffenen und der Aufgaben der öffentlichen Stelle **angemessen** ist.
   Bei der Prüfung der Angemessenheit sind die durch das Abrufverfahren für das Persönlichkeitsrecht des Betroffenen entstehenden **besonderen Gefährdungen** mit dem **Bedarf** für ein derartiges Verfahren, der sich aufgrund der Aufgaben der beteiligten Stellen ergibt, **abzuwägen**. Besondere Gefährdungen für das Persönlichkeitsrecht des Betroffenen beim Betrieb automatisierter Abrufverfahren ergeben sich bereits daraus, daß die bereithaltende Stelle nicht - wie in § 13 Abs. 2 SächsDSG grundsätzlich vorgesehen - die Möglichkeit hat, die Zulässigkeit der Datenübermittlungen im Einzelfall zu prüfen. Bei der Abwägung sind besonders der Grad der Schutzwürdigkeit der Daten, die Art des Verwendungszwecks sowie die Größe des Empfängerkreises (Mißbrauchsgefahr) zu berücksichtigen. Insbesondere ist unter Berücksichtigung des Erforderlichkeitsgrundsatzes stets zu fragen, ob

   - ein besonderer Grund für eine jederzeitige und schnelle Datenübermittlung besteht,

   - die zu erwartende Anzahl der Anfragen die Einführung eines automatisierten Abrufverfahrens rechtfertigt,

   - der durch die Einrichtung eines automatisierten Abrufverfahrens zu erbringende Aufwand in einem angemessenen Verhältnis zu dem erwarteten Nutzen steht (Aufwand-Nutzen-Analyse).

   Da personenbezogene Daten, die besonderen **Geheimhaltungsvorschriften** (z. B. besondere Berufs- und Amtsgeheimnisse) unterliegen, besonders schutzwürdig sind und automatisierte Abrufverfahren **stets** eine erhebliche Gefährdung für das

Persönlichkeitsrecht des Betroffenen bedeuten, sollten diese Daten grundsätzlich **nicht** im automatisierten Abrufverfahren verarbeitet werden.

9. Gemäß § 8 Abs. 2 Satz 1 SächsDSG muß **außerdem** mindestens eine stichprobenweise **Abrufkontrolle** gewährleistet sein. Dies hat die bereithaltende Stelle als "Herrin der Daten" sicherzustellen. Aufgrund des Protokolls müssen Inhalt und Zeitpunkt des Abrufs sowie die abrufende Stelle einschließlich des Benutzers feststellbar sein. Eine **Vollprotokollierung**, d. h. eine lückenlose Protokollierung aller Abrufe, wird nur ausnahmsweise erforderlich sein. Sie kann geboten sein, wenn besonders schutzwürdige Daten (z. B. Gesundheitsdaten) automatisiert abgerufen werden sollen oder ein vermuteter Datenmißbrauch festgestellt werden soll. Ausreichend ist in der Regel eine Protokollierung nach festen oder zufälligen Auswahlkriterien. Bei einer ausschnittsweisen Protokollierung können sich die Ausschnitte auf Zeiträume, Benutzer oder bestimmte Daten beziehen. Um einem möglichen Mißbrauch wirkungsvoll entgegentreten zu können, darf die Art und Weise der Protokollierung für die Benutzer nicht vorhersehbar sein; für sie muß **immer** das Risiko einer Protokollierung und Nachprüfung bestehen.
   Die Protokolldaten müssen nicht ausgedruckt vorliegen; es reicht aus, wenn sie maschinenlesbar verfügbar sind.
   Gemäß § 12 Abs. 4 SächsDSG dürfen die Protokolldaten **nur** zum Zwecke der Abrufkontrolle verwendet werden. Sie sind daher gegen zweckfremde Nutzung oder gegen sonstigen Mißbrauch durch geeignete Vorkehrungen zu schützen. Im allgemeinen erscheint eine Aufbewahrungsdauer für Protokolle dieser Art von einem Jahr als angemessen. Danach sind die Protokolldaten zuverlässig zu löschen.

10. Bei der **Auswertung der Protokolldaten** sollen diejenigen Teilmengen ermittelt werden, bei denen die erhöhte Wahrscheinlichkeit "kritischer Abrufe" besteht. Hierzu können Auswertungen nach Tageszeiten, nach abrufberechtigten Personen oder Stellen, nach Nutzungsfrequenz oder nach der Art der abgerufenen Daten in Betracht kommen. Erweisen sich bestimmte Teilmengen von Abrufen als überdurchschnittlich fehlerträchtig, ist für diese eine besonders intensive Auswertung vorzunehmen. Die Überprüfung kann, ungeachtet einer Kontrolle durch die zuständige Aufsichtsbehörde oder durch den Sächsischen Datenschutzbeauftragten, z. B. durch den jeweiligen Dienststellenleiter, durch eine vom Dienststellenleiter zu bestimmende Person (z. B. interner Datenschutzbeauftragter) oder das für Revisionen zuständige Amt (Rechnungsprüfungsamt) erfolgen.

11. Da Einrichtung und Betrieb automatisierter Abrufverfahren erhebliche Gefahren für das Persönlichkeitsrecht mit sich bringen, hat der Gesetzgeber das (vorsätzlich) unbefugte Bereithalten personenbezogener Daten zum Abruf und den (vorsätzlichen) unbefugten Abruf als **Ordnungswidrigkeiten** ins Sächsische Datenschutzgesetz aufgenommen (vgl. § 32 Abs. 1 Nr. 1 b, c SächsDSG). Werden solche Verstöße gegen Entgelt vorgenommen oder ist Bereicherungs- oder Schädigungsabsicht gegeben, ist dies nach § 33 SächsDSG sogar **strafbar**. Eine Befugnis liegt nur dann vor, wenn die **Zulässigkeitsvoraussetzungen** für die Einrichtung automatisierter Abrufverfahren beachtet werden (vgl. Nr. 4, 7, 8, 9).

12. Nach § 8 Abs. 2 Satz 2 SächsDSG sind vor Aufnahme des Abrufverfahrens von der bereithaltenden und abrufenden Stelle folgende Einzelheiten schriftlich festzulegen:

    (1) der Anlaß und der Zweck des Abrufverfahrens: Als Anlaß ist das jeweilige konkrete Ereignis (z. B. Wegzug aus einer Gemeinde, Sterbefall), das den Abruf rechtfertigen soll, festzuhalten. Als Zweck ist die gesetzliche Aufgabe der öffentlichen Stelle unter Angabe der Rechtsvorschrift anzugeben;

    (2) die Datenempfänger: Die abrufenden Stellen sind genau zu bezeichnen;

    (3) die abrufbaren Daten: Der abrufbare Datensatz ist bis auf Feldebene zu beschreiben;

    (4) die Maßnahmen zur Gewährleistung des Datenschutzes: Die zu treffenden Maßnahmen sind in § 9 SächsDSG aufgeführt. Insbesondere sind die Maßnahmen zur Abrufkontrolle (vgl. Nr. 9 und 10) anzugeben.

13. Nach § 8 Abs. 3 SächsDSG ist der Sächsische Datenschutzbeauftragte **vor** Einrichtung eines Abrufverfahrens zu unterrichten. Hinsichtlich des Umfangs der Unterrichtung gilt folgendes:

    - Bei Verfahren gemäß § 8 Abs. 1 SächsDSG sind das das automatisierte Abrufverfahren erlaubende Gesetz und ggf. die das Abrufverfahren näher regelnden Rechtsverordnungen und Satzungen mit Fundstelle anzugeben. Außerdem sind alle beabsichtigten technischen und organisatorischen Maßnahmen zur Gewährleistung des Datenschutzes im Sinne der vorliegenden Bekanntmachung mitzuteilen.

    - Bei Verfahren gemäß § 8 Abs. 2 SächsDSG hat sich der Umfang der Unterrichtung nach den in § 8 Abs. 2 Nr. 1 bis 4 SächsDSG genannten Vorgaben zu richten (vgl. Nr. 12).

14. Für den Abruf aus Datenbeständen, die der Allgemeinheit zur Benutzung offenstehen oder deren Veröffentlichung zulässig wäre, gelten gemäß § 8 Abs. 4 SächsDSG die Absätze 1 bis 3 nicht. Die Einrichtung automatisierter Abrufverfahren ist daher hinsichtlich dieser Daten unter den allgemeinen Voraussetzungen für Datenerhebungen und -übermittlungen zulässig (vgl. Nr. 4). Allerdings ist auch hier besonders zu prüfen, ob die Anwendung von § 8 Abs. 4 SächsDSG nicht durch eine speziellere Rechtsvorschrift ausgeschlossen ist. Beispielsweise dürfen nach § 33 Abs. 2 und 3 Sächsisches Meldegesetz Jubiläums-/Adreßbuchdaten zwar veröffentlicht werden, für den automatisierten Abruf dieser Daten bedarf es jedoch nach der speziellen Regelung des § 36 Nr. 4 Sächsisches Meldegesetz einer Erlaubnis durch Rechtsverordnung. Datenbestände stehen der Allgemeinheit zur Benutzung offen, wenn sie **allgemein zugänglich**, d. h. nicht auf eine bestimmte Nutzergruppe beschränkt sind. Dies trifft z. B. auf Literaturdatenbanken mit Autorenangabe in gemeindlichen Bibliotheken zu. Die **Veröffentlichung** personenbezogener Daten (=Übermittlung) ist beispielsweise durch öffentliche Stellen, die wissenschaftliche Forschung betreiben, unter den Voraussetzungen des § 30 Abs. 4 SächsDSG zulässig. Diese Daten könnten also automatisiert abgerufen werden, ohne daß dies durch ein

Gesetz erlaubt sein müßte oder die Voraussetzungen des § 8 Abs. 2 SächsDSG beachtet werden müßten.

Dresden, den 29. Juni 1994

Der Sächsische Datenschutzbeauftragte
In Vertretung
Schurig

16.1.2 **(SächsABl. S. 979)**

Bekanntmachung des Sächsischen Datenschutzbeauftragten zur Änderung der Bekanntmachung zur Datenverarbeitung im Auftrag und zur Rechtsstellung des beauftragten Unternehmers vom 3. November 1993 (SächsABl. S. 1304) Vom 29. Juni 1994

1. Die Rechtsauffassung, § 8 Abs. 2 des Gesetzes zum Schutz der informationellen Selbstbestimmung im Freistaat Sachsen (Sächsisches Datenschutzgesetz - SächsDSG) vom 11. Dezember 1991 (SächsGVBl. S. 401) gelte auch für die Einrichtung und den Betrieb automatisierter Abrufverfahren zwischen Auftraggeber und Auftragnehmer im Rahmen der Datenverarbeitung im Auftrag (im Sinne des § 7 SächsDSG), wird nicht aufrechterhalten.

2. Nummer 10 der Bekanntmachung vom 3. November 1993 erhält daher folgende dementsprechend **geänderte Fassung**:

   "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 SächsDSG (Übermitteln durch Abruf) finden daher keine Anwendung."

Dresden, den 29. Juni 1994

Der Sächsische Datenschutzbeauftragte
In Vertretung
Schurig

16.1.3 **(SächsABl. S. 979)**

Bekanntmachung des Sächsischen Datenschutzbeauftragten zu den Maßnahmen zur Gewährleistung des Datenschutzes (§ 9 Sächsisches Datenschutzgesetz - SächsDSG) Vom 30. Juni 1994

1. Das Sächsische Datenschutzgesetz verlangt in § 9 personelle, technische und organisatorische Maßnahmen zur Gewährleistung des Schutzes personenbezogener Daten.[1] Diese Maßnahmen sind nicht zu verwechseln mit technischen Maßnahmen zur "Datensicherung". Trotz großer Ähnlichkeit und sogar Gleichartigkeit können sie sich aufgrund der unterschiedlichen Zielstellung in ihrem Umfang unterscheiden. Dient der ”technische Datenschutz” dem gesetzgemäßen Umgang mit personenbezogenen Daten, hat die ”technische Datensicherung” dagegen den physischen Erhalt aller (nicht nur personenbezogener) Daten zum Ziel, die für die Datenverarbeitung benötigt werden. Dies ist bei der in § 10 Abs.1 Nr.8 SächsDSG von den Behörden geforderten Beschreibung der Maßnahmen gemäß § 9 SächsDSG zu beachten. Sie ist nicht auf die Datensicherung im technischen Sinn ausgerichtet, sondern auf die Gewährleistung des Grundrechts auf informationelle Selbstbestimmung.

   Bsp: Die ”technische Datensicherung” unterscheidet nicht zwischen befugter und unbefugter Kenntnisnahme personenbezogener Daten, wenn die Datenintegrität gewährleistet ist. Dagegen könnte unter datenschutzrechtlichen Gesichtspunkten der lesende Zugriff des Mitarbeiters untersagt werden, wenn er dadurch Einblick in personenbezogene Daten erhält, die er nicht zur Erfüllung seiner Aufgaben benötigt.

2. § 9 SächsDSG Abs.1 verlangt, daß der Aufwand der Maßnahmen in einem angemessenen Verhältnis zum Schutzzweck stehen muß, wobei die Art der zu schützenden Daten zu berücksichtigen ist. 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,
   Vermieterverzeichnisse

   Stufe B: Beeinträchtigung in der gesellschaftlichen Stellung oder den wirtschaftlichen Verhältnissen

   Beispiele: Mietverhältnisse,
   Geschäfts- und Vertragsbeziehungen,
   Zugehörigkeit zu Vereinen und Verbänden,

[1] Für die in § 35 SGB I genannten Stellen (Sozialleistungsträger) gelten § 79 Abs. 1 SGB X und § 9 BDSG. Diese Vorschriften enthalten ähnliche Regelungen wie § 9 SächsDSG.

verwandtschaftliche Beziehungen,
Bekanntenkreis.

Stufe C: Erhebliche Beeinträchtigung in der gesellschaftlichen Stellung oder den wirtschaftlichenVerhältnissen

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.

3. In § 9 Abs.2 SächsDSG wird für die zu treffenden geeigneten Maßnahmen der jeweilige Stand der Technik verlangt. Dies ist "der Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen oder Betriebsweisen, der die praktische Eignung einer Maßnahme zur Gewährleistung der Durchführung dieses Gesetzes gesichert erscheinen läßt. Bei der Bestimmung des Standes der Technik und der Organisation sind insbesondere vergleichbare Verfahren, Einrichtungen oder Betriebswesen heranzuziehen, die mit Erfolg im Betrieb erprobt worden sind" (§ 6 Abs. 2 BDSG alt). Damit sollen überspitzte Forderungen zur Sicherung des Datenschutzes vermieden werden, die zur Verhinderung von notwendiger Datenverarbeitung wegen fehlender ausreichender Datenschutzmöglichkeiten führen könnten. Andererseits könnten aber auch mit der gleichen Begründung wegen der Unverhältnismäßigkeit des Aufwandes an sich notwendige Datenschutzmaßnahmen eingespart werden. Um dies zu verhindern und einen den Umständen angemessenen Datenschutz zu gewährleisten, schreibt der Gesetzgeber einen dem technischen "Durchschnittswert" entsprechenden, in der Praxis bewährten Stand der Maßnahmen vor. Bei der Kostenfrage sollte bedacht werden, daß vordergründig billigere, einfachere Maßnahmen langfristig kostenträchtiger sein können als zum jetzigen Zeitpunkt noch teurere, aber innovativere Verfahren. Der

Neuaufbau der Verwaltung in Sachsen bietet die Möglichkeit, hier vorausschauend zu handeln.

4. Manipulationen, Transformationen und Gefährdungen von Daten sind bei ihrer Bearbeitung vielfältig möglich. Deshalb kann der Gesetzgeber keine konkreten Datensicherungsmaßnahmen vorschreiben. Neben Behördenleitern und Vorgesetzten ist jeder, der personenbezogene Daten verarbeitet, selbst dafür verantwortlich, spezielle Sicherheitsvorkehrungen vorzusehen und einzuhalten. § 9 Abs.2 SächsDSG fordert allgemeine Maßnahmen, die, obwohl sie im Wortlaut vorrangig auf die automatisierte Datenverarbeitung bezug nehmen, ebenso für die Datenverarbeitung in nicht-automatisierten Dateien oder Akten gelten. Darüber hinaus betont § 9 Abs.4 SächsDSG, daß für den letzteren Fall noch besondere Maßnahmen zu ergreifen sind. Dadurch soll verhindert werden, daß die nicht-automatisierte Verarbeitung personenbezogener Daten als angeblich datenschutzrechtlich "geringfügiger" angesehen wird und notwendige Maßnahmen vernachlässigt werden.

5. Der folgende Katalog konkreter Maßnahmen soll als **Hilfestellung** dienen. Er nimmt dem Anwender nicht ab, nach Maßgabe der gesetzlichen Vorschriften selbst zu entscheiden, welche personellen, technischen und organisatorischen Sicherungs-maßnahmen für den Schutz der bearbeiteten Daten sinnvoll, zweckmäßig und ausreichend sind. (Als generelle Regel bei der Vergabe von Rechten sollte gelten, daß von einer allgemeinen Zugriffsverweigerung ausgegangen wird und dann im Einzelfall Zugriffsrechte erteilt werden, sofern ein Nutzer die personenbezogenen Daten zu seiner Aufgabenerfüllung braucht und soweit er sie braucht.) Die Planung der Maßnahmen erfolgt zweckmäßigerweise auf Grundlage einer Risikoanalyse. Entscheidend ist, daß die einzelnen Maßnahmen nicht lösgelöst nebeneinander stehen, sondern in ihrer Gesamtheit zu einem abgestimmten Datenschutz- und Datensicherheitskonzept ohne Lücken führen. Neben technischen müssen auch bauliche und infrastrukturelle Aspekte berücksichtigt werden wie z. B. Lage des Raumes, Sicherheit der Fenster und Türen, Brandschutzvorschriften. Personelle Maßnahmen umfassen neben der personenbezogenen Festlegung von Verantwortlichkeiten auch die Schulung und die Information der Mitarbeiter, um so die persönliche Verantwortung und die Motivation des einzelnen Mitarbeiters für den Datenschutz zu fördern. Sicherheitstechnik bewirkt wenig, wenn sie wegen menschlicher oder organisatorischer Schwächen nicht oder nicht konsequent genutzt wird.

5.1 Zugangskontrolle

- Gebäudeschutz (außen, innen)
    - ° *Installation von Überwachungs- und Alarmanlagen (Feuer, Wasser, Bewegungsmelder)*
    - ° *Standortwahl (nicht im Erdgeschoß, Fenster-, Türsicherung)*
    - ° *Sicherheitsschlösser an den Zugangstüren*
    - ° *Schlüsselregelung*
- (automatisches) Zugangskontrollsystem mit Protokollierung
- revisionsfähiges Festlegen der Befugten (wer wann welche Zutrittsberechtigungen hat oder hatte)

- Löschen der Berechtigung beim Ausscheiden (Abgabe der Schlüssel und Ausweiskarte)
- Regelungen für Fremde (Besucher, Wartungspersonal, Reinigungsdienst)
- Schaffung von Sicherheitszonen (eingeschränkter Zugang für einzelne Räume, z. B. Archiv)
- Einsatz von Wachpersonal
- Verriegeln des PC
- Sperrung der Tastatur
- Verhindern von unberechtigtem Booten
- Paßwortzwang bei Inbetriebnahme

5.2 Datenträgerkontrolle

- Organisation der Datenträgerverwaltung
- Aufbewahrung in verschließbaren Schränken
- Aufbewahrung in Sicherheitsschränken (Data Safe)
- Abgabe der Datenträger nur an autorisierte Personen
- revisionsfähiger Datenträgeraustausch (Ausgangsbuch, Begleitzettel, Rücklaufkontrolle)
- vor Wiederverwendung beschriebener Datenträger physisches Löschen (z. B. Überschreiben)
- Bestandskontrolle
- ordnungsgemäße Vernichtung von Datenträgern
    - ° *Beachtung der DIN-Norm 32757*
    - ° *zuverlässige Vernichtung von Ausdrucken (Papier) durch Aktenvernichter*
    - ° *Protokollierung der Vernichtung (Verantwortlicher, Zeit, Ort, Art)*
- Verschlüsseln von Daten
- Sicherung der seriellen Schnittstelle
- Verhindern des Kopieren (z. B. Sperren des Copy-Befehls)

5.3 Speicherkontrolle

- Einsatz von Verfahren zur Identifizierung und Authentifikation
    - ° *Zuordnen von Benutzer und Funktion*
    - ° *Erstellen von Benutzerprofilen*
    - ° *Paßwortvergabe (Länge, Gültigkeitsdauer, Einwegverschlüsselung, Begrenzung der Fehlversuche)*
    - ° *Authentisierung durch andere Mittel (Chipkarte)*
- Zuordnen von Benutzer und Funktion an bestimmtes Terminal
- automatisierte Protokollierung und Auswertung der Protokolldatei (Festlegung von Art und Umfang)
- Versiegeln von Programmen (z. B. Checksummenprüfung)
- Plausibilitätskontrollen
- Einsatz von Sicherheitssoftware
- Sperren der Betriebssystemebene
- Löschen nicht mehr benötigter Dateien (physisch)
- Einsatz von Verschlüsselungsroutinen
- Trennen von Test- und Programmlauf

- Programmdokumentation
- Verhindern des Kopieren (Sperrung des Laufwerkes)

5.4 Benutzerkontrolle

- Einsatz von Verfahren zur Identifizierung und Authentifikation
    - ° *revisionsfähiges Festlegen der Berechtigungen (Benutzerprofile)*
    - ° *Paßwortvergabe (vgl. 5.3)*
    - ° *Abweisen unberechtigter Benutzer*
    - ° *Authentifikation durch andere Mittel (Chipkarte)*
- Zuordnen Benutzer/Funktion an bestimmtes Terminal
- Sperrung der Tastatur
- Verriegeln des PC
- Bootschutz für Laufwerke
- Sicherung der Übertragungsleitung
- Protokollierung versuchter und erfolgreicher Zugriffe
- Bildschirmverdunkelung bei Arbeitsunterbrechung, Weiterarbeit erst nach erneuter Paßworteingabe

5.5 Zugriffskontrolle

- Einsatz von Verfahren zur Identifizierung und Authentifikation
    - ° *Zuordnen von Benutzer und Funktion*
    - ° *Zuordnung von Ressourcen*
    - ° *Paßwortvergabe (vgl. 5.3)*
    - ° *Meldung der Fehlversuche*
    - ° *Authentifikation durch andere Mittel (Chipkarte)*
- Zuordnen von Benutzer und Terminal
- automatisierte Protokollierung und Auswertung (Art und Umfang festlegen)
- Sperren der Betriebssystemebene
- lückenlose Menüführung
- Sperren der Laufwerke
- Verschlüsseln und Sperren von Dateien und Verzeichnissen
- Sperren der Tastatur
- Bildschirmverdunkelung bei Arbeitsunterbrechung, Weiterarbeit erst nach erneuter Paßworteingabe
- Einsatz geeigneter Sicherheitssoftware
- zeitliche Beschränkung der Zugriffsmöglichkeit

5.6 Übermittlungskontrolle

- Führen einer Übersicht der Empfänger
- Verfahrensdokumentation
    - ° *für selbsttätige Abrufe und Übermittlungen*
- Netzwerkdokumentation
- sichere Übertragungsleitungen
- Protokollierung der Abrufe/ Übermittlungen
    - ° *stichprobenartig*

° *versuchter und erfolgreicher Zugriff*
- Einsatz von Verschlüsselungsverfahren

5.7 Eingabekontrolle

- Festlegen der Zuständigkeiten
  ° *schriftliche Dokumentation der Eingabeberechtigung für den Mitarbeiter*
- Vermerk auf Erfassungsunterlage
- Dokumentation von Eingabeprogrammen
  ° *Eingabe- oder Änderungsart*
  ° *eingegebene oder geänderteDaten*
- Protokollierung der Eingabe und Auswertung der Protokolle

5.8 Auftragskontrolle

(siehe dazu Bekanntmachung des Sächsischen Datenschutzbeauftragten zur Datenverarbeitung im Auftrag (§ 7 SächsDSG) vom 3. November 1993, SächsABl. S.1304)

- sorgfältige Auswahl des Auftragnehmers
- klare, schriftliche Vertragsgestaltung im Bereich des Datenschutzes
  ° *Kompetenzen und Pflichten abgrenzen*
  ° *Regelungen bei Datenschutzverstößen (z. B. Vertragsstrafen)*
- ordnungsgemäße Übergabe von Arbeitsergebnissen
  ° *schriftlicher Nachweis*
- sorgsamer Umgang mit maschinell lesbaren Datenträgern (Restdaten)
- Regelung für nicht mehr benötigte Unterlagen/ Daten (Rückgabe, Vernichtung)
- Einhaltung des Datengeheimnisses
- Kontrolle der Vertragsausführung

5.9 Transportkontrolle

- Übertragung über Standleitung
- Abschottung gegen unberechtigten Zugriff bei Wählleitung
- abgeschirmtes Kabel, Glasfaserkabel
- Einsatz von Verschlüsselungsverfahren
- Festlegung und Kontrolle der Transportwege
- sichere Transportbehälter
  ° *geschlossen*
  ° *versiegelt, verplombt*
- Transportbegleitpapiere
- Postversand als Wertsendung
- Sicherung gegen Verfälschung (elektr. Unterschrift, Checksummenbildung)
- Kopierschutz
- Vollständigkeitsprüfung

5.10 Organisationskontrolle

- Bestellen eines behördlichen Datenschutzbeauftragten
- Verpflichtung auf das Datengeheimnis

- Funktionstrennung
- schriftliche Dienstanweisung zum Datenschutz und zur Datensicherheit
- Mitarbeiterschulung
- Archivordnung
- Richtlinie über Aufbewahrungsfristen, Entsorgung und Datenträgerverwaltung
- Führen des Datei- und Geräteverzeichnisses (s. Bekanntmachung des Sächsischen Datenschutzbeauftragten zur Führung des Dateien -und Geräteverzeichnisses nach § 10 SächsDSG vom 29. September 1993, SächsABl. S.1175)
- Brand- und Katastrophenordnung (Notfallkonzept)
- revisionsfähige Dokumentation von Programmen
- Kontrolle der festgelegten Maßnahmen
- Risikoanalyse erstellen
    - ° *Schutzbedürftigkeit der Daten*
    - ° *mögliche Gefährdungen*
    - ° *Vorkehrungen zur Katastrophenabwehr (z.B. Feuer, Wasser)*

Dresden, den 30. Juni 1994

Der Sächsische Datenschutzbeauftragte
In Vertretung
Schurig

16.1.4 **(SächsABl. S. 982)**

Bekanntmachung des Sächsischen Datenschutzbeauftragten zur Auskunft nach § 17 des Sächsischen Datenschutzgesetzes Vom 1. Juli 1994

Nur eine Rechtsordnung, in der die Bürger aufgrund ihres aus dem allgemeinen Persönlichkeitsrecht folgenden Rechts auf informationelle Selbstbestimmung erfahren können, wer was wann bei welcher Gelegenheit weiß, ist nach dem Volkszählungsurteil des Bundesverfassungsgerichts (BVerfGE 65, 1 ff.) mit dem Grundgesetz vereinbar.

Aus diesem Grunde enthält das für die Behörden und sonstigen öffentlichen Stellen des Freistaates Sachsen geltende Sächsische Datenschutzgesetz (SächsDSG) mit § 17 eine Vorschrift, die den Bürgern die Informationsverarbeitung der Verwaltung - unabhängig von einem Verwaltungsverfahren - transparent und begreifbar machen soll.

Als das grundlegende Datenschutzrecht ist das Auskunftsrecht nach § 17 SächsDSG eine Vorbedingung für die Geltendmachung der weitergehenden Rechte auf Berichtigung, Sperrung und Löschung von Daten oder des Rechts auf Schadensersatz. Demgemäß hat jeder unabhängig von Alter, Wohnsitz und Nationalität das Recht auf Auskunft über die zu seiner Person gespeicherten Daten.

Die Behörden und sonstigen öffentlichen Stellen des Freistaates Sachsen sind somit verpflichtet, dem Betroffenen auf dessen Antrag **kostenfrei** Auskunft zu erteilen über:

- die zu seiner Person in einer Datei oder in Akten (einschließlich Bild- und Tonträger nach § 3 Abs. 5 SächsDSG) gespeicherten Daten,
- den Zweck der Speicherung, d. h. die zugrunde liegende Verwaltungsaufgabe,
- die Herkunft der Daten und über Personen und Stellen, an die übermittelt worden ist, sowie die übermittelten Daten, soweit dies gespeichert oder sonst bekannt ist.

Im einzelnen haben die öffentlichen Stellen folgendes zu beachten:

- **Zuständig** für die Auskunft ist die **speichernde Stelle**. Diese Zuständigkeit bleibt auch bestehen, wenn die Daten durch einen Auftragnehmer nach § 7 SächsDSG gespeichert werden. Gehen Auskunftsersuchen bei Auftragnehmern ein, sind sie an den Auftraggeber weiterzuleiten. Dies hat der Auftraggeber sicherzustellen.

- Voraussetzung für die Auskunft ist ein **Antrag des Betroffenen**, der möglichst an Hand von Suchkriterien (z. B. Aktenzeichen) beschreiben sollte, über welche Datenarten Auskunft erteilt werden soll. Weil die Funktionsfähigkeit der Verwaltung durch die Auskunft aber nicht beeinträchtigt werden darf, ist nach § 17 Abs. 3 Satz 2 SächsDSG der Auskunftsanspruch bei einer Speicherung von Daten in nicht zur Person geführten Akten davon abhängig, daß der Betroffene Angaben zur Auffindbarkeit macht und sein Informationsinteresse den Suchaufwand überwiegt. Diese Einschränkung des Auskunftsanspruchs gilt auch für personenbezogene Daten in nicht-automatisierten Dateien, die nicht zur Übermittlung an Dritte bestimmt sind (z. B. Karteien, die als Arbeitsplatzablage geführt werden).

- Die zur Auskunft verpflichtete speichernde Stelle bestimmt nach § 17 Abs. 4 SächsDSG nach pflichtgemäßem Ermessen das **Verfahren der Auskunftserteilung**. Liegen die Voraussetzungen für eine Auskunft aus **Akten** nach § 17 Abs. 3 SächsDSG vor, hat die speichernde Stelle auf Verlangen dem Betroffenen Akteneinsicht zu gewähren, jedoch nur, wenn berechtigte Interessen Dritter hierdurch nicht beeinträchtigt werden. Deshalb ist bei der Einsichtnahme sicherzustellen, daß der Auskunftssuchende nur die zu seiner Person gespeicherten Daten zur Kenntnis nehmen kann und keine personenbezogenen Daten dritter privater Personen, deren Persönlichkeitsrecht ebenfalls schutzbedürftig ist, zur Kenntnis erhält. Ist dies nicht möglich, ist nur Auskunft durch Übersendung einer die Daten Dritter nicht enthaltenden Abschrift (Ablichtung) der betreffenden Aktenstücke zu erteilen.

  Als Grundsatz ist zu beachten, daß durch die Auskunft der Betroffene in die Lage versetzt werden muß, den Prozeß des Umgangs mit den ihn betreffenden Informationen nachzuvollziehen und seine Bedeutung abzuschätzen. Es reicht nicht aus, dem Betroffenen lediglich mitzuteilen, daß bestimmte Daten über ihn gespeichert sind (z. B. "im Zusammenhang mit Ihrem Antragsverfahren sind Daten über Sie gespeichert"). Erforderlich ist vielmehr die Erläuterung der Verwendung (z. B. "zu den in § ... (Rechtsvorschrift) genannten Zwecken sind bei uns zu Ihrer Person folgende Daten gespeichert:").

- Die Auskunft ist nach dem Datenbestand zum **Zeitpunkt des Auskunftsantrages** zu erteilen. Die Auskunftsverpflichtung entfällt nicht dadurch, daß eine datenverarbeitende Stelle nach Eingang des Antrages feststellt, eine Datenspeicherung sei unzulässig und die Daten müßten gelöscht werden. Hat sich der Datenbestand seit dem Zeitpunkt des Auskunftsantrages verändert, sollte auch hierüber Auskunft erteilt werden.

- Vor der Auskunftserteilung muß die **Identität des Antragstellers** geprüft werden. Spricht der Antragsteller persönlich bei der speichernden Stelle vor, ist die Identität auf Grund der üblichen Legitimationspapiere (Personalausweis, Paß und ähnliche Legitimationspapiere) zu prüfen und der Antrag und das **Ergebnis** der Identitätsprüfung schriftlich festzuhalten, wobei die Ausweisdaten nicht gespeichert werden dürfen (z. B. "persönlich bekannt" oder "Paß/Personalausweis hat vorgelegen").

  Wird das Auskunftsersuchen schriftlich gestellt, ist je nach Lage des Einzelfalls, insbesondere nach der Schutzwürdigkeit, zu beurteilen, ob bei postalischer Versendung an den Antragsteller in ausreichendem Maße sichergestellt ist, daß die Auskunft nur an ihn persönlich gelangt. Enthält die Auskunft besonders sensible Daten, von denen auch Angehörige keine Kenntnis erhalten sollen, sind besondere Vorkehrungen (z. B. "Einschreiben - eigenhändig") zu treffen.

  Fernmündliche Auskünfte sind ausgeschlossen, wenn der Antragsteller auch durch Rückruf nicht sicher identifiziert werden kann. Auch für eine Auskunft über Telefax sind besondere Sicherungsvorkehrungen zu beachten (siehe hierzu Bekanntmachung des Sächsischen Datenschutzbeauftragten vom 14. Juni 1993, Sächsisches Amtsblatt S. 894).

- Das umfassende Auskunftsrecht des Betroffenen ist nach § 17 Abs. 5 SächsDSG eingeschränkt, wenn die Auskunft mit dem **Geheimnisschutz** unvereinbar wäre, weil die personenbezogenen Daten oder die Tatsache ihrer Speicherung wegen einer **Rechtsvorschrift** oder der **überwiegenden Geheimhaltungsinteressen** der speichernden Stelle oder eines Dritten als Geheimnis behandelt werden müssen. Hier muß das Informationsinteresse des Betroffenen zurücktreten. Die Auskunft darf dann nicht erteilt werden. In diesem Zusammenhang zu beachtende Rechtsvorschriften sind in erster Linie auf dem Gebiet des materiellen und persönlichen Geheimschutzes zu finden. Weil die meisten Geheimhaltungsvorschriften dem Schutz des Betroffenen dienen, wird eine Auskunftsverweigerung aber nur in seltenen Fällen auf eine der Auskunft entgegenstehende Rechtsvorschrift gestützt werden können. Ein Beispiel findet sich in § 61 Abs. 2 und 3 Personenstandsgesetz, wonach eine Mitteilung über den Geburtseintrag im Personenstandsbuch an das noch nicht über sechzehn Jahre alte angenommene Kind bzw. im Falle eines Sperrvermerks an das nicht über sechzehn Jahre alte nichteheliche oder für ehelich erklärte Kind ausgeschlossen ist. Auch ist denkbar, daß personenbezogene Daten Gegenstand eines Staatsgeheimnisses sind und keine Befugnis zur Mitteilung an den Betroffenen besteht (§§ 93 ff. StGB).

Die überwiegende Zahl der Auskunftsverweigerungen wird darauf gestützt werden, daß die Daten wegen der berechtigten Interessen einer dritten Person geheimgehalten werden müssen. In Betracht kommt hier in erster Linie das Interesse von Hinweisgebern und Gewährspersonen der speichernden Stelle an der Geheimhaltung ihres Namens - allerdings nur, wenn die Informationssammlung durch die Gewährsperson nicht als verwerflich anzusehen ist. Die Geheimhaltung muß in diesem Falle auch im Interesse der öffentlichen Stelle und der Allgemeinheit liegen.

- Die **Auskunftsverweigerung** ist ein belastender Verwaltungsakt. Sie ist grundsätzlich zu begründen, damit der Betroffene seine Rechtsschutzmöglichkeiten prüfen kann. Von der **Pflicht zur Begründung** ist die speichernde Stelle gemäß § 17 Abs. 6 SächsDSG nur in den Fällen befreit, in denen die Mitteilung der tatsächlichen und rechtlichen Gründe die mit der Ablehnung verfolgten Zwecke gefährden würde. Damit soll vermieden werden, daß aus der Begründung einer Auskunftsverweigerung Rückschlüsse auf den Inhalt der gespeicherten Daten gezogen werden können.

  Mit der Auskunftsverweigerung verliert der Betroffene die Möglichkeit, selbst zu prüfen, ob sein Recht auf informationelle Selbstbestimmung und seine sonstigen schutzwürdigen Belange durch die Verarbeitung der auf ihn bezogenen Daten verletzt ist. Damit auch in diesem Fall eine rechtliche Prüfung ermöglicht wird, hat die auskunftsverweigernde Stelle nach § 17 Abs. 6 Satz 2 SächsDSG dem Betroffenen auf den Sächsischen Datenschutzbeauftragten und auf dessen Kontrollmöglichkeiten hinzuweisen. Diesem ist auf Verlangen des Betroffenen die Auskunft zu erteilen, wobei die Mitteilung des Sächsischen Datenschutzbeauftragten an den Betroffenen keine Rückschlüsse auf den Erkenntnisstand der speichernden Stelle zulassen darf, es sei denn, diese stimmt einer weitergehenden Auskunft zu.

- **Einschränkungen der Auskunftspflicht** der speichernden Stelle sieht § 17 Abs. 7 SächsDSG in den Fällen vor, in denen sich die Auskunftserteilung auf die Übermittlung personenbezogener Daten an Staatsanwaltschaften, Polizeidienststellen, andere für die Strafverfolgung zuständige Stellen, Verfassungsschutzbehörden, dem Bundesnachrichtendienst oder dem Militärischen Abschirmdienst bezieht. Um auszuschließen, daß mit einer Auskunftserteilung die Belange dieser Stellen gefährdet werden, ist jeweils vorher die Erklärung dieser Stellen einzuholen, daß Geheimhaltungsvorschriften und Geheimhaltungsinteressen dieser Stellen und Dritter nicht vorliegen.

- Zu beachten ist, daß **besondere Regelungen zur Auskunftspflicht** öffentlicher Stellen dem § 17 SächsDSG vorgehen. Solche Rechtsvorschriften sind z. B. § 24 des Sächsischen Meldegesetzes, § 9 des Sächsischen Verfassungsschutzgesetzes, § 120 des Sächsischen Beamtengesetzes (Personalakteneinsichtsrecht für Beamte), § 31 Abs. 3 SächsDSG (Anspruch der Angestellten und Arbeiter auf Auskunft über ihre Personalunterlagen und die Art der aus diesen Unterlagen gefertigten automatisierten Auswertungen). Wichtig sind in diesem Zusammenhang auch die Akteneinsichtsregelungen in Verfahrensgesetzen wie z. B. § 29 des Verwaltungsverfahrensgesetzes (VwVfG), § 99 der Verwaltungsgerichtsordnung (VwGO), § 34 des Gesetzes über Angelegenheiten der freiwilligen Gerichtsordnung (FGG). Für die in § 35 SGB I genannten Stellen (Sozialleistungsträger) gelten § 79 I SGB X i. V. m. § 19 des Bundesdatenschutzgesetzes: § 17 SächsDSG wird nicht angewandt. An die Stelle des in § 19 Abs. 6 genannten Bundesbeauftragten für den Datenschutz tritt der Sächsische Datenschutzbeauftragte.

  Diese die Verfahrensbeteiligten betreffenden bereichsspezifischen Auskunftsregelungen haben gemäß dem Subsidiaritätsprinzip des § 2 Abs. 4 SächsDSG Vorrang vor § 17 SächsDSG.

Dresden, 1. Juli 1994

Der Sächsische Datenschutzbeauftragte
In Vertretung
Schurig

16.2 Entschließungen der Datenschutzbeauftragten des Bundes und der Länder

16.2.1 Entschließung der 48. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 26./27. September 1994 in Potsdam zum geänderten Vorschlag für eine Europäische Richtlinie zum Datenschutz im ISDN und in Mobilfunknetzen vom 13. Juni 1994 (KOM (94) 128 endg. - COD 288)

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt es, daß die Europäische Kommission mit der Vorlage des geänderten Vorschlags für eine Richtlinie zum Datenschutz im ISDN ihre Absicht bekräftigt hat, unionsweit bereichsspezifische Regelungen für den Datenschutz in Telekommunikationsnetzen zu schaffen. Es kann kein Zweifel daran bestehen, daß die digitalen Telekommunikationsnetze in der Europäischen Union zunehmend zur wichtigsten Infrastruktur für die Verarbeitung personenbezogener Daten werden. Der Regelungsdruck wird erhöht durch die Tatsache, daß die Europäische Union die rechtlichen und technischen Voraussetzungen für die Liberalisierung der Telekommunikationsmärkte in weiten Bereichen bereits geschaffen hat und mehrere Mitgliedsstaaten, darunter Deutschland, derzeit ihr nationales Telekommunikationsrecht auf die Vorgaben der EU umstellen.

Aus diesem Grund sollte der geänderte Vorschlag für eine ISDN-Richtlinie so bald wie möglich vom Ministerrat und vom Europäischen Parlament abschließend beraten werden. Die Bundesregierung sollte die deutsche Ratspräsidentschaft dazu nutzen, den geänderten Vorschlag für eine ISDN-Richtlinie im Rat behandeln zu lassen.

Dabei sollte sich die Bundesregierung insbesondere für folgende Verbesserungen des Richt- linienvorschlags aus datenschutzrechtlicher Sicht einsetzen:

1. Für Telekommunikationsorganisationen und Diensteanbieter müssen die gleichen gemeinschaftsrechtlichen Regelungen zum Datenschutz gelten. Die Verarbeitung personenbezogener Daten durch Diensteanbieter darf nicht privilegiert werden.

2. Die Beschränkung der Datenverarbeitung auf Zwecke der Telekommunikation sollte wieder in die Richtlinie aufgenommen werden. Der allgemeine Zweckbindungsgrundsatz der Datenschutzrichtlinie läßt die Zweckentfremdung schon bei "berechtigten Interessen" der Verarbeiter zu. Das ist angesichts zunehmender Diversifizierung der Aktivitäten von Netzbetreibern und Diensteanbietern eine zu weitgehende Lockerung der Zweckbindung im Telekommunikationsbereich.

3. Das ursprünglich vorgesehene Verbot, personenbezogene Daten zur Erstellung von elektronischen Profilen der Teilnehmer zu nutzen, sollte wieder in die Richtlinie aufgenommen werden.

4. Die Speicherung von Inhaltsdaten nach Beendigung der Übertragung sollte - wie im ursprünglichen Richtlinienentwurf vorgesehen - untersagt werden.

5. Die Vertraulichkeit der Kommunikationsbeziehungen und -inhalte (Fernmeldegeheimnis) sollte - wie es der ursprüngliche Richtlinienvorschlag ebenfalls vorsah - auf Unionsebene garantiert werden.

6. Um eine Harmonisierung des Gemeinschaftsrechts beim Einzelgebührennachweis zu erreichen, sollten konkrete Vorgaben in die Richtlinie aufgenommen werden, z. B. indem den angerufenen Teilnehmern die Aufnahme ihrer Rufnummer in Einzelgebührennachweise freigestellt wird.

7. Im Fall der Anrufweiterschaltung sollte die automatische Information des anrufenden Teilnehmers darüber, daß sein Anruf (z. B. bei einem Arzt) an einen Dritten weitergeschaltet wird, gewährleistet sein.

Die Konferenz begrüßt die im geänderten Vorschlag vorgesehene Kostenfreiheit für die verschiedenen Optionen der Anzeige der Rufnummer des Anrufers und für die Nichtaufnahme von Daten in das Teilnehmerverzeichnis (Telefonbuch).

Diese Vorschläge berücksichtigen das Subsidiaritätsprinzip und beschränken sich auf Änderungen, die zur Gewährleistung der Vertraulichkeit der Kommunikation in der Europäischen Union realisiert werden müssen. Zudem wird die Europäische Union insoweit im Rahmen ihrer ausschließlichen Zuständigkeit tätig. Die Konferenz bittet auch die Entscheidungsträger auf Unionsebene sowie die Datenschutzbehörden der anderen Mitgliedsstaaten, diese Anregungen zu unterstützen.

16.2.2 Entschließung der 48. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 26./27. September 1994 in Potsdam zu Vorschlägen zur Überprüfung der Erforderlichkeit polizeilicher Befugnisse und deren Auswirkungen für die Rechte der Betroffenen

Angesichts der aktuellen Diskussion über die innere Sicherheit weisen die Datenschutzbeauftragten des Bundes und der Länder darauf hin, daß umfangreiche polizeiliche Befugnisse zur Erhebung und Verarbeitung personenbezogener Daten, insbesondere im technischen Bereich, gesetzlich verankert worden sind.

Zum Kreis der Betroffenen zählen dabei nicht nur Personen, gegen die Verdachtsgründe vorliegen, sondern auch nichtverdächtige Kontakt- und Begleitpersonen und Unbeteiligte, deren Schutz nach Auffassung der Datenschutzbeauftragten besonders wichtig ist.

Vor diesem Hintergrund schlagen die Datenschutzbeauftragten vor, den derzeitigen Erkenntnisstand über die Erforderlichkeit polizeilicher Befugnisse zur Erhebung und Verarbeitung personenbezogener Daten sowie ihre Auswirkungen auf die Rechte der Betroffenen durch folgende Maßnahmen zu verbessern:

1. Die Datenschutzbeauftragten teilen die von einigen Innenministern vertretene Auffassung, daß bloße Angaben über Einsatzzahlen der besonderen Befugnisse zur Datenerhebung nur einen begrenzten Aussagewert haben. Aufschluß über die tatsächliche Praxis, ihre Erforderlichkeit und Verhältnismäßigkeit läßt sich nur durch

Überprüfung und Auswertung der einzelnen Einsätze gewinnen. Hierzu müssen unter Beteiligung der Datenschutzbeauftragten und der Wissenschaft, insbesondere der Kriminologie und des Polizeirechts, objektive und nachprüfbare Auswertungskriterien entwickelt werden.

Die Datenschutzbeauftragten begrüßen daher die Initiative für eine sogenannte Rechtstatsachensammlung, die Erhebungen zu polizeilichen Ermittlungsmethoden und Eingriffsbefugnissen durchführen soll. Sie schlagen vor, in diese Rechtstatsachensammlung insbesondere Angaben über den Anlaß einer Datenerhebung mit besonderen Mitteln, die Örtlichkeit und die Dauer der Maßnahme, den Umfang der überwachten Gespräche, den betroffenen Personenkreis sowie die Anzahl der ermittelten, verurteilten, aber auch der entlasteten Personen einzubeziehen. Derartige Aufstellungen wären nicht nur für elektronische Überwachungsmethoden, sondern auch für Observationen, den Einsatz verdeckter Ermittler und V-Personen sowie für Rasterfahndungen denkbar.

2. Einige Polizeigesetze verpflichten dazu, zu überprüfen, ob es notwendig ist, bestehende Dateien weiterzuführen oder zu ändern. Dabei soll nicht nur darauf eingegangen werden, ob die Anwendungen, das heißt die Dateien, weiterhin erforderlich sind, sondern auch auf ihren Nutzen sowie auf ihre Schwachstellen und Mängel. Ferner sind Vorschläge zu machen, wie festgestellte Defizite beseitigt oder minimiert werden können.

3. Die Datenschutzbeauftragten gehen davon aus, daß sie bei den Überlegungen zur Rechtstatsachensammlung rechtzeitig beteiligt und die jeweiligen Materialien und Zwischenergebnisse mit ihnen erörtert werden.

16.2.3 Entschließung der 48. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 26./27. September 1994 in Potsdam zu fehlenden bereichsspezifischen gesetzlichen Regelungen bei der Justiz

Obwohl seit dem Volkszählungsurteil des Bundesverfassungsgerichts mehr als 10 Jahre vergangen sind, werden im Bereich der Justiz sensible personenbezogene Daten nach wie vor ohne die vom Bundesverfassungsgericht geforderten bereichsspezifischen gesetzlichen Grundlagen erhoben und verarbeitet. Stattdessen sind in den letzten Jahren in zunehmendem Maße automatisierte Verfahren neu eingesetzt worden. Die Eingriffe in das Recht auf informationelle Selbstbestimmung stützen die Justizverwaltungen auf die Rechtsprechung des Bundesverfassungsgerichts zum sogenannten Übergangsbonus.

Die Datenschutzbeauftragten des Bundes und der Länder weisen im Hinblick auf die kommende Legislaturperiode den Bundesgesetzgeber erneut darauf hin, daß gesetzliche Regelungen im Bereich der Justiz überfällig sind. Dabei ist nicht die jeweils geübte Praxis zu legalisieren, sondern es muß vorab unter datenschutzrechtlichen Gesichtspunkten geprüft werden, welche Form der Datenerhebung und -verarbeitung in welchem Umfang erforderlich ist. Der zur Zeit dem Bundesrat vorliegende Entwurf eines Strafverfahrensänderungsgesetzes beispielsweise wird datenschutzrechtlichen Anforderungen in keiner Weise gerecht.

Im Bereich der Justiz fehlen ausreichende gesetzliche Regelungen für die
- Datenverarbeitung im Strafverfahren, insbesondere in automatisierten Dateien,
- Datenerhebung, -verarbeitung und -nutzung im Strafvollzug,
- Übermittlung von Daten aus den bei Gerichten geführten Registern (z. B. Grundbuch) und deren Nutzung durch die Empfänger,
- Datenübermittlung von Amts wegen durch Gerichte und Staatsanwaltschaften an Gerichte, Behörden und sonstige öffentliche Stellen (Justizmitteilungsgesetz),
- Aufbewahrung von Aktenkarteien und sonstigen Unterlagen sowie die Dauer der Speicherung in automatisierten Dateien.

Eine Berufung auf den sogenannten Übergangsbonus auf unbegrenzte Zeit steht nicht in Übereinstimmung mit der Rechtsprechung des Bundesverfassungsgerichts. Die Datenschutzbeauftragten halten es deshalb zum Schutz des Rechts des Einzelnen auf informationelle Selbstbestimmung für geboten, wegen der mit der Datenerhebung, Verarbeitung und Nutzung verbundenen Rechtseingriffe in der neuen Legislaturperiode unverzüglich bereichsspezifische Regelungen der materiellen Voraussetzungen sowie der organisatorischen und verfahrensrechtlichen Vorkehrungen zu schaffen, welche der Gefahr einer Verletzung des Persönlichkeitsrechtes des Bürgers entgegenwirken.

16.2.4 Entschließung der 48. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 26./27. September 1994 in Potsdam zu datenschutzrechtlichen Anforderungen an ein Übereinkommen der Mitgliedstaaten der Europäischen Union über die Errichtung eines europäischen Polizeiamtes (Europol)

Die Datenschutzbeauftragten der Länder gehen gemeinsam mit dem Bundesdatenschutzbeauftragten davon aus, daß bei den Verhandlungen mindestens folgende Punkte berücksichtigt werden:

- Das Übereinkommen muß der verfassungsrechtlichen Kompetenzverteilung in Bund und Ländern für die Polizei entsprechen. Die materielle Verantwortung für die Daten verarbeitung muß, soweit die Daten von Landesbehörden erhoben worden sind, weiterhin bei den Ländern liegen. Davon bleiben die Zuständigkeiten und die dazugehörigen Befugnisse des BKA als nationale Stelle für den Informationsverkehr mit EUROPOL unberührt.

- Die Regelungen zur Verarbeitung personenbezogener Daten müssen präzise sein und dem Grundsatz der Verhältnismäßigkeit entsprechen. Beispielsweise erfüllen die in den bisherigen Entwürfen vorgesehenen Befugnisse zur europaweiten Speicherung von Daten unbeteiligter Personen diese Voraussetzungen nicht.

Die Datenschutzbeauftragten erwarten, daß die deutsche Seite eine Klarstellung über die Verantwortung der Länder, z. B. durch eine Protokollerklärung zum EUROPOL-Übereinkommen, trifft.

16.2.5 Entschließung der 48. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 26./27. September 1994 in Potsdam zu Art. 12 Verbrechensbekämpfungsgesetz zur Trennung von Polizei und Nachrichtendiensten

Geheimdienstliche Informationsmacht und polizeiliche Exekutivbefugnisse müssen strikt getrennt bleiben. Die Datenschutzbeauftragten des Bundes und der Länder stellen mit Besorgnis Entwicklungen fest, die die klare Trennungslinie zwischen Nachrichtendiensten und Polizeibehörden weiter zu verwischen drohen. Dies betrifft vor allem den Einsatz des Bundesnachrichtendienstes nach dem Verbrechensbekämpfungsgesetz:

- Der BND erhält danach bei der Fernmeldeaufklärung auch Befugnisse, die auf eine gezielte Erhebung von Daten für polizeiliche Zwecke hinauslaufen können. Deshalb ist bei dem Vollzug des Gesetzes darauf zu achten, daß nicht gezielt Informationen gesammelt werden, die vom Auftrag des BND nicht umfaßt werden.

- Zwischen nachrichtendienstlichen Vorfelderkenntnissen und polizeilichen Zwangsmaßnahmen ist ein Filter erforderlich, der vor allem Unbeteiligte vor überzogenen Belastungen schützt.

Die Datenschutzbeauftragten fordern, für die Zusammenarbeit von Nachrichtendiensten und Polizei in der Durchführung und Gesetzgebung das Trennungsgebot strikt zu beachten. Dies gilt auch bei der Fernmeldeaufklärung des BND. Eine wirksame Kontrolle durch den Datenschutzbeauftragten in diesem sensiblen Bereich ist auch nach der Rechtsprechung des Bundesverfassungsgerichts sicherzustellen.

16.2.6 Entschließung der 49. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 9./10. März 1995 in Bremen zum Entwurf eines Gesetzes über das Bundeskriminalamt (BKA-Gesetz) - Bundesrats-Drucksache 94/95

Zu den Beratungen des Entwurfs für ein Gesetz über das Bundeskriminalamt erklären die Datenschutzbeauftragten des Bundes und der Länder:

Auch aus Sicht des Datenschutzes ist es zu begrüßen, daß die seit langem überfälligen bereichsspezifischen Regelungen zur bundesweiten polizeilichen Datenverarbeitung insbesondere im polizeilichen Informationssystem (INPOL) nunmehr in das Gesetzgebungsverfahren eingebracht werden. Der Gesetzentwurf enthält im Vergleich zu den Vorentwürfen eine Reihe von Vorschriften, die datenschutzrechtlich positiv zu werten sind. Hierzu gehören:

- der Verzicht auf die im Vorentwurf vorgesehenen Befugnisse zur sogenannten "Feststellung des Anfangsverdachts";

- das Erfordernis der Einwilligung für die Speicherung von Daten über Zeugen und mögliche Opfer;

- Übermittlungsverbote bei überwiegenden schutzwürdigen Interessen der Betroffenen oder bei entgegenstehenden gesetzlichen Verwendungsregelungen;

- die Beachtung landesgesetzlicher Löschungsfristen.

Andererseits begegnet der Gesetzentwurf jedoch nach wie vor gewichtigen Bedenken, da er tiefe Eingriffe in die Rechte von Betroffenen ermöglicht, deren Voraussetzungen und Reichweite unklar oder nicht durch überwiegende Interessen der Allgemeinheit gerechtfertigt sind. Dies gilt insbesondere für

- die Verwendung des Begriffs der Straftaten von erheblicher Bedeutung ohne Definition, um welche Tatbestände es sich handelt, weil damit nicht mehr voraussehbar ist, wann die an diesen Begriff anknüpfenden Eingriffsbefugnisse zur Datenverarbeitung eröffnet sind;

- die Befugnisse der Zentralstelle zu selbständigen Datenerhebungen und Übermittlungen bis hin zum automatisierten Datenverbund mit ausländischen und zwischenstaatlichen Stellen ohne Einvernehmen mit den jeweils verantwortlichen Länderpolizeien;

- die unklare Abgrenzung der Datenverarbeitungsbefugnisse im Hinblick auf die unterschiedlichen Befugnisse zur Strafverfolgung, Gefahrenabwehr, Verhütung von Straftaten und Vorsorge für künftige Strafverfolgung sowie die fehlende klare Zweckbindungs- und Zweckänderungsregelung;

- die Befugnis zur verdeckten Datenerhebung aus Wohnungen ohne eindeutige Begrenzung auf den Schutz gefährdeter Ermittler.

Die Datenschutzbeauftragten fordern den Gesetzgeber auf, die Schwachstellen des Entwurfs auszuräumen. Insbesondere fordern sie klare verfassungskonforme Regelungen zur Auskunftserteilung an Betroffene und der Prüfrechte für INPOL-Daten dahingehend, daß die Datenschutzkontrollrechte bei der datenschutzrechtlichen Verantwortung der Stellen anknüpfen, die die Speicherung im INPOL-System selbst vornehmen oder veranlassen.

16.2.7 Entschließung der 49. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 9./10. März 1995 in Bremen zum Datenschutz bei elektronischen Mitteilungssytemen

Es ist damit zu rechnen, daß in Zukunft mit Hilfe elektronischer Mitteilungssysteme rechtsverbindliche bedeutsame Informationen und insbesondere personenbezogene Daten über Netze ausgetauscht werden.

Die zunehmende Nutzung von elektronischen Mitteilungssystemen (Electronic-Mail, Dokumentenaustausch über Datenfernübertragung, Message Handling Systems MHS/X.400) hat zur Folge, daß Bedrohungen wie Verlust von Vertraulichkeit, Integrität, Verfügbarkeit und Verbindlichkeit verschärft werden, weil Unbefugte Zugriffe auf Daten und Programme erhalten können und die Übertragungswege vom Kommunikationspartner nicht sicher zu kontrollieren sind. Deshalb ist beim Einsatz solcher Systeme das

Risikobewußtsein bei den Verantwortlichen sowie den Anwendern zu schärfen. In diesem Zusammenhang gewinnt der Schutz der elektronisch gespeicherten, verarbeiteten und übertragenen Information durch eine Vielzahl umfassender aufeinander abgestimmter Sicherheitsmaßnahmen an Bedeutung.

Die Datenschutzbeauftragten des Bundes und der Länder fordern, daß den folgenden Sicherheitsaspekten beim Einsatz von elektronischen Mitteilungssystemen Rechnung getragen wird:

1. Authentizität von Benutzern, Nachrichten und Systemmeldungen

Für den Empfänger einer Nachricht muß jederzeit die Möglichkeit bestehen, anhand bestimmter Kriterien die Authentizität des Absenders, der Nachricht sowie der an ihn gerichteten Systemmeldungen (z. B. Empfangs- und Weiterleitungsbestätigungen, Sendeanforderungen, Teilnehmerkennungen, Teilnehmereinstufungen) zu überprüfen.

2. Vertraulichkeit von übertragenen Daten

Für alle Arten von Daten in elektronischen Mitteilungssystemen - Nachrichten sowie Verkehrs- und Verbindungsdaten - muß die Vertraulichkeit gewahrt bleiben. Sie ist durch geeignete Maßnahmen, z. B. kryptografische Verfahren, sicherzustellen.

3. Integrität von Nachrichten und Meldungen

Es ist zu gewährleisten, daß bei Speicherung und Weiterleitung von Daten keine unbefugte, unerkannte Veränderung erfolgen kann.

4. Fälschungssichere Kommunikationsnachweise

Die für die Anerkennung einer elektronischen Kommunikation erforderlichen fälschungssicheren Sende-, Empfangs- und Übertragungsnachweise müssen dem Anwender auf Wunsch zur Verfügung stehen.

5. Ausschluß von Kommunikationsprofilen

Die Erstellung von Kommunikationsprofilen muß verhindert werden. Gespeicherte Protokollierungsdaten dürfen nur zu Zwecken des Datenschutzes und der Datensicherung (§§ 14 Abs. 4, 31 BDSG bzw. landesgesetzliche Regelungen) verwendet werden.

Empfehlungen zum Einsatz von elektronischen Mitteilungssystemen:

Zum sicheren Einsatz von elektronischen Mitteilungssystemen sind als Grundschutzmaßnahmen folgende Empfehlungen zu beachten.

1. Grundsätzlich sind nur solche Produkte einzusetzen, die die Sicherheitsfunktionen der X.400-Empfehlung aus dem Jahre 1988 erfüllen. Vorhandene Systeme - insbesondere solche, die noch auf Empfehlungen von 1984 basieren - sollen künftig durch geeignete

Zusatzprodukte hinsichtlich ihrer Sicherheit verbessert oder durch neuere Softwareversionen ersetzt werden.

2. Bei Übertragung von personenbezogenen Daten ist eine Verschlüsselung vorzusehen. Die Verschlüsselung der Daten muß mit einem hinreichend sicheren Verschlüsselungsverfahren erfolgen. Neben der Auswahl eines effektiven Verschlüsselungsalgorithmus (z. B. DES, IDEA) muß dabei insbesondere eine ordnungsgemäße Schlüsselerzeugung, -verwaltung und -verteilung gewährleistet sein. Verschlüsselungskomponenten sind durch technische, bauliche und organisatorische Maßnahmen vor dem Zugriff Unbefugter zu schützen.

3. Zur Absicherung der Integrität der Daten sollte auf Verfahren der "elektronischen Unterschrift" zurückgegriffen werden.

4. Nach Möglichkeit ist die Funktion des Systemverwalters von der des Netzwerkverwalters - insbesondere der Verwaltung des elektronischen Mitteilungssystems - aus Sicherheitsgründen zu trennen.

5. Es ist grundsätzlich separat administrierbare Hard- oder Software - z. B. in Form eines Kommunikationsservers - für das elektronische Mitteilungssystem vorzusehen.

6. Bei Verwendungen von öffentlichen Übertragungswegen, sind die vorhandenen Sicherheitsmechanismen dieser Netze z. B. geschlossene Benutzergruppen, Rufnummernidentifikation, Teilnehmerzeichengabe und automatische Rückruffunktion zur Abwehr des Zugriffs durch externe zu nutzen.

7. Zur Beweissicherung einer stattgefundenen Kommunikation sollte die eingesetzte Software folgende Funktionen beinhalten:
   - Zustellung/Empfangsnachweise
   - Sende/Empfangsübergabenachweise.

16.2.8 Entschließung der 49. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 9./10. März 1995 in Bremen zur automatischen Erhebung von Straßennutzungsgebühren

Gegenwärtig werden Systeme zur automatischen Erhebung von Straßenbenutzungsgebühren in mehreren Versuchsfeldern erprobt. Sie können im Rahmen der weiteren Entwicklung zu zentralen Komponenten umfassender Verkehrstelematiksysteme (z. B. Verkehrsinformation und -leitung) werden.

Mit der Einführung derartiger Verkehrstelematiksysteme besteht die Gefahr, daß personenbezogene Daten über den Aufenthaltsort von Millionen Verkehrsteilnehmern, erhoben und verarbeitet werden. Exakte Bewegungsprofile können dadurch erstellt werden. Damit wären technische Voraussetzungen geschaffen, daß Systembetreiber und andere nachvollziehen können, wer wann wohin gefahren ist. Derartige Datensammlungen wären aus datenschutzrechtlicher Sicht nicht hinnehmbar, weil das Grundrecht auf freie Entfaltung der Persönlichkeit auch das Recht umfaßt, sich möglichst

frei und unbeobachtet zu bewegen. Vor diesem Hintergrund ist es besonders wichtig, elektronische Mautsysteme datenschutzgerecht auszugestalten. Bei den anstehenden Entscheidungen sind andere Verfahren wie z. B. die Vignette einzubeziehen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt, daß der Grundsatz der datenschutzgerechten Ausgestaltung von Systemen zur automatischen Erhebung von Straßenbenutzungsgebühren von allen Beteiligten am Feldversuch auf der BAB A 555 akzeptiert wird. Zur Umsetzung dieses Grundsatzes fordern die Datenschutzbeauftragten:

- Der Grundsatz der "datenfreien Fahrt" muß auch künftig gewährleistet sein. Über Verkehrsteilnehmer, die ordnungsgemäß bezahlen, dürfen keine Daten erhoben oder verarbeitet werden, die die Herstellung eines Personenbezugs ermöglichen. Es sind ausschließlich solche Zahlungsverfahren anzuwenden, bei denen die Abrechnungsdaten nur dezentral beim Verkehrsteilnehmer gespeichert werden. Die Verkehrsteilnehmer dürfen jedoch nicht gezwungen werden, einen lückenlosen Nachweis über ihre Bewegungen zu führen.

- Die Überwachung der Gebührenzahlung darf nur stichprobenweise erfolgen. Die Möglichkeit einer flächendeckenden Kontrolle ist von vornherein technisch und rechtlich auszuschließen. Die Gebührenkontrolle ist so zu gestalten, daß die Identität des Verkehrsteilnehmers nur dann aufgedeckt wird, wenn tatsächliche Anhaltspunkte dafür bestehen, daß die Gebühren nicht entrichtet worden sind.

- Die Verfahren der Gebührenerhebung und -kontrolle müssen für die Verkehrsteilnehmer durchschaubar sein. Der Verkehrsteilnehmer muß jederzeit über sein Guthaben, die Abbuchung und den eventuellen Kontrollvorgang informiert sein.

- Alle datenschutzrelevanten Systemkomponenten sind so auszugestalten, daß sie weder vom Betreiber noch von anderer Seite beeinträchtigt oder zurückgenommen werden können.

Die hierbei anzuwendenden Verfahren wären gesetzlich abschließend vorzugeben. Dabei ist sicherzustellen, daß anfallende personenbezogene Daten von allen beteiligten Stellen vertraulich behandelt werden und einer strikten Zweckbindung unterliegen. Ferner ist zu gewährleisten, daß Betreiber derartiger Systeme - unabhängig von ihrer Rechtsform - einer Datenschutzkontrolle nach einheitlichen Kriterien unterliegen. Die Bundesregierung wird aufgefordert, bei der anstehenden internationalen Normierung elektronischer Mautsysteme die datenschutzrechtlichen Anforderungen durchzusetzen.

16.2.9 Entschließung der 49. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 9./10. März 1995 in Bremen zu Anforderungen an den Persönlichkeitsschutz im Medienbereich

Die unabhängige und unzensierte Berichterstattung durch Presse, Rundfunk und Film (Art. 5 Abs. 1 Satz 2 GG) dient der freien individuellen und öffentlichen Meinungsbildung. Das Bundesverfassungsgericht hat die freie Meinungsbildung als

Voraussetzung sowohl der Persönlichkeitsentfaltung als auch der demokratischen Ordnung bezeichnet. Insofern besteht ein enger Zusammenhang zwischen der Selbstbestimmung des Einzelnen und der Medienfreiheit.

Die rasante Entwicklung der Medientechnik, die Zunahme interaktiver Teledienste und die verstärkte kommerzielle Nutzung von Pressedatenbanken eröffnen einerseits neue Informationsmöglichkeiten für den Bürger, verschärfen aber die Gefährdungen des Rechts auf informationelle Selbstbestimmung. Diesen Gefährdungen muß der Datenschutz auf rechtlicher und technisch-organisatorischer Ebene angemessen begegnen.

Electronic Publishing und Medienarchive

Neue Formen der Verbreitung von Informationen über Netze und auf elektronischen Datenträgern führen in bisher unbekanntem Maß zu großen Informationsbeständen, in denen potentiell jedermann gezielt auf personenbezogene Daten zugreifen kann. Zudem öffnen Medienarchive, die bislang ausschließlich für journalistische Zwecke genutzt wurden, riesige Datensammlungen für medienfremde Nutzer. In Persönlichkeitsrechte wird dann besonders tief eingegriffen, wenn auch lange zurückliegende Publikationen praktisch von jedermann recherchiert werden können. Damit droht das in verschiedenen Rechtsbereichen vorgesehene "Recht auf Vergessen" wirkungslos zu werden, das z. B. durch die Löschungsvorschriften für das Bundeszentralregister gewährleistet werden soll.

Angesichts dieser Entwicklungen muß die Reichweite der datenschutzrechtlichen Sonderstellung der Medien ("Medienprivileg") neu bestimmt werden. Es ist zumindest gesetzlich klarzustellen, daß die geschäftsmäßige Verwendung personenbezogener Daten außerhalb des eigenen Medienbereichs, insbesondere durch kommerzielle Pressedatenbanken, nicht unter das "Medienprivileg" fällt.

Interaktive Dienste und Mediennutzungsprofile

Auch beim Ausbau neuer digitaler Kommunikationsformen (interaktive Dienste wie z. B. Video on Demand) müssen die Persönlichkeitsrechte der Nutzer gewahrt werden. Dabei ist stärker als bisher von vornherein Wert darauf zu legen, daß datenschutzfreundliche Techniken entwickelt werden und zum Einsatz kommen, bei denen personenbezogene Verbindungs und Nutzungsdaten erst gar nicht entstehen. Von besonderer Bedeutung sind hier anonyme Zahlverfahren, z. B. Prepaid-Karten, auf denen Informationen über die Nutzung ausschließlich dezentral gespeichert werden.

Entsprechend den Bestimmungen im Bildschirmtextstaatsvertrag und in den neueren Mediengesetzen ist sicherzustellen, daß sich die Erhebung und die Aufzeichnung von Verbindungs- und Abrechnungsdaten auf das erforderliche Maß beschränken. Dieser strikte Verarbeitungsrahmen darf auch nicht dadurch ausgeweitet werden, daß die Nutzung eines Dienstes von der Einwilligung in eine zweckfremde Verwendung der Daten abhängig gemacht wird. Die Länder sollten entsprechende einheitliche Regelungen für alle interaktiven Dienste treffen. Da es sich bei den angesprochenen Diensten um Bestandteile einer entstehenden globalen Informationsinfrastruktur handelt, wird die Bundesregierung aufgefordert, sich auf internationaler Ebene für entsprechende Regelungen einzusetzen.

Rechte der Betroffenen gegenüber den Medien

Während die von der Berichterstattung Betroffenen - neben dem für alle Bereiche geltenden Gegendarstellungsrecht - gegenüber den öffentlich-rechtlichen und privaten Rundfunkveranstaltern inzwischen weitere elementare Datenschutzrechte besitzen, gibt es gegenüber der Presse keine vergleichbaren Regelungen.

So kann derjenige, der durch die Berichterstattung der Rundfunkveranstalter in seinem Persönlichkeitsrecht beeinträchtigt wird, in den meisten Fällen nach der Publikation Auskunft über die der Berichterstattung zugrundeliegenden, zu seiner Person gespeicherten Daten verlangen. Gegenüber der Presse hat er kein entsprechendes Auskunftsrecht. Die meisten Rundfunkveranstalter sind - anders als die Presse - zudem verpflichtet, etwaige Gegendarstellungen zu den gespeicherten Daten zu nehmen, auf die sie sich beziehen (Mitspeicherungspflicht). Ein sachlicher Grund für diese Unterscheidungen ist nicht erkennbar.

Das Presserecht sollte insofern der Rechtslage nach dem Rundfunkrecht (z. B. § 41 Abs. 3 BDSG und Art. 17 Abs. 2 ZDF-Staatsvertrag) angeglichen werden.

Gegenüber Pressedatenbanken, die nicht nur dem eigenen internen Gebrauch dienen, sollte der Betroffene darüber hinaus ein Auskunftsrecht bezüglich des zu seiner Person gespeicherten veröffentlichen Materials haben.

Öffentlichkeitsarbeit der Behörden

Personenbezogene Veröffentlichungen von Behörden können das Recht auf informationelle Selbstbestimmung erheblich beeinträchtigen. Das gilt für die Personen, auf die die Aktivitäten der Behörde unmittelbar gerichtet sind, wie auch für andere Verfahrensbeteiligte (wie z. B. Einwender, Opfer von Straftaten, Zeugen) und im besonderen Maße für unbeteiligte Personen aus dem sozialen Umfeld des Betroffenen. Deshalb ist bei der Weitergabe von Daten aus Strafermittlungsverfahren an die Medien besonders zurückhaltend zu verfahren.

Für den Umfang des Anspruchs der Medien auf Weitergabe personenbezogener Daten in Form von Presseerklärungen und Auskünften gibt es keine konkreten gesetzlichen Festlegungen. Die Datenschutzbeauftragten des Bundes und der Länder halten es daher für geboten, daß der Gesetzgeber Kriterien für die Abwägung zwischen dem Persönlichkeitsrecht des Betroffenen und der Freiheit der Berichterstattung durch Rundfunk und Presse deutlicher als bisher festlegt. Dafür kommen die Vorschriften des Landespresserechts, in besonders sensiblen Bereichen aber auch spezialgesetzliche Regelungen wie etwa die Strafprozeßordnung in Betracht.

Gerichtsfernsehen

Die Datenschutzbeauftragten des Bundes und der Länder treten den in jüngster Zeit zunehmend erhobenen Forderungen nach einer Aufhebung des Verbots der Hörfunk- und Fernsehberichterstattung aus Gerichtsverhandlungen entgegen. Insbesondere bei

Strafprozessen vor laufenden Mikrofonen und Kameras würde es unweigerlich zu einer gravierenden Beeinträchtigung des Persönlichkeitsrechts der Angeklagten, der Opfer, der Zeugen und ihrer Angehörigen kommen. Selbst mit Einwilligung aller Prozeßbeteiligten darf die Hörfunk- und Fernsehberichterstattung nicht zugelassen werden.

Die Gerichtsverhandlung darf nicht zu einem massenmedial vermittelten "modernen Pranger" werden.

16.2.10 Entschließung der 49. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 9./10. März 1995 in Bremen zum Sozialgesetzbuch VII

Verfassungsgemäßer Datenschutz für Unfallversicherte erforderlich

Durch die Träger der gesetzlichen Unfallversicherung werden oft Daten der Versicherten hinter deren Rücken oder zumindest ohne deren konkrete Kenntnis erhoben und weitergegeben. Der vorliegende Referentenentwurf des Bundesministeriums für Arbeit und Sozialordnung zum Unfallversicherungs-Einordnungsgesetz - SGB-VII sieht dazu keine Änderungen vor.

Aus dem Recht auf informationelle Selbstbestimmung der Versicherten, insbesondere auf Transparenz der einzelnen Verfahrensschritte, ergeben sich mehrere grundlegende Forderungen, die bei einer Überarbeitung des Referentenentwurfes berücksichtigt werden müssen:

l. Auskunftspflicht behandelnder Ärzte gegenüber Unfallversicherungsträgern

Für behandelnde Ärzte sollte eine gesetzliche Auskunftspflicht gegenüber Unfallversicherungsträgern nur festgelegt werden, soweit dies erforderlich ist für eine sachgerechte und schnelle Heilung (§ 557 Abs. 2 RVO - § 34 Referentenentwurf SGB VII). Die gesetzliche Auskunftspflicht ist daher auf Angaben über die Behandlung und den Zustand des Verletzten zu beschränken. Danach dürfen Vorerkrankungen, die aus Sicht des Arztes mit dem aktuellen Status in keinem Zusammenhang stehen oder keine Bedeutung im Zusammenhang mit dem Arbeitsunfall oder der Berufskrankheit haben, nicht übermittelt werden (Beispiel: Handverletzung und Salmonellenvergiftung).

2. Datenerhebung, -verarbeitung und -nutzung durch Durchgangsärzte und Berufskrankheitenärzte

Soweit von den Unfallversicherungsträgern bestellte Durchgangsärzte personenbezogene Daten über den Unfallverletzten erheben und Unfallversicherungsträgern und anderen Stellen mitteilen, muß dies auf eine normenklare gesetzliche Grundlage gestellt werden; die bisherige Regelung in dem zwischen den Verbänden der Kassenärzte und der Unfallversicherungsträger geschlossenen "Ärzteabkommen" reicht für die damit verbundenen Eingriffe in das informationelle Selbstbestimmungsrecht der Betroffenen nicht aus. Entsprechendes gilt für die geplante Einführung eines Berufskrankheitenarztes.

3. Mitteilung personenbezogener Patientendaten durch Unfallversicherungsträger an ärztliche Gutachter

Im Hinblick auf das Recht der Betroffenen, der Bestellung eines bestimmten Gutachters im Einzelfall aus wichtigem Grund - z. B. wegen möglicher Befangenheit - zu widersprechen, haben die Betroffenen ein besonderes berechtigtes Interesse an der Transparenz dieser Datenübermittlungen.

Gesetzlich festzulegen ist daher, daß dem Betroffenen vor Übermittlung seiner Daten an einen Gutachter der Zweck des Gutachtens und die Person des Gutachters unter Hinweis auf sein Widerspruchsrecht nach § 76 Abs. 2 SGB X mitzuteilen sind.

4. Eingriffe der Unverfallversicherungsträger und ihrer Verbände in das Recht auf informationelle Selbstbestimmung

Aufgaben der Unfallversicherungsträger und ihrer Verbände und ihre Befugnisse zur Datenerhebung, -verarbeitung und -nutzung - einschließlich der Aufbewahrungsfristen - sind differenziert in der verfassungsrechtlich gebotenen Klarheit gesetzlich zu regeln. Der vorliegende Referentenentwurf erscheint in diesem Punkt weitgehend unzureichend. So werden undifferenziert Unfallversicherungsträger und ihre Verbände behandelt, die Fachaufgaben dieser Stellen nicht oder nicht hinreichend deutlich genannt und andererseits Selbstverständlichkeiten wie das Führen von Dateien über erforderliche Daten aufgeführt. Außerdem beschränkt sich die Regelung auf die Datenverarbeitung in Dateien und übergeht die gerade im Bereich der Berufsgenossenschaften mit Gutachten und ähnlichen Unterlagen stark ausgeprägte Datenverarbeitung in Akten.

Die Zuweisung von Aufgaben und Befugnissen an Verbände der gesetzlichen Unfallversicherung muß zudem wie bei allen anderen Verbänden von Leistungsträgern durch die Einrichtung einer staatlichen Aufsicht ergänzt werden.

Soweit Vorschriften der Unfallversicherungsträger und ihrer Verbände (z. B. Unfallverhütungsvorschriften) durch Regelungen über die Erhebung, Verarbeitung und Nutzung sensibler medizinischer Daten in das Recht auf informationelle Selbstbestimmung eingreifen, sind diese Eingriffe gesetzlich zu regeln.

5. Anzeige eines Berufsunfalls und einer Berufskrankheit

Bei Datenschutzkontrollen der bisherigen Anzeigen von Berufsunfällen und -krankheiten hat sich gezeigt, daß der Umfang der an die verschiedenen Stellen übermittelten Daten zum Teil dem Grundsatz der Verhältnismäßigkeit, insbesondere der Erforderlichkeit nicht Rechnung trägt. Der Inhalt dieser Anzeigen muß an diesen Grundsätzen gemessen neu festgelegt werden

6. Zentraldateien mehrerer Unfallversicherungsträger oder ihrer Verbände

Zweck und Inhalt zentral geführter Dateien sind in angemessenem Umfang gesetzlich präzise zu regeln. Dasselbe gilt für die Datenverarbeitung und -nutzung sowie die Festlegung der jeweils speichernden Stelle.

Die rechtzeitige Beteiligung des jeweils zuständigen Bundes- oder Landesbeauftragten für den Datenschutz vor Einrichtung einer Zentraldatei ist vorzusehen.

7. Anforderung medizinischer Unterlagen bei anderen Sozialleistungsträgern

Der in § 76 Abs. 2 SGB X vorgesehene Hinweis auf das Widerspruchsrecht gegen die Übermittlung medizinischer Daten geht stets dann ins Leere, wenn bei der speichernden bzw. übermittelnden Stelle keine Verwaltungsverfahren läuft.

Es ist daher festzulegen, daß ein Unfallversicherungsträger vor der Anforderung von Sozialdaten im Sinne des § 76 SGB X bei anderen Sozialleistungsträgern den Versicherten auf dessen Widerspruchsrecht nach § 76 Abs. 2 SGB X gegenüber der übermittelnden Stelle hinzuweisen hat.

8. Akteneinsichtsrecht der Versicherten

Hinsichtlich des gesetzlichen Akteneinsichtsrechts nach § 25 SGB X treten in der Praxis seitens der Unfallversicherungsträger Unsicherheiten auf, ob zum Schutz von Betriebs- und Geschäftsgeheimnissen oder Urheberrechten das Einsichtsrecht beschränkt werden muß. Hierzu ist eine gesetzliche Klarstellung geboten, daß diese Rechte dem Akteneinsichtsrecht nicht entgegenstehen.

16.2.11 Entschließung der 49. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 9./10. März 1995 in Bremen zum eingeschränkten Zugriff auf Versichertendaten bei landesweiten oder überregionalen gesetzlichen Krankenkassen

Die gesetzlichen Krankenkassen schließen sich zunehmend zu landesweiten oder überregionalen gesetzliche Krankenkassen zusammen. Es stellt sich daher verstärkt die Frage, welche bzw. wiewiele Geschäftsstellen solcher Krankenkassen umfassend auf alle gespeicherten Daten eines Versicherten zugreifen können.

Die Datenschutzbeauftragten halten nur folgendes für vertretbar:

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

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

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

16.2.12 Entschließung der 49. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 9./10. März 1995 in Bremen zum Maßhalten beim vorbeugenden personellen Sabotageschutz

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert, bei Sicherheitsüberprüfungen zum personellen Sabotageschutz Augenmaß zu bewahren. Bei diesen Sicherheitsüberprüfungen werden sensible Daten, z. B. über politische Anschauungen oder Alkoholkonsum, vorbeugend erhoben, also ohne daß der Betroffene dazu Anlaß geboten hätte. Polizei und Verfassungsschutz sind routinemäßig beteiligt. Schon wenn der Betroffene im Verlauf der Überprüfung auch nur in den Verdacht der Unzuverlässigkeit gerät, kann dies bereits erheblichen Einfluß zumindest auf das berufliche Fortkommen nehmen.

Gegenwärtig sind solche Überprüfungen spezialgesetzlich für den Atombereich und für Flughäfen vorgesehen. Das Bundesministerium des Innern will jetzt klären, inwieweit Beschäftigte in anderen Einrichtungen überprüft werden sollen.

Unstreitig können solche Überprüfungen unbescholtener Bürger nur zum Schutz von "lebens- und verteidigungswichtigen Einrichtungen" angemessen sein und nur Personen betreffen, die dort an "sicherheitsempfindlichen Stellen" tätig sind. Als "lebenswichtig" sehen die Innenminister und -senatoren aber bereits Stellen an, "die für das Funktionieren des Gemeinwesens unverzichtbar sind". Damit könnten Beschäftigte in weiten Bereichen des öffentlichen Dienstes und der Wirtschaft mit Sicherheitsüberprüfungen überzogen werden.

Die Datenschutzbeauftragten meinen, daß das Persönlichkeitsrecht hier größere Zurückhaltung gebietet. Die Sicherheitsüberprüfungen müssen auf Bereiche beschränkt bleiben, in denen einer erheblichen Bedrohung für das Leben zahlreicher Menschen vorgebeugt werden muß.

Soweit in solchen Bereichen Sicherheitsüberprüfungen durchgeführt werden sollen, bedarf es einer ebenso klaren gesetzlichen Grundlage, wie bisher im Atomgesetz und im Luftverkehrsgesetz. Die zu schützenden Arten lebens- und verteidigungswichtiger Einrichtungen müssen durch Rechtsvorschrift abschließend festgelegt sein. Dabei sind für die jeweiligen Bereiche angemessene Regelungen zu treffen, die mit Rücksicht auf die Interessen Betroffener folgende allgemeine Grundsätze beachten:

- möglichst klare Vorgaben zur "Sicherheitsempfindlichkeit" in der Vorschrift und exakte Festlegung dieser Stellen durch die zuständige Behörde nach Anhörung der Personalvertretung der einzelnen Einrichtung,

- Zustimmung des Betroffenen als Verfahrensvoraussetzung,

- abschließender Katalog der regelmäßig durchzuführenden Maßnahmen, dabei Beschränkung auf vorhandene Erkenntnisse, keine Ausforschungsermittlungen,

- strenge Zweckbindung und angemessene organisatorische Vorkehrungen zu deren Gewährleistung, insbesondere Trennung von Personalakte,

- eigene Verfahrensrechte des Betroffenen, insbesondere rechtliches Gehör vor ablehnender Entscheidung und aktenkundige Gegendarstellung,

- angemessener Auskunftsanspruch, einschließlich Akteneinsicht,

- effektive Datenschutzkontrolle, auch zur Datenverarbeitung in Akten bei nichtöffentlichen Stellen.

Im Regelfall muß zusätzlich gelten:

- Überprüfung durch die zuständige Aufsichtsbehörde selbst, nicht durch Verfassungsschutzbehörden,

- keine Einbeziehung weiterer Personen (wie Ehegatten usw.).

Ausnahmetatbestände wären - auch zum Verfahren - präzise zu fassen.

Die Praxis der Sicherheitsüberprüfungen zum personellen Sabotageschutz steht in Bund und Ländern vor einer wichtigen Weichenstellung. Sie muß klar und angemessen sein.

16.2.13 Entschließung der 49. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 9./10. März 1995 in Bremen zu Aufbewahrungsbestimmungen und Dateiregelungen im Justizbereich

Bisher ist der Gesetzgeber im Bereich der Justiz den verfassungsrechtlichen Forderungen nach ausreichenden normenklaren Regelungen über die Aufbewahrung von Akten und die Speicherung personenbezogener Daten in Dateien nicht nachgekommen. So enthalten z. B. die bislang bekannt gewordenen Entwürfe zu einem Strafverfahrensänderungsgesetz nur unzureichende Generalklauseln. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder[2] erklärt deshalb:

1. Aufbewahrung, Aussonderung und Vernichtung der Akten und die Speicherung personenbezogener Daten in Dateien im Bereich der Justiz müssen nach den Grundsätzen des Bundesverfassungsgerichts im Volkszählungsurteil für die Gerichte, Staatsanwaltschaften und Strafvollzugsbehörden gesetzlich geregelt werden, wobei sich die Aufbewahrungsdauer am Recht auf informationelle Selbstbestimmung und am Zweck der Speicherung zu orientieren hat.

   Hierbei hat der Gesetzgeber die grundlegenden Entscheidungen zur Aufbewahrungsdauer selbst zu treffen. Aufgrund einer hinreichend konkreten Verordnungsermächtigung können die Einzelheiten durch Rechtsverordnung bestimmt werden.

[2] Bei Stimmenthaltung von Hamburg.

2. Die derzeit bestehenden Aufbewahrungsfristen sind konsequent zu vereinfachen und zu verkürzen. Soweit geboten sind Verkürzungen vorzunehmen.

3. Die derzeit geltende generelle 30-jährige Aufbewahrungsfrist für Strafurteile und Strafbefehle mit der Folge der umfassenden Verfügbarkeit der darin enthaltenen Informationen ist nicht angemessen. Bei der Bemessung der Aufbewahrungsfrist von Strafurteilen und Strafbefehlen sowie für die Bestimmung des Zeitpunkts der Einschränkung der Verfügbarkeit ist vielmehr nach Art und Maß der verhängten Sanktionen zu differenzieren.

   Bei der Festlegung des Beginns der Aufbewahrungsfrist sollte - abweichend von der bisherigen Praxis, nach der es auf die Weglegung der Akte ankommt - regelmäßig auf den Zeitpunkt des Eintritts der Rechtskraft der ergangenen gerichtlichen Entscheidung abgestellt werden.

   Ergeht keine rechtskraftfähige Entscheidung, so sollte die Aufbewahrungsfrist mit dem Erlaß der Abschlußverfügung beginnen.

4. Wird der Akteninhalt auf Bild- oder Datenträgern, die an die Stelle der Urschrift treten, aufbewahrt, so sind gleichwohl unterschiedliche Löschungsfristen für einzelne Aktenteile zu beachten. Aus datenschutzrechtlicher Sicht sind Datenträger zu wählen, die eine differenzierte Löschung gewährleisten. Ist bei Altbeständen eine teilweise Aussonderung technisch nicht möglich oder nur mit unverhältnismäßigem Aufwand zu bewerkstelligen, so hat eine Sperrung der an sich auszusondernden Teile zu erfolgen.

5. Sind in einer Akte Daten mehrerer beteiligter Personen gespeichert, so ist eine Sperre hinsichtlich solcher Aktenteile, die einzelne beteiligte Personen betreffen, vorzusehen, wenn diese Aktenteile eigentlich ausgesondert werden müßten, aus praktischen Gründen aber keine Vernichtung erfolgen kann.

6. Bei Freisprüchen und Einstellungen des Verfahrens wegen Wegfalls des Tatverdachts ist dafür Sorge zu tragen, daß ein Zugriff auf die automatisiert gespeicherten Daten nur noch zu Zwecken der Aktenverwaltung erfolgen kann.

7. Für die Daten von Nebenbeteiligten (z. B. Anzeigeerstatter, Geschädigte) ist eine vorzeitige Löschung vorzusehen. Hinsichtlich der Hauptbeteiligten sollte eine Teillöschung der Personen- und Verfahrensdaten stattfinden, sobald die vollständigen Daten zur Durchführung des Verfahrens nicht mehr erforderlich sind.

8. Soweit Daten verschiedener Gerichtszweige oder verschiedener speichernder Stellen in gemeinsamen Systemen verarbeitet werden, ist durch rechtliche, technische und organisatorische Maßnahmen sicherzustellen, daß die Zweckbindung der gespeicherten Daten beachtet wird.

16.2.14 Entschließung der 49. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 9./10. März 1995 in Bremen zum Datenschutz bei Wahlen

Bei der Durchführung von Wahlen haben sich Probleme bei der Verarbeitung personenbezogener Daten ergeben. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat hierzu die folgende Entschließung[1] gefaßt:

1. Durchführung von Wahlstatistiken

Diejenigen Wahlberechtigten, in deren Wahlbezirk eine repräsentative Wahlstatistik durchgeführt werden soll, sind bereits mit der Wahlbenachrichtigung hierüber zu informieren. In allgemeiner Form ist auch im Wahllokal ein gut sichtbarer Hinweis auf die Einbeziehung in die Wahlstatistik anzubringen.

Die Statistik sollte nur in solchen Wahlbezirken durchgeführt werden, in denen jede Geschlechts- und Altersgruppe wenigstens so viele Wahlberechtigte aufweist, daß das Wahlgeheimnis mit Sicherheit gewahrt bleibt. Das Kriterium ist vom Landeswahlleiter vor der Festlegung der Auswahlbezirke zu prüfen. Gegebenenfalls sind ungeeignete Wahlbezirke auszutauschen.

Die Auszählung der Wahlberechtigten und der Wahlbeteiligung auf der Grundlage der Wählerverzeichnisse sollte durch den Wahlvorstand erfolgen, während die statistische Auszählung der Stimmzettel durch die jeweils für die Durchführung der Statistik zuständige Stelle vorzunehmen ist.

Untersuchungen, bei denen Angaben über die Wahlbeteiligung oder die Stimmabgabe aus verschiedenen Wahlen einzelfall- und personenbezogen zusammengeführt werden, gefährden das Wahlgeheimnis und sind daher unzulässig..

2. Auslegung von Wählerverzeichnissen

Durch die Einsicht in das Wählerverzeichnis besteht nach der jetzigen Rechtslage die Gefahr, daß Daten sowohl von Bürgern, über die in Melderegistern eine Auskunftssperre eingetragen ist, als auch von Bürgern, die in einer speziellen sozialen Situation leben (z. B. Justizvollzugsanstalten, Frauenhäuser, psychiatrische Kliniken, Obdachlose), offenbart werden.

Um einerseits die Kontrollmöglichkeit durch die Öffentlichkeit im Vorfeld einer Wahl weiterhin zu gewährleisten, andererseits die datenschutzrechtlichen Belange der genannten Betroffenen zu wahren und dem Mißbrauch einer Adreßrecherche vorzubeugen, fordern die Datenschutzbeauftragten des Bundes und der Länder, daß bei allen Wahlen

- entweder in den öffentlich ausliegenden Wählerverzeichnissen, nur Name, Vorname und Geburtsdatum der Wahlberechtigten aufgeführt werden.

[1] Bei Gegenstimme vom Baden-Württemberg zu Nr. 4.

- oder aber bei Wiedergabe der Adressen im Wählerverzeichnis nur Auskünfte zu bestimmten Personen an den Auskunftssuchenden erteilt werden, wenn er vorher die Adresse dieser Personen aufgegeben hat.

Im übrigen sind Daten von Bürgern, für die in Melderegistern eine Auskunftssperre eingetragen ist, im Wählerverzeichnis nicht zu veröffentlichen.

3. Gewinnung von Wahlhelfern

Bei der Gewinnung von Wahlhelfern sind folgende Grundsätze zu beachten:

Es dürfen nur die zur Bestellung erforderlichen Daten, wie Name, Vorname und Wohnanschrift, erhoben werden. Die Betroffenen sind über den Zweck der Datenerhebung und die weitere Datenverarbeitung umfassend zu unterrichten.

Über die Abwicklung der jeweiligen Wahl hinaus dürfen die Daten der Wahlhelfer, soweit sie nicht ausdrücklich widersprochen haben, in einer Wahlhelferdatei nur gespeichert werden, wenn sie dieser Speicherung nicht widersprochen haben. Die Wahlhelfer sind auf ihr Widerspruchsrecht hinzuweisen.

Beschäftigtendaten dürfen nur auf freiwilliger Basis übermittelt werden, sofern nicht eine besondere Rechtsvorschrift die Übermittlung zuläßt. Im Falle der Freiwilligkeit muß es den Beschäftigten möglich sein, selbst die Meldung unmittelbar gegenüber der Wahlbehörde abzugeben. Nach Gründen, die einer Übernahme des Ehrenamtes entgegenstehen, darf erst im förmlichen Verfahren durch die Wahlbehörde gefragt werden.

4. Erteilung von Wahlscheinen

Die in den Wahlordnungen des Bundes und der Länder enthaltene Regelung, nach der die Antragstellung für die Erteilung eines Wahlscheines auf einem Vordruck zu begründen ist und der Grund gegenüber der Gemeinde glaubhaft gemacht werden muß, ist aus datenschutzrechtlicher Sicht unverhältnismäßig. Da sich aus der geforderten Differenzierung der Begründung keine unterschiedlichen Rechtsfolgen ableiten, ist diese entbehrlich. Es genügt in der Antragstellung eine Erklärung des Wahlberechtigten, daß er am Tag der Wahl aus wichtigem Grund das für ihn zuständige Wahllokal nicht aufsuchen kann.

16.2.15 Entschließung der 49. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 9./10. März 1995 in Bremen zur ASYL-Card

Überlegungen einer "Bund-Länder-Arbeitsgruppe zur Harmonisierung der Verwaltungsabläufe im Asylverfahren" sehen die Einführung einer sogenannten ASYL-Card vor, zu deren Benutzung jeder Asylbewerber verpflichtet werden soll. Auf der Chipkarte sollen neben Fingerabdruck und Lichtbild unter anderem Daten über das Asylverfahren, das Vorliegen einer Arbeitserlaubnis und den Empfang von Sach- und Geldleistungen erfaßt sein. Die Karte soll sowohl Verfahrensdaten für die zuständigen Behörden schnell verfügbar machen (z. B. Asylverfahren, Arbeitserlaubnis) als auch Kontrollzwecken dienen (z. B. Aufenthaltskontrolle, Zutrittskontrolle und anderes) und die Abwicklung fürsorglicher Leistungen unterstützen.

Die Zusammenführung von Daten aus dem Arbeitsbereich verschiedener Stellen auf einer Chipkarte stellt einen erheblichen Eingriff in das informationelle Selbstbestimmungsrecht dar, das auch für Asylbewerber gilt. Die Datenschutzbeauftragten halten einen solchen Eingriff nicht für vertretbar, zumal die Überlegungen zur ASYL-Card durch Mängel im Vollzug des bisherigen Verfahrens ausgelöst werden. Die Datenschutzbeauftragten sind der Ansicht, daß diese Defizite behoben werden sollten, anstatt ein neues datenschutzrechtlich problematisches Verfahren einzuführen.

Die Datenschutzbeauftragten weisen aus diesem Anlaß auf die allgemeine Gefährlichkeit einer Entwicklung zur multifunktionellen Datenspeicherung auf Chipkarten für Überwachungszwecke hin. Effektivitätsgesichtspunkte, Mißbrauchsbekämpfung, Überwachung auferlegter Pflichten und ähnliches könnten auch für andere Verwaltungsverfahren geltend gemacht werden. Je mehr Bereiche mit Kartenlösungen versehen werden, umso mehr wächst das Bedürfnis, aus praktischen Erwägungen heraus eine Vereinheitlichung oder Zusammenführung der Informationen auf einer Karte anzustreben. Damit wächst die Gefahr der "Rundumerfassung", die mit dem verfassungsrechtlichen Gebot der Verhältnismäßigkeit nicht vereinbar wäre.

Die Einführung der "ASYL-Card" bedürfte im übrigen eines erheblichen technischen und finanziellen Aufwands. Kryptographische Verfahren, Hard- und Software für die mit der ASYL-Card arbeitenden Stellen und Personal- und Arbeitseinsatz für die Herstellung, Verteilung und Verwaltung der Karten würden einen Aufwand erfordern, der zu den von der Arbeitsgruppe erwarteten Vorteilen außer Verhältnis stehen dürfte.

16.2.16 Entschließung der 49. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 9./10. März 1995 in Bremen zur Rechtstatsachensammlung zur Überprüfung polizeilicher Befugnisse

Die Datenschutzbeauftragten des Bundes und der Länder hatten in ihrer 48. Konferenz am 26./27. September 1994 Vorschläge zur Überprüfung der Erforderlichkeit polizeilicher Befugnisse und deren Auswirkungen für die Rechte der Betroffenen erarbeitet.
Ziel dieser Vorschläge war es, die Diskussion über die Erforderlichkeit der bestehenden Instrumente zur polizeilichen Datenverarbeitung und deren Ausweitung auf Erkenntnisse zu stützen, die stärker als bisher gesichert sind.

Auch von seiten der Polizei, insbesondere des Bundeskriminalamtes, sind Vorschläge für eine umfassende Rechtstatsachensammlung über die Anzahl besonderer Erhebungsmethoden, den Erfolg dieser Maßnahmen und Durchführungsschwierigkeiten unterbreitet worden. Sie sind jedoch bisher von der Mehrzahl der Länderpolizeien abgelehnt worden.
Stattdessen soll eine Bund/Länder-Fallsammlung eingerichtet werden. Hierzu stellen die Datenschutzbeauftragten des Bundes und der Länder fest:
Die Einrichtung einer Rechtstatsachensammlung als objektives Instrument zur Bewertung polizeilicher Eingriffsbefugnisse wäre auch aus datenschutzrechtlicher Sicht zu begrüßen. Diese Sammlung darf jedoch nicht einseitig das Ziel verfolgen, Forderungen der Polizei zur Einführung zusätzlicher Befugnisse argumentativ zu unterstützen. Das Vorhaben geht in die falsche Richtung, wenn es von vornherein aufgrund des angelieferten Datenmaterials auf bestimmte Ergebnisse festgelegt ist. Vielmehr muß die Sammlung ohne rechtspolitische Vorgaben angelegt werden. Sie soll eine objektive Beurteilung des Einsatzes und der Ergebnisse besonderer Methoden zur Datenerhebung ermöglichen.

Das Bundesverfassungsgericht hat im Volkszählungsurteil gefordert, daß der Gesetzgeber "ungewissen Auswirkungen eines Gesetzes dadurch Rechnung tragen muß, daß er die ihm zugänglichen Erkenntnisquellen ausschöpft, um die Auswirkungen so zuverlässig wie möglich abschätzen zu können; bei einer sich später zeigenden Fehlprognose ist er zur Korrektur verpflichtet. Der Gesetzgeber kann aufgrund veränderter Umstände zur Nachbesserung einer ursprünglich verfassungsgemäßen Regelung gehalten sein."
Die Datenschutzbeauftragten halten daher ihren Vorschlag einer ergebnisoffenen Überprüfung der bestehenden Befugnisse aufrecht. Sie erwarten, daß sich die Polizeien der Diskussion über die Erforderlichkeit und Angemessenheit weitreichender Befugnisse zu Eingriffen in das Persönlichkeitsrecht nicht entziehen werden. In Betracht kommt auch eine unabhängige Überprüfung der bestehenden polizeilichen Eingriffsbefugnisse durch das kriminalistische Institut beim BKA in enger Kooperation mit einem fachlich qualifizierten unabhängigen Forschungsinstitut.
Die Datenschutzbeauftragten des Bundes und der Länder fordern die Innenministerkonferenz auf, die Überlegungen für eine offene und aussagekräftige Rechtstatsachensammlung weiterzuverfolgen und die Datenschutzbeauftragten zu beteiligen.

16.2.17 Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, vom 25. August 1994, zum Vorschlag der Kommission der Europäischen Union für eine Verordnung (EG) des Rates über die Tätigkeit der Gemeinschaft im Bereich der Statistik - EG-Statistikverordnung - (KOM(94) 78 endg.; Ratsdok. 5615/94 = BR-Drs. 283/94)

Die Datenschutzbeauftragten des Bundes und der Länder begrüßen, daß die Europäische Union eine allgemeine Regelung für die Gemeinschaftsstatistik trifft, weisen allerdings daraufhin, daß die datenschutzrechtliche Entwicklung bei der Europäischen Union mit dem Aufbau der europäischen Statistik keineswegs Schritt gehalten hat.

Sie stellen mit Besorgnis fest, daß der vorliegende Vorschlag einer EG-Statistikverordnung die nationalen datenschutzrechtlichen Grundsätze und wesentlichen Standards des Statistikrechts weitgehend nicht berücksichtigt. Sie fordern daher zur Wahrung des Rechts der Betroffenen auf informationelle Selbstbestimmung mit Nachdruck, daß die Bundesregierung ihre Bedenken gegen diesen Vorschlag geltend macht und diese bei den Beratungen auf europäischer Ebene zum Tragen bringt.

Die Datenschutzbeauftragten des Bundes und der Länder unterstützen ausdrücklich den Beschluß des Deutschen Bundesrates vom 8. Juli 1994 (BR-Drs. 283/94 - Beschluß -).

Gegen den vorgelegten Vorschlag einer *Verordnung (EG) des Rates über die Tätigkeit der Gemeinschaft im Bereich der Statistik* (EG-Statistikverordnung) erheben sie insbesondere die folgenden datenschutzrechtlichen Bedenken.

1. In Art. 1 sollte als die zuständige Gemeinschaftsdienststelle unmißverständlich das Statistische Amt der Europäischen Gemeinschaft (EUROSTAT) bestimmt werden, weil die erforderlichen rechtlichen, administrativen, technischen und organisatorischen Maßnahmen - insbesondere zur Sicherung der Zweckbindung der zu statistischen Zwecken erhobenen Daten sowie zur Wahrung der statistischen Geheimhaltung - bei dieser Stelle bereits aufgrund der EG-Übermittlungsverordnung 1588/90 vom 11. Juni 1990 getroffen werden können. Eine jederzeit revidierbare Organisationsentscheidung der Kommission darüber, welche Dienststelle der Europäischen Union für statistische Aufgaben zuständig ist, birgt dagegen die Gefahr, daß Daten an unterschiedliche Stellen der Kommission zu unterschiedlichen Zwecken übermittelt werden.

   Zugleich sollte EUROSTAT zumindest einen der Selbständigkeit der Statistischen Ämter in der Bundesrepublik Deutschland vergleichbaren organisationsrechtlichen Status erhalten, der die unter dem Gesichtspunkt der Objektivität und Neutralität gebotenen Eigenständigkeit bei der Aufgabenerfüllung garantiert. Dies könnte anläßlich der für 1996 vorgesehenen Revision des Vertrages über die Europäische Union geschehen.

2. Das mehrjährige statistische Programm sollte nicht wie in Art. 3 vorgesehen von der Kommission beschlossen werden. Die grundlegenden Entscheidungen über die Bürger belastende Datenerhebungen sollten dem Rat mit Zustimmung des Europäischen Parlaments vorbehalten bleiben. Dabei sollte der Planungscharakter des Programms in den Vordergrund gestellt werden.

3. Art. 5 sollte festlegen, daß statistische Einzelmaßnahmen durch einen Rechtsakt gemäß dem Verfahren nach Art. 189 b EG-Vertrag angeordnet werden. Dies gilt auch für die statistischen Auswertungen von Daten, die bei den administrativen Stellen bereits vorliegen (sog. Sekundärstatistik). Die im Vorschlag vorgesehene generelle Befugnis der Kommission, statistische Einzelmaßnahmen zu regeln, ist viel zu weitgehend.

4. Die in Art. 12 vorgesehene Übertragung der Befugnis zur Organisation der Verbreitung der statistischen Daten auf die Kommission widerspricht dem Grundsatz der Subsidiarität nach Art. 3 b EG-Vertrag, auf dem folgt, daß grundsätzlich die Mitgliedstaaten nach ihrem nationalen Recht zur Verbreitung der statistischen Daten zuständig sind. Ferner sollte in Art. 12 festgelegt werden, daß an Stellen außerhalb der statistischen Gemeinschaftsdienststelle nur nicht-vertrauliche statistische Daten übermittelt werden dürfen.

5. Der in Art. 13 gegenüber der Definition in der EG-Übermittlungsverordnung 1588/90 neu definierte Begriff "statistische Geheimhaltung" muß präzisiert werden. Dazu gehört insbesondere, daß festgelegt wird, unter welchen Voraussetzungen statistische Daten vertraulich sind und nicht nur als vertraulich gelten. Dies gilt um so mehr , als im Verordnungsvorschlag dieser Begriff nicht nur in Art. 13, sondern auch in Art. 9 Abs. 2 - allerdings mit einem anderen Begriffsinhalt - definiert wird. Der Begriff "statistische Geheimhaltung" sollte an einer Stelle in der Verordnung und so definiert werden, daß er Art. 2 Nr. 1 der EG-Übermittlungsverordnung 1588/90 und damit den derzeit geltenden nationalen Begriffsbestimmungen entspricht. Dies stände auch im Einklang mit dem Grundsatz der Subsidiarität nach Art. 3 b EG-Vertrag.

6. Gemäß dem Grundsatz der Subsidiarität sollte - ebenso wie die Befugnis zur Verbreitung statistischer Ergebnisse (Art. 11 Abs. 1) - auch die Festlegung der Zuständigkeit für die Durchführung der statistischen Einzelmaßnahmen (Art. 7) den Mitgliederstaaten überlassen bleiben.

7. Auch die in Art. 16 vorgesehene generelle Zugangsregelung einzelstaatlicher Stellen und der Gemeinschaftsdienststelle zu Registern der Verwaltung widerspricht dem Grundsatz der Subsidiarität nach Art. 3 b EG-Vertrag. Dieser gebietet hier, daß - jedenfalls grundsätzlich - die Mitgliedsstaaten zu bestimmen haben, in welcher Weise sich die für die Erstellung der Gemeinschaftsstatistiken zuständigen nationalen Stellen Daten beschaffen. Damit ist aber nicht zu vereinbaren, daß auch Stellen der Kommission unmittelbar Zugang zu nationalen Verwaltungsregistern haben sollen.

   Ferner bleibt unklar, ob die nach Art. 16 erhobenen Daten Erhebungs- oder Hilfsmerkmale sein sollen. Im übrigen darf über Art. 16 ein Zugang zu solchen personenbezogenen Daten, die nach nationalem Recht einer besonderen Geheimhaltung, z. B. dem Steuer- oder auch dem Sozialgeheimnis unterliegen, nicht eröffnet werden.

8. Die Regelung des Art. 17 ist mißglückt. Allem Anschein nach soll hier eine weitgehende Ausnahmeregelung von der statistischen Geheimhaltung zugunsten von Forschungsinstituten, einzelner Stellen vorgesehen werden, die die Möglichkeit

eröffnet, die in diesem Bereich geltenden strengeren Regelungen zu umgehen. Außerdem würde von der EUROSTAT geltenden EG-Übermittlungsverordnung 1588/90 abgewichen werden. Art. 17 sollte deshalb so gefaßt werden, daß die nationalen Zugangsregelungen für Einrichtungen mit der Aufgabe der unabhängigen wissenschaftlichen Forschung nicht umgangen werden können.

9. Der Vorschlag der Kommission sieht weder eine alsbaldige Trennung und Aufbewahrung von Erhebungs- und Hilfsmerkmalen noch eine alsbaldige Löschung personenbezogener Hilfemerkmale vor. In der Bundesrepublik Deutschland dagegen gehören entsprechende Regelungen (vgl. § 12 BStatG) zum Kernbereich des Statistikrechts. Im Volkszählungsurteil hat das Bundesverfassungsgericht ihnen grundrechtssichernde Bedeutung beigemessen.

10. Schließlich fehlt es für die Organe der Europäischen Union noch immer an einer unabhängigen und effektiven Datenschutzkontrollinstanz, an die sich jeder wenden kann, wenn er der Ansicht ist, bei der Verarbeitung seiner personenbezogenen Daten durch Stellen der Europäischen Union in seinen Rechten verletzt zu sein.

Stand 20.04.1995

Sächsischer Datenschutzbeauftragter
Dr. Giesen

Tel.: 0351 / 4935-400
Fax.: 0351 / 4935-490

Holländische Str. 2
01067 Dresden

Eingang: Kleine Packhofstraße
(Containergebäude)

Stellvertreter des Sächsischen Datenschutzbeauftragten	Tel.
Herr Schurig	405

Sekretariat	Tel.
Frau Janew	401
Frau Rostankowski	402
Frau Zimmermann	403

Referat 1
Technik, Informatik

Zentrale Aufgaben, Organisation
Datenschutztechnische Grundsatzfragen
Technik und Information
Telekommunikation
Automatisierte Datenverarbeitung
Religionsgemeinschaften

		Tel.
RL	Herr Schurig	405
R	Frau Zipser	406
R	Herr Bertelmann	407
BSB	N.N.	

Referat 2
Altdaten, Umwelt, Statistik

Land- u. Forstwirtschaft
Umwelt- u. Landesentwicklung
Altdaten, Archivwesen
Statistik, Krebsregister
Recht der Wiedervereinigung
Lebensmittelüberwachung
Veterinärwesen
Tätigkeitsbericht, Bibliothekswesen

		Tel.
RL	Herr Dr. Schnoor	410
R	Herr Bannasch	411
SB	Herr Rösch	412

Referat 3
Personalwesen, Kommunales, Steuerrecht

Kommunal- u. Wahlangelegenh.
Wirtschafts- u. Gewerberecht,
IHK-Gesetz, Handwerksordnung
öffentl.Dienstrecht, Personaldaten
Bau-, Wohnungs-,Vemessungs,-
Straßenverkehrswesen, Paß-,
Ausweis-, Meldewesen, Steuern/
Abgaben, Asyl- u. Ausländerrecht
Gleichstellung von Mann u. Frau

		Tel.
RL	Herr Rokoß	415
R	Frau Bondiek	416
R	Herr Leschke	417

Referat 4
Justiz, Sicherheit, Grundsatzfragen

Datenschutzrechtliche Grundsatzfragen
Internationales
Justiz, Polizei
Verfassungsschutz
Öffentlichkeitsarbeit

		Tel.
RL	Herr Schrader	420
R	Frau Matthiesen	421
R	Frau Nolting	422

Referat 5
Bildung, Gesundheit, Soziales

Gesundheitswesen
Sozialwesen
Schule
Universitäten und Hochschulen
Kunst und Kultur
Medien

		Tel.
RL	Herr Kaimeier	425
R	Herr Dr. Saeltzer	426
SB	Herr Hadamik	427