Sächsischer Landtag
2. Wahlperiode

DRUCKSACHE 2/6035

Schutz des Persönlichkeitsrechts im öffentlichen Bereich

5. Tätigkeitsbericht

des

Sächsischen Datenschutzbeauftragten

Dem Sächsischen Landtag

vorgelegt zum 31. März 1997

gemäß § 27 des Sächsischen Datenschutzgesetzes

Eingegangen am: 25 Juni 1997

Ausgegeben am: 26 Juni 1997

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. (Übrigens gibt es auch den umgekehrten Fall: Der [männliche] Entbindungspfleger ist eine Hebamme i. S. v. § 53 Abs. 1 Nr. 3 StPO.)

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 1008 Dresden
Telefon: 0351/4935401
Telefax: 0351/4935490

Vervielfältigung erwünscht.

Herstellung: OTTO Verlag &Druckerei OHG
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.

ABoZuV	Verordnung des SMU über die Regelung der Zuständigkeit bei der Durchführung abfallrechtlicher und bodenschutzrechtlicher Vorschriften vom 12. Februar 1996 (GVBl. S. 87)
AgrStatG	Gesetz über Agrarstatistiken (Agrarstatistikgesetz) in der Fassung der Bekanntmachung vom 23. September 1992 (BGBl. I S. 1632), zuletzt geändert durch Art. 21 des Gesetzes vom 2. August 1994 (BGBl. I S. 2018); vgl. auch Art. 1 der VO vom 20. November 1996 (BGBl. I S. 1804)
AO	Abgabenordnung
AuslG	Gesetz über die Einreise und den Aufenthalt von Ausländern im Bundesgebiet (Ausländergesetz) vom 9. Juli 1990 (BGBl. I S. 1354), zuletzt geändert durch Art. 2 Verbrechensbekämpfungsgesetz vom 28. Oktober 1994 (BGBl. I S. 3186)
BAföG	Bundesgesetz über individuelle Förderung der Ausbildung (Bundesausbildungsförderungsgesetz) in der Fassung der Bekanntmachung vom 6. Juni 1983 (BGBl. I S. 645), zuletzt geändert durch Art. 9 des Gesetzes zur Reform des Sozialhilferechts vom 23. Juli 1996 (BGBl. I S. 1088)
BAT(-O)	Erster Tarifvertrag zur Anpassung des Tarifrechts - Manteltarifliche Vorschriften (BAT-O) vom 10. Dezember 1990 (SächsABl. 1991 Nr. 10 S. 1), zuletzt geändert durch Änderungstarifvertrag Nr. 7 vom 15. Dezember 1995 (noch nicht veröffentlicht)
BauGB	Baugesetzbuch
2.BauStatG	Zweites Gesetz über die Durchführung von Statistiken der Bautätigkeit und die Fortschreibung des Gebäudebestandes vom 27. Juli 1978 (BGBl. I S. 1118), geändert durch Art. 9 des Gesetzes vom 6. Juni 1994 (BGBl. I S. 1184, 1798); vgl. auch Art. 12 der VO vom 20. November 1996 (BGBl. I S. 1804)

BBG	Bundesbeamtengesetz vom 27. Februar 1985, zuletzt geändert durch Art. 1 des Neunten Gesetzes zur Änderung dienstrechtlicher Vorschriften vom 11. Juni 1992 (BGBl. I S. 1030)
BBiG	Berufsbildungsgesetz
BDSG	Gesetz zur Fortentwicklung der Datenverarbeitung und des Datenschutzes (Bundesdatenschutzgesetz)
BGB	Bürgerliches Gesetzbuch
BImSchG	Gesetz zum Schutz vor schädlichen Umwelteinwirkungen durch Luftverunreinigungen, Geräusche, Erschütterungen und ähnliche Vorgänge (Bundes-Immissionsschutzgesetz) vom 15. März 1974 (BGBl. I S. 721, 1193) in der Neufassung vom 14. Mai 1990 (BGBl. I S. 880), zuletzt geändert durch Art. 1 des Gesetzes vom 9. Oktober 1996 (BGBl. I S. 1498)
4.BImSchV	Verordnung über genehmigungsbedürftige Anlagen vom 24. Juli 1985 (BGBl. I S. 1586), zuletzt geändert durch ÄndVO vom 16. Dezember 1996 (BGBl. I S. 1959)
BRAO	Bundesrechtsanwaltsordnung vom 1. August 1959 (BGBl. I S. 565), zuletzt geändert durch das Gesetz zur Neuordnung des Berufsrechts der Rechtsanwälte und der Patentanwälte vom 2. September 1994 (BGBl. I S. 2278)
BSeuchG	Gesetz zur Verhütung und Bekämpfung übertragbarer Krankheiten beim Menschen (Bundes-Seuchengesetz) in der Fassung der Bekanntmachung vom 18. Dezember 1979 (BGBl. I S. 2262, ber. 1980 I S. 151), zuletzt geändert durch Art. 17 des Gesetzes zur Reform der Arbeitsförderung vom 24. März 1997 (BGBl. I S. 594)
BSHG	Bundessozialhilfegesetz in der Fassung der Bekanntmachung vom 10. Januar 1991 (BGBl. I S. 94, ber. S. 808), zuletzt geändert durch Art. 20 des Gesetzes zur Reform der Arbeitsförderung vom 24. März 1997 (BGBl. I S. 594)

BstatG	Gesetz über die Statistik für Bundeszwecke (Bundesstatistikgesetz) vom 22. Januar 1987 (BGBl. I S. 462, 565), zuletzt geändert durch Art. 2 des Mikrozensusgesetzes und Gesetzes zur Änderung des Bundesstatistikgesetzes vom 17. Januar 1996 (BGBl. I S. 34)
BtBG	Gesetz über die Wahrnehmung behördlicher Aufgaben bei der Betreuung Volljähriger (Betreuungsbehördengesetz) vom 12. September 1990 (BGBl. I S. 2002, 2025)
BtG	Gesetz zur Reform des Rechts der Vormundschaft und Pflegschaft für Volljährige (Betreuungsgesetz) vom 12. September 1990 (BGBl. I S. 2002)
BVG	Gesetz über die Versorgung der Opfer des Krieges (Bundesversorgungsgesetz) vom 20. Dezember 1950 (BGBl. I S. 791) in der Fassung der Bekanntmachung vom 22. Januar 1982 (BGBl. I S. 21), zuletzt geändert durch Art. 72 des Gesetzes zur Reform der Arbeitsförderung vom 24. März 1997 (BGBl. I S. 594)
BVFG	Gesetz über die Angelegenheiten der Vertriebenen und Flüchtlinge (Bundesvertriebenengesetz) in der Fassung der Bekanntmachung vom 2. Juni 1993 (BGBl. I S. 829), zuletzt geändert durch Art. 30 des Gesetzes zur Reform der Arbeitsförderung vom 24. März 1997 (BGBl. I S. 594)
EGAB	Erstes Gesetz zur Abfallwirtschaft und zum Bodenschutz im Freistaat Sachsen vom 12. August 1991 (GVBl. S. 306), zuletzt geändert durch Art. 6 des Gesetzes vom 4. Juli 1994 (GVBl. S. 1261)
Einkommensteuer-Richtlinien	vom 18. Mai 1994 (BAnz. Nr. 104 a)
EStG	Einkommensteuergesetz
FischVO	Vierte Verordnung des SML zur Durchführung des Fischereigesetzes für den Freistaat Sachsen (Fischereiverordnung) vom 25. September 1995 (GVBl. S. 339)
GewAnzVwV	Verwaltungsvorschrift zur Durchführung der §§ 14, 15 und 55 c der Gewerbeordnung vom 6. Oktober 1995 (SächsABl. S. 1253)

GewO	Gewerbeordnung
GG	Grundgesetz für die Bundesrepublik Deutschland (Grundgesetz)
GVO	Verordnung über den Verkehr mit Grundstücken (Grundstücksverkehrsordnung [früher Grundstücksverkehrsverordnung - GVVO]) vom 15. Dezember 1977 (DDR-GBl. I 1978 Nr. 5 S. 73) in der Fassung der Bekanntmachung vom 18. April 1991 (BGBl. I S. 999), geändert durch Art. 4 des 2. VermRÄndG vom 14. Juli 1992 (BGBl. I S. 1257, 1266), neu gefaßt durch Art. 15 § 1 des Registerverfahrensbeschleunigungsgesetzes vom 20. Dezember 1993 (BGBl. I S. 2182, 2221), geändert durch Art. 2 des Gesetzes vom 4. Juli 1995 (BGBl. I S. 895)
HGB	Handelsgesetzbuch
IHK-Gesetz	Gesetz zur vorläufigen Regelung des Rechts der Industrie- und Handelskammern vom 18. Dezember 1956 (BGBl. I S. 920), zuletzt geändert durch Gesetz vom 23. November 1994 (BGBl. I S. 3475)
ImSchZuV	Verordnung des SMU über Zuständigkeiten zur Ausführung des Bundes-Immissionsschutzgesetzes, des Benzinbleigesetzes und der aufgrund dieser Gesetze ergangenen Verordnungen (Zuständigkeitsverordnung Immissionsschutz) vom 5. Juli 1994 (GVBl. S. 1282)
IuKDG	Entwurf eines Gesetzes zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste (Informations- und Kommunikationsdienstegesetz)
JGG	Jugendgerichtsgesetz in der Fassung der Bekanntmachung vom 11. Dezember 1974 (BGBl. I S. 3427), zuletzt geändert durch das Verbrechensbekämpfungsgesetz vom 28. Oktober 1994 (BGBl. I S. 3186)
KomPrO	Verordnung des SMI über das Kommunale Prüfungswesen (Kommunalprüfungsordnung) vom 14. August 1995 (GVBl. S. 290), zuletzt geändert durch VO vom 13. Januar 1996 (GVBl. S. 65)
KpS-Richtlinien	Richtlinien des Sächsischen Staatsministeriums des Innern für die Führung Kriminalpolizeilicher personenbezogener Sammlungen in den Polizeidienststellen des Freistaates Sachsen vom 15. Juli 1993 (SächsABl. S. 1094)
KRG	Gesetz über Krebsregister (Krebsregistergesetz) vom 4. November 1994 (BGBl. I S. 3351)
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. 1 des Gesetzes vom 25. November 1994 (BGBl. I S. 3538)
LStR	Lohnsteuerrichtlinien vom 10. November 1995 (BAnz. Nr. 224 a)
LwAnpG	Landwirtschaftsanpassungsgesetz [ursprünglich: Gesetz über die strukturelle Anpassung der Landwirtschaft an die soziale und ökologische Marktwirtschaft in der Deutschen Demokratischen Republik] in der Fassung der Bekanntmachung vom 3. Juli 1991 (BGBl. I S. 1418), zuletzt geändert durch das Vierte Gesetz zur Änderung des Landwirtschaftsanpassungsgesetzes vom 20. Dezember 1996 (BGBl. I S. 2082)
MDR-Staatsvertrag	Staatsvertrag über den Mitteldeutschen Rundfunk (MDR) vom 30. Mai 1991 (GVBl. S. 169)
Mediendienste-Staatsvertrag	Entwurf eines Staatsvertrages über Mediendienste
MiStra	Anordnungen über Mitteilungen in Strafsachen vom 15. März 1985 (BAnz. Nr. 60)
MHRG	Gesetz zur Regelung der Miethöhe vom 18. Dezember 1974 (BGBl. I S. 3603, 3604), zuletzt geändert durch das Gesetz zur Änderung des Gesetzes zur Regelung der Miethöhe vom 15. Dezember 1995 (BGBl. I S. 1722)
MRRG	Melderechtsrahmengesetz in der Fassung der Bekanntmachung vom 24. Juni 1994 (BGBl. I S. 1430)
MV	Verordnung über Mitteilungen an die Finanzbehörden durch andere Behörden und öffentlich-rechtliche Rundfunkanstalten (Mitteilungsverordnung) vom 7. September 1993 (BGBl. I S. 1554), zuletzt geändert durch Erste Verordnung zur Änderung der Mitteilungsverordnung vom 19. Dezember 1994 (BGBl. I S. 3848)

NW-DSG	Gesetz zum Schutz personenbezogener Daten (Datenschutzgesetz Nordrhein-Westfalen) vom 15. März 1988 (NW-GVBl. S. 160), geändert durch Gesetz vom 22. November 1994 (NW-GVBl. S. 1064)
Pflegebedürftigkeitsrichtlinien	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)
PStÄndG	Fünftes Gesetz zur Änderung des Personenstandsgesetzes (Entwurf)
PStG	Personenstandsgesetz
PStV	Verordnung zur Ausführung des Personenstandsgesetzes (Personenstandsverordnung) in der Fassung der Bekanntmachung vom 25. Februar 1977, zuletzt geändert durch Art. 1 der 13. ÄndVO vom 24. März 1994 (BGBl. I S. 621)
PTRegG	Gesetz über die Regulierung der Telekommunikation und des Postwesens vom 14. September 1994 (BGBl. I S. 2325)
RAFachBezG	Gesetz über Fachanwaltsbezeichnungen nach der Bundesrechtsanwaltsordnung und zur Änderung der Bundesrechtsanwaltsordnung vom 27. Februar 1992 (BGBl. I S. 369)
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)

SächsBG	Beamtengesetz für den Freistaat Sachsen in der Fassung der Bekanntmachung vom 16. Juni 1994 (GVBl. S. 1153), zuletzt geändert durch Art. 1 des Gesetzes vom 30. Oktober 1996 (GVBl. S. 417)
SächsDSG	Gesetz zum Schutz der informationellen Selbstbestimmung im Freistaat Sachsen (Sächsisches Datenschutzgesetz) vom 11. Dezember 1991 (GVBl. S. 401), geändert durch Gesetz vom 7. April 1997 (GVBl. S. 350)
SächsFFG	Gesetz zur Förderung und der Vereinbarkeit von Familie und Beruf im öffentlichen Dienst im Freistaat Sachsen (Sächsisches Frauenförderungsgesetz) vom 31. März 1994 (GVBl. S. 684)
SächsFFStatVO	Verordnung der Sächsischen Staatsministerin für Fragen der Gleichstellung von Frau und Mann über die statistischen Angaben für die Frauenförderung in Dienststellen im Freistaat Sachsen (Sächsische Frauenförderungsstatistikverordnung) vom 22. August 1995 (GVBl. S. 295)
SächsGDG	Gesetz über den öffentlichen Gesundheitsdienst im Freistaat Sachsen (Sächsisches Gesundheitsdienstgesetz) vom 11. Dezember 1991 (GVBl. S. 413)
SächsGemO	Gemeindeordnung für den Freistaat Sachsen vom 21. April 1993 (GVBl. S. 301), zuletzt geändert durch Gesetz vom 20. Februar 1997 (GVBl. S. 105)
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)
SächsJAPO	Ausbildungs- und Prüfungsordnung für Juristen des Freistaates Sachsen vom 22. August 1991 (GVBl. S. 327), zuletzt geändert durch VO vom 3. Juni 1994 (GVBl. S. 1073)
SächsKHG	Gesetz zur Neuordnung des Krankenhauswesens (Sächsisches Krankenhausgesetz) vom 19. August 1993 (GVBl. S. 675), zuletzt geändert durch Art. 3 Haushaltbegleitgesetz 1996 vom 22. Juli 1996 (GVBl. S. 278)
SächsKRGAG	Sächsisches Ausführungsgesetz zum Krebsregistergesetz (Sächsisches Krebsregistergesetz) vom 7. April 1997 (GVBl. S. 352)

SächsKVZ	Verordnung des Sächsischen Staatsministeriums der Finanzen über die Festsetzung der Verwaltungsgebühren und Schreibauslagen (Sächsisches Kostenverzeichnis) vom 14. Februar 1994 (GVBl. S. 493)
SächsLErzGG	Gesetz über die Gewährung von Landeserziehungsgeld im Freistaat Sachsen vom 16. Oktober 1992 (GVBl. S. 467), zuletzt geändert durch Art. 2 d Haushaltbegleitgesetz 1996 vom 22. Juli 1996 (GVBl. S. 278)
SächsLKrO	Landkreisordnung für den Freistaat Sachsen vom 19. Juli 1993 (GVBl. S. 577), zuletzt geändert durch Gesetz vom 20. Februar 1997 (GVBl. S. 105)
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)
SächsPsychKG	Sächsisches Gesetz über die Hilfen und die Unterbringung bei psychischen Krankheiten vom 16. Juni 1994 (GVBl. S. 1097)
SächsSchulG	Schulgesetz für den Freistaat Sachsen vom 3. Juli 1991 (GVBl. S. 213), zuletzt geändert durch Gesetz zur Änderung des Schulgesetzes für den Freistaat Sachsen vom 15. Juli 1994 (GVBl. S. 1434)
SächsStatG	Sächsisches Statistikgesetz vom 17. Mai 1993 (GVBl. S. 453)
SächsStudDatVO	Verordnung des Sächsischen Staatsministeriums für Wissenschaft und Kunst zur Verarbeitung personenbezogener Daten der Studienbewerber, Studenten und Prüfungskandidaten für 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)
SchwbAV	Zweite Verordnung zur Durchführung des Schwerbehindertengesetzes (Schwerbehinderten-Ausgleichsabgabeverordnung) vom 28. März 1988 (BGBl. I S. 483), zuletzt geändert durch Art. 79 des Gesetzes zur Reform der Arbeitsförderung vom 24. März 1997 (BGBl. I S. 594)
SchwbG	Gesetz zur Sicherung der Eingliederung Schwerbehinderter in Arbeit, Beruf und Gesellschaft (Schwerbehindertengesetz) in der Neufassung vom 26. August 1986 (BGBl. I S. 421), zuletzt geändert durch Art. 78 des Gesetzes zur Reform der Arbeitsförderung vom 24. März 1997 (BGBl. I S. 594)
SGB I	Sozialgesetzbuch - Allgemeiner Teil - vom 11. Dezember 1975 (BGBl. I S. 3015), zuletzt geändert durch Art. 2 des Gesetzes zur Reform der Arbeitsförderung vom 24. März 1997 (BGBl. I S. 594)
SGB III	Sozialgesetzbuch - Arbeitsförderung - Gesetz zur Reform der Arbeitsförderung (Arbeitsförderungs-Reformgesetz - AFRG) vom 24. März 1997 (BGBl. I S. 594)
SGB IV	Sozialgesetzbuch - Gemeinsame Vorschriften für die Sozialversicherung - vom 23. Dezember 1976 (BGBl. I S. 3845), zuletzt geändert durch Art. 1 des Dritten Gesetzes zur Verbesserung des Wahlrechts für die Sozialversicherungswahlen und zur Änderung anderer Gesetze vom 29. April 1997 (BGBl. I S. 968)
SGB V	Sozialgesetzbuch - Gesetzliche Krankenversicherung - vom 20. Dezember 1988 (BGBl. I S. 2477), zuletzt geändert durch Art. 5 des Gesetzes zur Reform der Arbeitsförderung vom 24. März 1997 (BGBl. I S. 594)
SGB VI	Sozialgesetzbuch - Gesetzliche Rentenversicherung - vom 18. Dezember 1989 (BGBl. I S. 2261, ber. BGBl. 1990 I S. 1337), zuletzt geändert durch Art. 2 des Dritten Gesetzes zur Verbesserung des Wahlrechts für die Sozialversicherungswahlen und zur Änderung anderer Gesetze vom 29. April 1997 (BGBl. I S. 968)

SGB VII	Sozialgesetzbuch - Gesetzliche Unfallversicherung - vom 7. August 1996 (BGBl. I S. 1254), zuletzt geändert durch Art. 7 des Gesetzes zur Reform der Arbeitsförderung vom 24. März 1997 (BGBl. I S. 594)
SGB VIII	Sozialgesetzbuch - Kinder- und Jugendhilfe - vom 26. Juni 1990 (BGBl. I S. 1163) in der Fassung der Bekanntmachung vom 15. März 1996 (BGBl. I S. 447), zuletzt geändert durch das Gesetz zur Reform des Sozialhilferechts vom 23. Juli 1996 (BGBl. I S. 1088)
SGB X	Sozialgesetzbuch - Verwaltungsverfahren - vom 18. August 1980 (BGBl. I S. 1469) und 4. November 1982 (BGBl. I S. 1450), zuletzt geändert durch Art. 4 des Dritten Gesetzes zur Verbesserung des Wahlrechts für die Sozialversicherungswahlen und zur Änderung anderer Gesetze vom 29. April 1997 (BGBl. I S. 968)
SGB XI	Sozialgesetzbuch - Soziale Pflegeversicherung - vom 26. Mai 1994 (BGBl. I S. 1014), zuletzt geändert durch Art. 10 des Gesetzes zur Reform der Arbeitsförderung vom 24. März 1997 (BGBl. I S. 594)
SHG	Gesetz über die Hochschulen im Freistaat Sachsen (Sächsisches Hochschulgesetz) vom 4. August 1993 (GVBl. S. 693)
StBerG	Steuerberatungsgesetz in der Fassung der Bekanntmachung vom 4. November 1975 (BGBl. I S. 2735), zuletzt geändert durch das Jahressteuer-Ergänzungsgesetz 1996 vom 18. Dezember 1995 (BGBl. I S. 1959)
StGB	Strafgesetzbuch
StPO	Strafprozeßordnung
StUG	Gesetz über die Unterlagen des Staatssicherheitsdienstes der ehemaligen Deutschen Demokratischen Republik (Stasi-Unterlagen-Gesetz) vom 20. Dezember 1991 (BGBl. I S. 2272), zuletzt geändert durch das Dritte Gesetz zur Änderung des Stasi-Unterlagen-Gesetzes vom 20. Dezember 1996 (BGBl. I S. 2026)
StVG	Straßenverkehrsgesetz

StVollZG	Gesetz über den Vollzug der Freiheitsstrafe und der freiheitsentziehenden Maßregeln der Besserung und Sicherung (Strafvollzugsgesetz) vom 16. März 1976 (BGBl. I S. 581, ber. S. 2088 und 1977 I S. 436), zuletzt geändert durch das Rechtspflege-Vereinfachungsgesetz vom 17. Dezember 1990 (BGBl. I S. 2847)
StVZO	Straßenverkehrs-Zulassungs-Ordnung
TDSV	Verordnung über den Datenschutz für Unternehmen, die Telekommunikationsdienstleistungen erbringen (Telekommunikationsdienstunternehmen-Datenschutzverordnung) vom 12. Juli 1996 (BGBl. I S. 982)
TKG	Telekommunikationsgesetz vom 25. Juli 1996 (BGBl. I S. 1120)
UWG	Gesetz gegen den unlauteren Wettbewerb
VermG	Gesetz zur Regelung offener Vermögensfragen (Vermögensgesetz) vom 23. September 1990 (BGBl. II S. 885, 1159) in der Fassung der Bekanntmachung vom 2. Dezember 1994, BGBl. I S. 3610), geändert durch Art. 1 des Vermögensrechtsanpassungsgesetzes vom 4. Juli 1995 (BGBl. I S. 895)
Verpflichtungsgesetz	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)
VfG	Gesetz über das Verwaltungsverfahren der Kriegsopferversorgung in der Neufassung vom 6. Mai 1976 (BGBl. I S. 1169), zuletzt geändert durch Art. II § 16 des Sozialgesetzbuches - Verwaltungsverfahren - vom 18. August 1980 (BGBl. I S. 1469)
VwGO	Verwaltungsgerichtsordnung
VwVBauStat	Verwaltungsvorschrift des SMI zum Vollzug des Zweiten Gesetzes über die Durchführung von Statistiken der Bautätigkeit und die Fortschreibung des Gebäudebestandes (2.BauStatG) vom 5. März 1993 (SächsABl. S. 555)
VwVfG	Verwaltungsverfahrensgesetz
WoGG	Wohngeldgesetz in der Fassung der Bekanntmachung vom 1. Februar 1993 (BGBl. I S. 183), zuletzt geändert durch Art. 41 des Gesetzes zur Reform der Arbeitsförderung vom 24. März 1997 (BGBl. I S. 594)
WoGSoG	Gesetz über Sondervorschriften für die vereinfachte Gewährung von Wohngeld in dem in Art. 3 des Einigungsvertrages genannten Gebiet in der Fassung der Bekanntmachung vom 16. Dezember 1992 (BGBl. I S. 2406), zuletzt geändert durch Art. 8 des Sechsten Gesetzes zur Änderung der Verwaltungsgerichtsordnung und

	anderer Gesetze vom 1. November 1996 (BGBl. I S. 1226)
ZPO	Zivilprozeßordnung

Sonstiges

ÄndVO	Änderungs-Verordnung
a. F.	alte Fassung
AfNS	Amt für Nationale Sicherheit
AKG	Arbeitsgemeinschaft Kammerleitstelle für Bemessungsgrundlagen e. V.
AOK	Allgemeine Ortskrankenkasse
ARoV	Amt zur Regelung offener Vermögensfragen
AZR	Ausländerzentralregister
BAGE	Amtliche Sammlung der Entscheidungen des Bundesarbeitsgerichts
BAnz.	Bundesanzeiger
BayVBl.	Bayerische Verwaltungsblätter
BayVGH	Bayerischer Verwaltungsgerichtshof
BfD	Der Bundesbeauftragte für den Datenschutz
BGBl.	Bundesgesetzblatt
BGH	Bundesgerichtshof
BGHZ	Amtliche Sammlung der Entscheidungen des Bundesgerichtshofs in Zivilsachen
BMF	Bundesministerium der Finanzen
BMI	Bundesministerium des Innern
BMJ	Bundesministerium der Justiz
BML	Bundesministerium für Ernährung, Landwirtschaft und Forsten

BSI	Bundesamt für Sicherheit in der Informationstechnik
BStU	Der Bundesbeauftragte für die Unterlagen des Staatssicherheitsdienstes der ehemaligen Deutschen Demokratischen Republik
BVerfG	Bundesverfassungsgericht
BVerfGE	Amtliche Sammlung der Entscheidungen des Bundesverfassungsgerichts
BVerwG	Bundesverwaltungsgericht
BVerwGE	Amtliche Sammlung der Entscheidungen des Bundesverwaltungsgerichts
BVS	Bundesanstalt für vereinigungsbedingte Sonderaufgaben (bis 31. Dezember 1994: THA)
BZR	Bundeszentralregister
CD-ROM	Compact disc-read only memory
CR	Computer und Recht [Zeitschrift; früher auch "CuR"]
DSMeld	Datensatz für das Meldewesen
DVBl	Deutsches Verwaltungsblatt
DVO	Durchführungsverordnung
ed-	erkennungsdienstlich
EG	Europäische Gemeinschaften
EU	Europäische Union
EWG	Europäische Wirtschaftsgemeinschaft
FTP	File transfer protocol
Gauck-Behörde	Der Bundesbeauftragte für die Unterlagen des Staatssicherheitsdienstes der ehemaligen Deutschen Demokratischen Republik
GEZ	Gebühreneinzugszentrale der öffentlich-rechtlichen Rundfunkanstalten der Bundesrepublik Deutschland
GVBl.	Sächsisches Gesetz- und Verordnungsblatt
IKK	Innungskrankenkasse
IM	Inoffizieller Mitarbeiter (des MfS/AfNS)
ISD	Internationaler Suchdienst Arolsen
ISDN	Integrated services digital network
JVA	Justizvollzugsanstalt
KBA	Kraftfahrtbundesamt in Flensburg
KGSt	Kommunale Gemeinschaftsstelle für Verwaltungsvereinfachung
LARoV	Landesamt zur Regelung offener Vermögensfragen

LfF	Landesamt für Finanzen des Freistaates Sachsen
LfV	Landesamt für Verfassungsschutz des Freistaates Sachsen
LKA	Landeskriminalamt Sachsen
LRA	Landratsamt
LUA	Landesuntersuchungsanstalt für das Gesundheits- und Veterinärwesen
LÜVA	Lebensmittelüberwachungs- und Veterinäramt
MDR	Mitteldeutscher Rundfunk
MedR	Medizinrecht [Zeitschrift]
MfS	Ministerium für Staatssicherheit
NJW	Neue Juristische Wochenschrift
NVwZ	Neue Zeitschrift für Verwaltungsrecht
OSA	Oberschulamt
OVG	Oberverwaltungsgericht
PASS	Polizeiliches Auskunftssystem Sachsen
PIN	Personal identification number (Persönliche Identifikationsnummer)
RP	Regierungspräsidium
RPA	Rechnungsprüfungsamt
SächsABl.	Sächsisches Amtsblatt
SächsJMBl.	Sächsisches Justizministerialblatt
SLFS	Sächsisches Landesamt für Familie und Soziales
SächsVerfGH	Verfassungsgerichtshof des Freistaates Sachsen
SK	Sächsische Staatskanzlei
SLT	Sächsischer Landkreistag e. V.
SMF	Sächsisches Staatsministerium der Finanzen
SMI	Sächsisches Staatsministerium des Innern
SMJus	Sächsisches Staatsministerium der Justiz
SMK	Sächsisches Staatsministerium für Kultus
SML	Sächsisches Staatsministerium für Landwirtschaft, Ernährung und Forsten
SMS	Sächsisches Staatsministerium für Soziales, Gesundheit und Familie
SMU	Sächsisches Staatsministerium für Umwelt und Landesentwicklung

SMWA	Sächsisches Staatsministerium für Wirtschaft und Arbeit
SMWK	Sächsisches Staatsministerium für Wissenschaft und Kunst
SSG	Sächsischer Städte- und Gemeindetag e. V.
StUFA	Staatliches Umweltfachamt
TB	Tätigkeitsbericht
TCP/IP	Transmission control protocol/Internet protocol
TdL	Tarifgemeinschaft deutscher Länder
THA	Treuhandanstalt
TK-Anlage	Telekommunikationsanlage
VZR	Verkehrszentralregister
WWW	World wide web

1 Datenschutz im Freistaat Sachsen

Mit besonderer Freude lege ich dem Sächsischen Landtag nunmehr meinen 5. Tätigkeitsbericht vor. Denn dies ist der letzte Tätigkeitsbericht der 1. Wahlperiode eines Sächsischen Datenschutzbeauftragten.

Herausragendes Ereignis des Berichtszeitraums war die *Entscheidung des Sächsischen Verfassungsgerichtshofs* zur Verfassungswidrigkeit einiger Bestimmungen des Sächsischen Polizeigesetzes, die sich mit der Datenverarbeitung, insbesondere der Datenerhebung mit besonderen Mitteln befassen. Im einzelnen berichte ich zum Inhalt der Entscheidung unter Abschnitt 5.9.1.

Das Urteil hat weit über Sachsen hinaus Aufsehen erregt. Denn zum ersten Mal hat sich ein Verfassungsgericht mit den verfassungsrechtlich wesentlichen Einzelheiten polizeilicher Datenverarbeitung befaßt. Namhafte Wissenschaftler und Praktiker haben das Urteil in der Fachliteratur - zumeist positiv - kommentiert.

Das Urteil ist nicht nur in seinem Tenor, sondern auch in seinen tragenden Gründen für den Sächsischen Landtag sowie für alle sächsischen Gerichte und Behörden verbindlich (§ 14 Abs. 1 SächsVerfGHG i. V. m. der ständigen Rechtsprechung des BVerfG zu § 31 BVerfGG). Demgemäß hat das SMI unverzüglich mit den Arbeiten zur Novellierung des Sächsischen Polizeigesetzes begonnen. Dankenswerterweise hat der Sächsische Innenminister mir Gelegenheit gegeben, frühzeitig daran mitzuarbeiten.

In meinem 4. Tätigkeitsbericht habe ich in Kapitel 3 über den wesentlichen Inhalt der *Europäischen Richtlinie zum Datenschutz* berichtet. Sie schreibt vor, das nationale (deutsche) sowie das regionale (sächsische) Recht bis Herbst 1998 den verbindlichen Vorgaben der Richtlinie anzupassen. Das Bundesinnenministerium hat kürzlich einen ersten Referentenentwurf zur Änderung des Bundesdatenschutzgesetzes vorgelegt; das SMI hat Arbeiten zur Novellierung des Sächsischen Datenschutzgesetzes aufgenommen. Zwar will sich der Bundesinnenminister zunächst auf eine Anpassung des Bundesdatenschutzgesetzes an die Richtlinie beschränken und die in Anbetracht der rasanten technischen Entwicklungen erforderliche grundsätzliche, umfassendere Novellierung parallel, aber ohne Zeitdruck erarbeiten. Erfreulich ist, daß das SMI jedoch darüber hinausgeht und beabsichtigt, das Sächsische Datenschutzgesetz insgesamt alsbald zu novellieren. Auf seine Bitte habe ich dem SMI mehrere vorläufige Stellungnahmen der in meiner Behörde eingerichteten Arbeitsgruppe zur Novellierung des Sächsischen Datenschutzgesetzes überreichen können. Den Ergebnissen dieser Zusammenarbeit, die in einem Gesetzentwurf der Staatsregierung ihren Niederschlag finden werden, möchte ich hier nicht vorgreifen. Die ersten Verhandlungen haben zwar noch bedeutsame Unterschiede, aber auch eine Reihe gemeinsamer Absichten deutlich werden lassen.

Am 18. März 1997 konnten meine Mitarbeiter und ich in die *renovierten Räume* im

Gebäude des Sächsischen Landtages umziehen. Gemeinsam mit den Abgeordneten, den Fraktionen sowie der Verwaltung des Sächsischen Landtages sind wir funktional sinnvoll und angenehm untergebracht. Wir fühlen uns hier dienstlich wohl aufgehoben. Ich halte die Konstruktion, den Datenschutzbeauftragten auch organisatorisch der Parlamentsverwaltung anzugliedern, für zweckmäßig, zumal er für seine (derzeit einzige) Aufgabe, im Informationszeitalter für einen sinnvollen und gesetzmäßigen Umgang mit personenbezogenen Informationen zu sorgen und insoweit die Exekutive zu kontrollieren, gemäß Art. 57 der Sächsischen Verfassung dem Parlament attachiert ist, das er bei seiner Kontrolltätigkeit auch hinter sich weiß.

Art. 28 der Europäischen Datenschutzrichtlinie schreibt vor, daß die Datenschutzkontrollbehörde auch im privaten Bereich "ihre Aufgaben in völliger Unabhängigkeit erfüllen" muß. Sofern es deshalb dazu kommen sollte - in einer Reihe von Ländern ist es schon so -, daß die Datenschutzaufsicht über private Unternehmen ebenfalls einem unabhängigen Datenschutzbeauftragten übertragen wird, ist dieser insoweit Teil der Exekutive im ministerialfreien Raum; seine Entscheidungen unterliegen der verwaltungsgerichtlichen Kontrolle (Art. 19 Abs. 4 GG, Art 38 SächsVerf). Gegen die Beibehaltung der - insoweit bloß organisatorischen - Anbindung an die Parlamentsverwaltung sehe ich keine durchgreifenden verfassungsrechtlichen Hinderungsgründe, zumal der Datenschutzbeauftragte im nicht-öffentlichen Bereich nicht mit der Schärfe des Verhältnismäßigkeits-Maßstabes mißt und seine Hauptaufgabe in der Kontrolle der Exekutive liegt.

Die Verwaltung des Sächsischen Landtages erledigt bauliche, technische, organisatorische und personalrechtliche Probleme für den Datenschutzbeauftragten unbürokratisch und kollegial. Für die gute Zusammenarbeit möchte ich an dieser Stelle dem Präsidenten des Sächsischen Landtages, dem Präsidium sowie allen Kolleginnen und Kollegen aus der Landtagsverwaltung herzlich danken.

Andere Datenschutzbeauftragte, die beispielsweise selbst als oberste Landesbehörden konstruiert oder separat untergebracht sind, erfahren diese Erleichterung des Dienstbetriebes nicht. Hinzu kommt, daß in informellen Gesprächen und anläßlich zufälliger Begegnungen kleinere, manchmal auch größere Datenschutz-Probleme mit den Parlamentariern besprochen und erledigt werden können, ohne daß der Aufwand eines langwierigen Schriftwechsels getrieben werden muß. Bei der anstehenden Novellierung des Sächsischen Datenschutzgesetzes sollte daran nichts geändert werden.

In den Tätigkeitsberichten habe ich zur inhaltlichen Arbeit meiner Dienststelle berichtet und jeweils eine *Bilanz* der Qualität unserer Arbeit ziehen können. Wiederholt werden wir aber auch danach gefragt, *wieviel* wir eigentlich tun, zumal die Tätigkeit eines Datenschutzbeauftragten für viele weder direkt spürbar noch vorstellbar ist. Wohl wissend um den angeblichen Ausspruch Winston Churchills: "Traue keiner Statistik, die Du nicht selbst gefälscht hast", haben wir deshalb einige Monate lang unsere 'kundenorientierten' Tätigkeiten registriert und die Ergebnisse dann auf ein

Jahr hochgerechnet. Naturgemäß ist die Aussagekraft einer solchen Statistik angreifbar und beschränkt: Es sind kurze Anfragen und langwierige Beratungen, leichte Probleme und schwierige Fälle, häufig wiederkehrende, mittlerweile zur Routine gewordenen Stellungnahmen, aber auch intensive, ins Detail gehende Mitwirkungen bei Gesetzen und anderen Vorschriften gezählt worden. Trotzdem war - jeden-falls für uns - das entstandene Bild interessant; es gibt einen ungefähren Überblick über das Jahr:

Eingaben:	ca. 180
Beratung von Bürgern:	ca. 380
Beratung von Landtagsabgeordneten:	ca. 25
Beratung von Behörden:	ca. 950
Kontrollen von Behörden:	ca. 40
Beteiligung beim Entwurf von Rechts- und Verwaltungsvorschriften:	ca. 100
Stellungnahmen zur automatisierten Verarbeitung von Personaldaten:	ca. 160
Beteiligung bei automatisierten Abrufverfahren:	ca. 20
Erarbeitung von Arbeitshilfen:	ca. 10
Mitarbeit in Fach-Arbeitskreisen:	ca. 40
Öffentlichkeitsarbeit:	ca. 30
Vortragstätigkeit:	ca. 45

Hier möchte ich allen Mitarbeitern in meiner Behörde sehr für ihre Tätigkeit danken.

1.1 Über die Grenzen des Datenschutzes*

Nach dem Volkszählungsurteil des Bundesverfassungsgerichts von 1983 weist die ab 1998 verbindliche Richtlinie der EG zum Datenschutz den deutschen Datenschutzbeauftragten eine institutionalisierte Rolle in der Informationsgesellschaft zu. Über Beobachtungs-, Beratungs-, Kontroll- und Beanstandungsbefugnisse hinaus sollen sie auch behördliche und gerichtliche Verfahren initiieren und klassische Exekutivfunktionen (Gebote und Verbote auszusprechen) übernehmen. Nach schwerer Geburt und mancher Pubertätserscheinung ist der Datenschutz dabei, erwachsen zu werden.

Die Seelenlage mancher Datenschutzbeauftragten ist aber leider noch immer von der Mißstimmung geprägt, auf die sie bei ihren Beratungen und Kontrollen stoßen. Es ist höchste Zeit, darüber nachzudenken, wieweit sie selbst daran schuld sind.

Der - manchmal milde - Spott, die Reserviertheit, ja die Ressentiments, mit denen in

*Nachdruck meines im Januar 1997 in "Computer und Recht" erschienenen Aufsatzes, mit freundlicher Genehmigung des Verlages Dr. Otto Schmidt, Köln.

Deutschland Politiker und Verwaltung "den Datenschützern" begegnen, lassen uns darüber nachdenken, wo wir stehen, was wir tatsächlich bewirken. Sind wir als staatliche Institutionen, gebunden an die verfassungsmäßige Ordnung, intellektuell redlich? Stellen wir uns maßvoll in den Kontext der Verfassung, beteiligen wir uns konstruktiv an der Durchsetzung des Rechtsstaates und an der Machtbalance? Oder huldigen wir nur einer politisch-modischen Antihaltung? Kann sich dieser Staat bunte Vögel leisten, die freiweg agieren?

Die Aufgabe der Datenschutzbeauftragten ist geprägt von ihrer Unabhängigkeit; sie unterliegen einer Dienstaufsicht nur, soweit diese Unabhängigkeit nicht berührt wird. Die damit verbundenen Gefahr der Einsamkeit und Selbstüberschätzung muß erkannt und benannt werden, es sei denn, die Datenschutzbeauftragten lassen sich weiter nachsagen, sie seien Überzeugungstäter mit Ofenrohrblick, sie seien Fundamentalisten.

Beauftragte passen nicht in die aus guten Gründen hierarchische Verwaltungsstruktur, sie entziehen sich rationaler Betrachtung, weil sie sich aus dem Kraftfeld der Gewalten gelöst haben. Sie werden zwar gestützt von einem unergründlichen Mißtrauen mancher Zeitgenossen und vieler Medienvertreter gegenüber aller staatlichen Ordnung. Die einzige Legitimation für Beauftragte ist aber die, daß sie die Interessen derer wahrnehmen, die sich nicht selbst artikulieren können, (z. B. Ausländer), die vielleicht oder angeblich Angst vor der Wahrnehmung ihrer Rechte haben (Soldaten) oder die gar nicht merken, daß und wie weit in ihre Rechte eingegriffen wird (Betroffene der Datenverarbeitung). Beauftragte sollen denen helfen, die sich aus eigener Kraft nicht gegen verfassungswidrige oder rechtswidrige Übergriffe wehren können. Beauftragte müssen also die Verfassungsordnung und die Rechtsordnung im Blick haben und nicht ihre private politische Überzeugung.

Die zunehmende Anzahl ministerialfreier Räume[1] verkompliziert aber die im Grundgesetz ohnehin schon komplex verschränkte Trennung der Gewalten und entpersonalisiert die Verantwortlichkeiten. Deshalb müssen die Datenschutzbeauftragten ihren gesetzlichen Pflichten konstruktiv nachkommen, berechenbar werden und persönliche Verantwortung übernehmen.

Ein Eingriff in die Privatsphäre durch eine ungesetzliche oder dem Grundsatz der Verhältnismäßigkeit nicht angemessene Datenverarbeitung wird vom Betroffenen regelmäßig nicht oder zu spät bemerkt. Das liegt in der Natur der Sache. Deshalb sagt das Bundesverfassungsgericht: "Wegen der für den Bürger bestehenden Undurchsichtigkeit der Speicherung und Verwendung von Daten unter den Bedingungen der automatischen Datenverarbeitung und *auch* im Interesse eines *vorgezogenen* Rechtsschutzes durch *rechtzeitige* Vorkehrungen ist die Beteiligung

[1] Wippermann, DÖV 1994, 929 ff.

unabhängiger Datenschutzbeauftragter von erheblicher Bedeutung für einen effektiven Schutz des Rechts auf informationelle Selbstbestimmung"[2]. Deshalb - und nur deshalb - muß es unabhängige Datenschutzbeauftragte geben, die für den Einzelnen und in seinem Interesse, jedoch ohne seinen konkreten Auftrag, die Verwaltung kontrollieren. Der große Unterschied zu den Gerichten besteht darin, daß diese keine Initiativrechte besitzen. Wer von der Rechtsverletzung nichts bemerkt, kann nicht initiativ werden. Deshalb kann der Einzelne seine Privatheit, seine Würde nur retten, wenn er einen "Anwalt" mit dem Datenschutzbeauftragten hat. Der aber muß *rechtzeitig* tätig werden und darf nicht nur nachkarten. Deshalb ist die frühzeitige Beteiligung durch Regierung und Parlament so wichtig[3].

Nun sollte man der Verwaltung nicht blind vertrauen, sich nicht vom Gehorsam gegenüber der Obrigkeit prägen lassen oder meinen, "unser" Grundrecht auf Privatheit sei in der Exekutive in den besten Händen. Zwar geht auch das Bundesverfassungsgericht davon aus, daß ein gesundes Mißtrauen gegenüber der Daten sammelnden, auswertenden, hortenden und übermittelnden Verwaltung durchaus berechtigt sei, unter den Bedingungen der automatisierten Datenverarbeitung sei dieses Mißtrauen gesteigert. Wären wir sicher, daß öffentliche und private Stellen mit unseren Daten von vornherein rechtmäßig und sorgsam umgingen, brauchten wir keine Datenschutzbeauftragten: Ein erneutes goldenes Zeitalter! Das bedeutet aber nicht, daß wir ewig den möglichen Daten-Mißbrauch an die Wand malen, jeder mutigen Innovation der Verwaltung mit Leichenbittermine begegnen und harmlose Fehler zum Anlaß nehmen, Behörden "öffentlich vorzuführen".

Mir fallen zu unserem juristischen Handwerkszeug einige Überlegungen ein, die diskutiert und vertieft werden sollten:

a) Da gibt es zunächst manche Widersprüchlichkeit: Interessant war z. B. unsere Zurückhaltung bei der Pflegeversicherung: Der Ruf nach allgemeiner Umsorgung, nach einer Kasko-Versicherung für alle Wechselfälle des Lebens und des Leidens prägt den "ideologischen Überbau" dieser Gesellschaft mehr als die Angst vor tiefgehender Durchleuchtung der Privatheit. Wenn es um öffentliche Fürsorge geht, soll auch der Grad der Inkontinenz des Einzelnen kein Tabu sein. Die sozialstaatliche Einmischung (Stichwort: Pflichtversicherung) in die Intimsphäre ist von unserer Kritik verschont worden: Wer die Gemeinschaft mit dem Lebens- und Leidensrisiko belastet, darf sich nicht wundern, wenn er dadurch über seine Privatheit disponiert. Denn der soziale Rechtsstaat ist notwendig ein Stück weit Kontrollstaat. Wird die Privatheit aber fallweise und partiell in den Dienst der polizeilichen Prävention oder der Strafverfolgung gestellt, ist offenbar Holland in Not.

[2] BVerfGE 65, 1 [46].
[3] Vorbildlich § 13 Abs. 5 der Geschäftsordnung der Sächsischen Staatsregierung und § 32 der Geschäftsordnung des Sächsischen Landtages.

b) Immer wieder ist zu lesen, daß "die Datensammlung auf Vorrat" rechtswidrig sei. Dabei wird zu wenig bedacht, daß Datensammlungen auf Vorrat für eine sorgsam planende und vorausschauende Verwaltung, aber auch z. B. für Polizei und Verfassungsschutz dringend erforderlich sind.[4] Wenn man es genau nachliest, sagt das Bundesverfassungsgericht, daß der Gesetzgeber den *Verwendungszweck* der Daten bereichsspezifisch und präzise zu bestimmen hat. Für diese staatliche Aufgabe müssen die Daten geeignet und erforderlich sein. Sodann: "Damit wäre die Sammlung nicht-anonymisierter Daten auf Vorrat zu unbestimmten oder zu noch nicht bestimmbaren Zwecken nicht zu vereinbaren". Das strikte Verbot der Sammlung personenbezogener Daten auf Vorrat besteht nur dann, wenn das Gebot einer konkreten Zweckumschreibung verletzt wird[5]. Ist also der Zweck einer Datensammlung gesetzlich hinreichend bestimmt, dann ist sie nicht per se rechtswidrig, sondern kann auf den Einzelfall bezogen durchaus verhältnismäßig sein. Das Ziel der Verwaltungstätigkeit (Aufgabe) darf nicht mit der Methode (Befugnis) verwechselt werden.

c) Bei der Beurteilung, ob bestimmte personenbezogene Daten zur Erreichung eines gesetzlichen Verwaltungszwecks geeignet sind, setzen sich die Datenschutzbeauftragten nicht selten an die Stelle der von ihnen beratenen oder kontrollierten Behörde und "entscheiden" darüber, ob es nicht noch andere Methoden gibt, die zum gleichen Ziel, also zur gleichen Erkenntnis der Behörde führen. Richtig ist, daß die Verwaltung bei Erfüllung ihrer Aufgaben unter mehreren möglichen Maßnahmen nur diejenigen treffen darf, die geeignet sind, den angestrebten Zweck zu erreichen. Stehen mehrere geeignete Wege zur Erreichung des erstrebten Erfolges offen, so bleibt der Behörde zunächst und insoweit das Ermessen, welche der Möglichkeiten sie wählt. Bei der Prüfung der Geeignetheit eines Mittels im Sinne der Möglichkeit, den angestrebten Zweck zu fördern, ist es nicht die Pflicht der Exekutive zu prüfen, ob der Erfolg auch in jedem Einzelfall tatsächlich erreicht werden kann oder erreicht wird. Die abstrakte Möglichkeit der Zweckerreichung genügt. Ein Datum ist jedenfalls geeignet, wenn es den Erfolg fördert. Die Datenschutzbeauftragten sind nicht befugt, hier über die Prüfungskompetenz der Verwaltungsgerichte hinauszugehen.

Ähnlich ist es bei der Prüfung und Abwägung der Erforderlichkeit: Das Problem der weniger belastenden Alternativlösungen stellt sich häufig nicht in der Schärfe, wie manche dies glauben: Der Begriff der Erforderlichkeit ist nicht gleichzusetzen mit der "condicio sine qua non". Die Lehre vom Grundsatz des einerseits notwendigen, andererseits mildesten Eingriffs[6] befiehlt, in jedem Einzelfall den Einschnitt in das

[4] Manchmal habe ich den Eindruck, daß an den Verwaltungsmethoden nur deshalb genörgelt wird, weil die "ganze Richtung" mißfällt, also das gesetzgeberische Ziel politisch nicht schmeckt.

[5] BVerfGE 65, 1 [46 f.].

[6] Ständige Rechtsprechung des Bundesverfassungsgerichts, zuletzt BVerfGE 80, 137 [153] unter Bezugnahme auf BVerfGE 17, 306 [314]; 55, 159 [165], 75, 108 [154 f.].

Persönlichkeitsrecht des Betroffenen gerechterweise so schonend wie möglich zu halten. "Dabei ist aber auch der Grad der größeren oder geringeren Beeinträchtigung der Allgemeinheit in den Blick zu nehmen"[7]. Die Suche nach einem gerechten Ausgleich zwischen Eingriff und Zweck hat mithin etwas mit der Vermeidung von Verwaltungsaufwand und mit Sparsamkeit zu tun. Nur dann, wenn Datenerhebung oder -verarbeitung tief in das Persönlichkeitsrecht einschneiden, sind derartige Aspekte nachrangig. Das Grundgesetz billigt zunächst dem *Gesetzgeber* in der Bestimmung der zur Verfolgung seiner Ziele erforderlichen Maßnahmen einen "weiten Gestaltungsspielraum" zu[8]. Zwar besteht ein derart weiter Spielraum für die *Exekutive* nicht:[9] Eine Datenerhebung und -verarbeitung ist aber erforderlich, wenn die Verwaltung nicht ein anderes, *gleich wirksames*, aber das Grundrecht nicht oder doch weniger fühlbar einschränkendes Mittel hätte wählen können[10]. Das Erforderlichkeitsprinzip zwingt zwar dazu, das Ziel mit individuellen und schonenden Mitteln zu erreichen, es schließt aber bestimmte Verwaltungsobliegenheiten, auch die der Einsparung finanzieller und persönlicher Ressourcen, nicht aus dem Katalog der zur Abwägung anstehenden Instrumentarien und Methoden aus.[11] Dies gilt insbesondere dann, wenn ein Grundrecht nur peripher berührt wird und zugleich eine große Zahl von (z. B. Kontroll-) Vorgängen zu erledigen ist. Hier - genau hier - scheiden sich die Geister: Nur wenn *eindeutig* feststeht, daß andere *gleichgeeignete, aber weniger tief einschneidende* Methoden und Mittel zur Verfügung stehen, liegt ein Ermessensfehlgebrauch vor[12]. Das heißt - um nicht mißverstanden zu werden - keineswegs, daß das Grundrecht auf dem Altar der Zweckmäßigkeit oder der Verwaltungsträgheit geopfert wird, und es bedeutet nicht, daß gängige Methoden, bloße Zweckmäßigkeiten oder datensammelnder Aktivismus den Ausschlag geben dürften.

Auch bei der Prüfung der Verhältnismäßigkeit im engeren Sinne, also bei einer Gesamtabwägung zwischen der Schwere des Eingriffs und dem Gewicht sowie der Dringlichkeit der ihn rechtfertigenden Gründe, muß zwar die Grenze der Zumutbarkeit gewahrt sein[13]. Die Prüfung, ob Zweck und Mittel zueinander und proportional angemessen sind, blendet jedoch Argumente legitimer Verwaltungseffizienz

[7] Stern, Staatsrecht Bd. III 2, § 84 II, 3 S. 781; Jarass-Pieroth, GG-Kommentar Art. 20 Rdnr. 60; BVerfGE 77, 84 [110 f.]; 81, 70 [91 f.].

[8] Ständige Rechtsprechung des Bundesverfassungsgerichts, zuletzt BVerfGE 81, 156 [192 f.].

[9] BVerfGE 80, 137 [161].

[10] Ständige Rechtsprechung des Bundesverfassungsgerichts, BVerfGE 30, 292 [316], zuletzt BVerfGE 92, 262 [273] unter Bezugnahme auf BVerfGE 70, 278 [286] m. w. N.

[11] Dies kommt z. B. auch bei den gesetzlichen Regelungen zur Datensicherung (technische und organisatorische Maßnahmen zur Datensicherung) zum Ausdruck: "Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht." (z. B. § 9 Abs. 1 S. 2 SächsDSG).

[12] Dazu z. B. Stern, Staatsrecht Bd. III/2, § 84, II 3, 4.

[13] Ständige Rechtsprechung des Bundesverfassungsgerichts, zuletzt BVerfGE 90, 145 [173] unter Berufung auf BVerfGE 70, 278 [286] m. w. N.

keineswegs völlig aus. Aufwand und Ertrag sind an der Ordnungs- und Wertstruktur des Grundgesetzes zu messen[14]. Die damit verbundenen - oft sehr ins einzelne gehenden - Rechtsfragen zu entscheiden ist grundsätzlich Aufgabe der Gerichte, deren Kontrollintensität aber relativ begrenzt ist (Unterschied von Rechtsstaat zu Justizstaat).[15] Zwar können die Datenschutzbeauftragten für sich eine uneingeschränkte Nachprüfungs- und Beanstandungsmöglichkeit reklamieren. Vordringlich ist es aber ihre Aufgabe, Augen zu öffnen, Alternativen aufzuzeigen und zu diskutieren, Plausibilitätsfragen zu stellen und entsprechende Prüfungen vorzunehmen sowie Hinweise zur Vermeidung von Härten für die Betroffenen zu geben. Dabei darf der Verwaltungsaufwand der öffentlichen Stellen nicht aus den Augen verloren werden. Dann trifft die Überzeugungsarbeit auf viel Verständnis.

Es ist nicht klug, in derart komplexen Bewertungsfragen zu dem scharfen Mittel der Beanstandung zu greifen, wenn nicht offenkundige Fehleinschätzungen und Fehlhaltungen der Behördenleitung zu beklagen sind.

d) Schnell und sorgenvoll wird von Datenschützern der Verlust des "Kernbereichs" des Grundrechts auf informationelle Selbstbestimmung behauptet. In den letzten Monaten geschah dies häufig in Publikationen zum Problem des Großen Lauschangriffs. Nun besagt die Wesensgehaltsgarantie des Art. 19 Abs. 2 des Grundgesetzes aber nicht, daß die restlose Entziehung eines Grundrechts im Einzelfall (partiell und befristet) verboten wäre. Schon zu Beginn seiner Rechtsprechung hat das Bundesverfassungsgericht dies - übrigens gültig bis heute - offengelassen[16]. Erst dann, wenn gesetzliche Regelungen insgesamt z. B. das Grundrecht auf Unverletzlichkeit der Wohnung oder das Grundrecht auf informationelle Selbstbestimmung in Teilbereichen des täglichen Lebens völlig aushebeln und aufheben würden, wären sie wegen Verstoßes gegen Art. 19 Abs. 2 GG nichtig. Was die Voraussetzungen und Kontrollen des Großen Lauschangriffs angeht, so darf ich auf die Rechtsprechung des Sächsischen Verfassungsgerichtshofs verweisen[17]. Dort werden Voraussetzungen und Verfahren eines Großen Lauschangriffs sowie der Schutz derjenigen Betroffenen festgelegt, die - ex post gesehen - zu unrecht belauscht, "heimgesucht" wurden. Zum räumlichen Kernbereich des Privatlebens wird immerhin auch ausgeführt: "Jeder Raum, der nach außen den Anschein absoluter Schutzwürdigkeit weckt, kann in einer Weise genutzt werden, die diesen Schutz nicht verdient"[18]. Werden also Räume, die dann ja nur scheinbar zum Kernbereich *privater* Lebensgestaltung gehören, zum Zwecke der Verabredung von schweren Straftaten mißbraucht, kommt für sie der Schutz des Kernbereichs nicht in Betracht. Stellt sich im

[14] Stern a.a.O.
[15] Dazu Lerche in Isensee-Kirchhof, Handbuch des Staatsrechts, Bd. V, § 122, Rdnr. 18, 19; Wittig, DÖV 1968, 817-825.
[16] BVerfGE 2, 266 [285]: 6, 32 [41].
[17] Urteil vom 14. Mai 1996, Vf. 44 - II - 94, S. 84 ff.
[18] a.a.O. S. 88.

nachhinein heraus, daß ein - verdichteter - Mißbrauchsverdacht unberechtigt war, sind alle Daten zu löschen (Verwertungsverbot). Allein die Gefahr, im Einzelfall trotz hinreichender Vorkehrungen den Kernbereich letztlich unberechtigt zu verletzen, führt folglich nicht zum absoluten Verbot staatlicher Eingriffe. Hier hilft nur der "Grundrechtsschutz durch Verfahren".

Dabei darf nicht vergessen werden, daß die klassische Legitimation jedes Staatswesens darin liegt, *jedem* seiner Einwohner innere und äußere Sicherheit im Sinne der Entfaltung (Art. 2 Abs. 1 GG), aber auch des staatlichen Schutzes seiner Persönlichkeit (Art. 2 Abs. 2 GG) zu gewährleisten.

e) Eine weitere juristische Fehleinschätzung mancher Datenschützer liegt ihrem Ruf nach bereichsspezifischen Regelungen zugrunde. Das Bundesverfassungsgericht führt aus, daß das Recht auf informationelle Selbstbestimmung nicht schrankenlos gewährleistet sei. Die Spannung Individuum - Gemeinschaft sei im Sinne der Gemeinschaftsbezogenheit und Gemeinschaftsgebundenheit der Person entschieden. Grundsätzlich müsse daher der Einzelne Einschränkungen seines Rechts auf informationelle Selbstbestimmung im überwiegenden Allgemeininteresse hinnehmen. "Diese Beschränkungen bedürfen nach Art. 2 Abs. 1 GG [...] einer (verfassungsmäßigen) gesetzlichen Grundlage, aus der sich die Voraussetzungen und der Umfang der Beschränkungen klar und für den Bürger erkennbar ergeben und die damit dem rechtsstaatlichen Gebot der Normenklarheit entspricht"[19].

Aus diesem Zitat leiten manche die Verpflichtung des Gesetzgebers her, im einzelnen diejenigen Daten bis ins Detail zu benennen, die von der Exekutive erhoben, verarbeitet oder übermittelt werden dürfen. Paradiesische Zustände sollten jedoch nicht in einer unermeßlichen Flut spezieller Normen ersehnt werden. Solchen Wünschen liegt ein zweifaches Mißverständnis zugrunde:

Die Exekutive ist zum einen nicht die bloße Umsetzungsmaschinerie von gesetzlichen Vorschriften. Sie hat vielmehr eigene Einschätzungsprärogativen und eigenständige Umsetzungskompetenzen. Die Wesentlichkeitstheorie[20] zwingt die Verwaltung nur bei wirklich spürbaren Eingriffen in Grundrechtspositionen unter das Joch des Gesetzes.

Zum anderen bedeutet das rechtsstaatliche Gebot der Normenklarheit, das für die Umsetzung in der Verwaltung konkret in § 37 Abs. 1 des Verwaltungsverfahrensgesetzes zum Ausdruck kommt, nichts anderes als Vorhersehbarkeit und Justitiabilität: Gesetzliche Vorschriften (und darauf fußende Verwaltungsakte) müssen in ihren Voraussetzungen und in ihrem Inhalt so formuliert sein, daß die von ihnen

[19] BVerfGE 65, 1 [43 f.] unter Berufung auf BVerfGE 45, 400 [420].
[20] BVerfGE 20, 150 [157 f. m. w. N.]; 80, 137 [161]. Siehe auch die Lehre vom Vorbehalt des Gesetzes.

Betroffenen die Rechtslage erkennen und ihr Verhalten danach einrichten können[21]. "Die Anforderungen an die Bestimmtheit der Norm erhöhen sich mit der Intensität, mit der auf der Grundlage der betroffenen Regelung in grundrechtlich geschützte Bereiche eingegriffen werden kann. Dies hat jedoch nicht zur Folge, daß die Norm dann überhaupt keine Auslegungsprobleme aufwerfen darf. Dem Bestimmtheitserfordernis ist vielmehr genügt, wenn diese mit herkömmlichen juristischen Methoden bewältigt werden können"[22]. Hier greift der Grundsatz der Verhältnismäßigkeit (siehe c).

Wenn beispielsweise im Sammlungsgesetz steht, daß der Sammlungsunternehmer seine Sammlung anzumelden hat, so bedarf es keiner Vorschrift dahin, welche Daten er dabei im einzelnen von sich selbst nennen muß. Wenn das gleiche Gesetz die Ziele und Maßstäbe einer Kontrolle der Sammlungen durch die Ordnungsbehörde nennt, so bedarf es keiner Norm, die im einzelnen die dazu geeigneten, erforderlichen und zumutbaren Daten aufzählt. Bei näherem Hinsehen wäre dies auch nicht möglich.

f) Gesetzliche Aufgabe der Datenschutzbeauftragten ist es gemeinhin, die öffentlichen Stellen zur Einhaltung von Datenschutzvorschriften zu beraten und sie zu kontrollieren. Dies schließt nicht aus, daß er - wenn auch sicherlich sehr selten - den Behörden einen Rat dahin gibt, daß sie zur ordnungsgemäßen Erfüllung ihrer Aufgabe weitere Daten erheben dürfen als dies bislang der Fall ist. Der Datenschutzbeauftragte ist nirgendwo in seiner Aufgabe dahin beschränkt, ein ewiger Nein-Sager zu sein. Effektive, gleichmäßige und glaubwürdige Verwaltung muß den Mut aufbringen, gesetzliche Spielräume der Datenerhebung und -verarbeitung auch tatsächlich zu nutzen, wenn dies erforderlich ist. Deshalb habe ich beispielsweise für eine Pflichtmeldung aller Krebserkrankungen zum Krebsregister plädiert. Wenn man die Meldung zum Krebsregister von einer Einzelfallentscheidung jedes Patienten abhängig macht, so führt dies dazu, daß der Arzt jeden Patienten vollinhaltlich über seine Krankheit aufzuklären hat. Dies wiederum erzeugt einen staatlichen Druck auf eine allein ärztlich verantwortete Aufklärungspraxis. Zum anderen werden die beim Krebsregister eingehenden Meldungen - wie in Hamburg geschehen - so unvollständig, daß der wissenschaftliche Wert der Datensammlung verlorengeht: Nur annähernd vollzählige Meldungen sind epidemiologisch wertvoll.[23]

g) In den letzten Monaten ist die schon seit mehreren Jahrzehnten geführte Diskussion

[21] Ständige Rechtsprechung des Bundesverfassungsgerichts, BVerfGE 21, 73 [79 f.], zuletzt BVerfGE 87, 234 [263 f.]: Typische Erscheinungen des sozialen Lebens können mit unbestimmten Rechtsbegriffen gekennzeichnet werden. Ihre Konkretisierung ist Aufgabe der Verwaltungsbehörden und der Fachgerichte (es folgen weitere Nachweise).

[22] BVerfGE 83, 130 [145]; 86, 288 [311]; 90, 1 [16 f.].

[23] Hier hängt in der Tat die Geeignetheit der Datensammlung zur Erreichung des Zwecks der epidemiologischen Forschung von der Tiefe des Eingriffs, also der Pflichtmeldung, ab.

darüber, ob wissenschaftliche Forschung durch Datenschutzrecht behindert oder gar verhindert wird, neu aufgelebt[24]. Diesen Vorwurf muß man sehr ernst nehmen. Die datenschutzrechtlichen Regelungen sind im wesentlichen Landesrecht[25]. Alle einschlägigen Vorschriften enthalten eine Privilegierung der Forschung, etwa indem sie die Zweckänderung von Daten erlauben, die ursprünglich zu einem anderen Zweck als zu dem konkreten Forschungsvorhaben erhoben worden waren. Das wird leider oft übersehen.

Häufig werden die für die Forschung benötigten personenbezogenen Daten bei einem Probanden erhoben. Dessen freiwillige Mitarbeit, besser: seine Einwilligung, setzt ausreichende Information voraus. Anders als bei Verwaltungsaufgaben und -befugnissen, die mit dem wohlfeilen Instrumentarium der Einwilligung weder wesentlich erweitert noch neu geschaffen werden dürfen, herrscht nach Art. 5 Abs. 3 GG, der insoweit auch für öffentliche Institutionen gilt, das Prinzip der Forschungsfreiheit. Von den Forschern wird immer wieder vorgetragen, daß die Information des Probanden unter Umständen die Gefahr einer zu hohen Ablehnungsquote berge, so daß das Vorhaben zu scheitern drohe. Besonders abschreckend wirke die Schriftform der Einwilligung, die nach den Datenschutzgesetzen für den Regelfall vorgesehen ist. Umfang und Form der Belehrung müssen - so will es der Grundsatz der Verhältnismäßigkeit - aber davon abhängen, wie tief das Persönlichkeitsrecht des Probanden berührt wird.

Grundsätzlich sind Daten beim Betroffenen zu erheben. Unter anderem sozialwissenschaftliche oder medizinische Forschung können jedoch nicht darauf verzichten, den Probanden auch zu anderen Personen, z. B. Familienmitgliedern (Dritte), zu befragen. Die Dritten sind meist nur in ihrer Beziehung zu dem Probanden von Interesse. Ihre unmittelbare Beteiligung kommt - auch aus Gründen der Praktikabilität - häufig nicht in Betracht. Dabei geht es in der Regel um Sichtweisen des Probanden oder um Einflüsse von Dritten auf ihn (z. B. Vererbung). Man kann deshalb durchaus diskutieren, ob es sich überhaupt um Daten Dritter handelt oder eigentlich doch um Daten des Probanden, die nur reflexiv mit Daten Dritter in Beziehung stehen. Sind solche relationalen Angaben immer mit einem doppelten Schutz zu versehen? Wessen Schutz steht bei solchen gemischten Angaben im Vordergrund? Schadet es dem Probanden, wenn man Dritte einbezieht?

Die Datenschützer müssen auf mehreren Ebenen mit den wissenschaftlichen Institutionen, seien sie privatrechtlich oder öffentlich-rechtlich organisiert, einen konstruktiven Dialog beginnen und von Unwesentlichem, das aus der Sicht der Forscher schreckliche Bürokratie ist, Abschied nehmen.

Fazit:

[24] Denkschrift der Deutschen Forschungsgemeinschaft "Forschungsfreiheit - Ein Plädoyer für bessere Rahmenbedingungen der Forschung in Deutschland", Weinheim 1996; Resolution der Arbeitsgemeinschaft der Wissenschaftlichen Medizinischen Fachgesellschaft, 6. Mai 1995, Frankfurt am Main.

[25] Siehe als Beispiele §§ 12, 13, 30 Sächsisches Datenschutzgesetz, § 34 Sächsisches Krankenhausgesetz, § 10 Sächsisches Archivgesetz, aber andererseits auch § 75 SGB X.

Nur durch kluge Selbstbeschränkung gewinnt der Datenschutz an Souveränität. Wenn er aber weiterhin in erster Linie emotional betrieben wird, wird er nicht mehr gehört. Wer die vorgenannten Rechtsprobleme zutreffend löst, hilft, den Staat kurz zu halten, ihn auf Wesentliches zu beschränken, dadurch Haushaltsmittel zu sparen und vor allem eine effektive interne und justitielle Kontrolle im Interesse aller Betroffenen zu gewährleisten. Also: Mehr Mut zur Normalität!

Viele meiner Kollegen in Bund und Ländern haben die vorstehenden Ausführungen für überspitzt gehalten. Sie meinen, ich hätte die Datenschützer schlimmer dargestellt, als sie sind. Damit kann ich leben, weiß ich jetzt doch, daß die aufgezeigten Fehler von allen als Fehler angesehen werden.

Insbesondere angesichts des klaren - auch durch (meines Wissens nicht schriftlich vorliegende) Protokollerklärungen der Mitgliedsstaaten nicht interpretierbaren - Wortlauts des Art. 28 der Richtlinie müssen Rechtsstellung, Aufgaben und Befugnisse der Datenschutzkontrollbehörden in Deutschland gründlich überdacht werden: Mir scheint, daß gesichert werden muß, daß die Datenschutzkontrollbehörden ihre Aufgaben im öffentlichen und privaten Bereich "in völliger Unabhängigkeit" erfüllen können und daß die Verbindlichkeit ihrer Entscheidungen einerseits gestärkt, andererseits aber auch unter richterliche Kontrolle gestellt werden muß, um den Vorgaben der Richtlinie und der deutschen Verfassungslage zu genügen. Auch hier hat der Gesetzgeber jedoch Entscheidungs-Spielräume; er wird sie zu nutzen wissen.

1.2 Die Aufdeckung von Stasi-Vergangenheit und Systemnähe ist gerecht

Zu den ebenso grundfalschen wie modischen Argumenten in der Betroffenheitsdiskussion in Deutschland gehört es, den Rechtsstaat zu kritisieren und ihm die Kraft abzusprechen, für Gerechtigkeit zu sorgen, wenn es darum geht, "die DDR aufzuarbeiten". Bärbel Bohley wird das wohlfeile Wort in den Mund gelegt, man habe Gerechtigkeit gewollt und den Rechtsstaat bekommen. Andere witzeln, vor Gericht erhalte man nicht sein Recht, sondern ein Urteil. Solchen Sprüchen liegt ein Fehlverständnis zugrunde: Keine weltliche Instanz kann es jedem recht machen. Einer verliert, und zwar auch dann, wenn er selbst für sich "auch ein bißchen recht hatte". Das Bild von Justitias Waage zeigt auf beiden Seiten Recht. Aber: Wo neigt sich die Schale? Gesetze zeigen die Kraft der Gesellschaft, dies zu entscheiden. Dazu gehören auch die Verfahrensregeln, die zu kennen und anzuwenden den guten Juristen erweisen (viele verlorene Prozesse, über die sich die Gerechten ereifern, sind das Ergebnis formeller Fehler ihrer Rechtsberater).

Der vorsichtige, trockene, übrigens nur ausnahmsweise auf Bestrafung angelegte Rechtsstaat und "der Datenschutz" werden in diesem Zusammenhang aber auch gerne als Vorwand benutzt: So behauptet der Leipziger Medienwissenschaftler Prof. Haller -

in amtlicher Eigenschaft - in einem Leserbrief an die F.A.Z. vom 11. Februar 1997 exemplarisch, datenschutzrechtliche Vorschriften stünden einer personenbezogenen Veröffentlichung der DDR-Vergangenheit entgegen. Einer seiner Studenten hat in seiner Diplomarbeit über die Wandlung der Leipziger Volkszeitung vom SED-Bezirksparteiorgan zur unabhängigen Tageszeitung unter anderem nachgewiesen, daß der jetzige Geschäftsführer des Verlags als ehemaliger Verlagsleiter von der Stasi als B-Kader bestätigt wurde, also die Aufgabe hatte, für den Spannungsfall verkürzte Weisungsstränge aktiv zu garantieren. Haller, der die Diplomarbeit betreut hat, äußert nun, sie dürfe nur unter bestimmten Auflagen veröffentlicht werden, weil sie sonst den Anforderungen des sächsischen Datenschutzrechts, insbesondere des Sächsischen Archivgesetzes, zum Schutz der Persönlichkeit nicht genüge.

Wie viele Interessierte setzt auch Haller den datenschutzgerechten Umgang mit Altdaten der DDR - jedenfalls soweit es um Sachsen geht - und mit Archivalien aus dem MfS in ein falsches Licht: Der Sächsische Landtag hat sich aus guten Gründen dafür entschieden, die historische Aufarbeitung der DDR-Vergangenheit aktuell und personenbezogen zu ermöglichen. Denn Vergangenheitsbewältigung ist immer zugleich Gegenwartsbewältigung. Schon 1991 hat er im Datenschutzgesetz jedermann - bei Androhung von Strafe - dazu verpflichtet, dem Datenschutzbeauftragten alle Altdatenbestände zu melden. Alle Datenträger, die die allgegenwärtige Obrigkeit der DDR dokumentieren, sollten bekannt und den staatlichen (später auch den kommunalen) Archiven zugeführt werden. Etwa 1200 Meldungen zu privaten und öffentlichen Standorten in Sachsen weisen auf viele Kilometer Akten hin, die Machtstrukturen in allen Lebensbereichen beispielhaft dokumentieren und beweisen, daß das Alltags-, Arbeits- und Familienleben der obrigkeitlichen Kontrolle unterworfen war. Alles diente dem Zweck, die "entwickelte sozialistische Persönlichkeit" zu schaffen.

Das Sächsische Archivgesetz nimmt - archivrechtlich eher ungewöhnlich, aber verfassungsrechtlich geboten - Amtsträger in Ausübung ihrer Ämter von dem durch Schutzfristen bewirkten Persönlichkeitsschutz grundsätzlich aus. Denn Funktionäre verkörpern den Staat, der selbst ja nicht Träger, sondern Adressat der Grundrechte, also auch des Rechts auf informationelle Selbstbestimmung, ist. Als Amtsträger gelten - neben den einschlägigen Personen im 'öffentlichen Dienst' der DDR - auch alle führenden Mitarbeiter ehemaliger wirtschaftsleitender Organe, der Kombinate, Betriebe, Genossenschaften, Parteien und gesellschaftlichen Organisationen auf dem heutigen Gebiet des Freistaates Sachsen in der Zeit zwischen der Kapitulation am 8. Mai 1945 und der Wiedervereinigung am 3. Oktober 1990. Dies ist übrigens ein gerechter und klüger gewählter Zeitraum als derjenige, der für die Eigentumsrestitution gilt. Für die Daten der Funktionäre aus dieser Zeit gelten nicht die üblichen Schutzfristen. Auch das geschichtswissenschaftlich durchaus umstrittene, aber rechtsstaatliche Gebot, den Personenbezug in Veröffentlichungen zu vermeiden, wenn der Forschungszweck das zuläßt, gilt nur, soweit überhaupt gesetzliche Schutzfristen greifen: Der Gesetzgeber hätte es leicht gehabt, dieses Anonymisierungsgebot - sozusagen erst recht - für die Fälle zu statuieren, in denen keine Schutzfristen gelten.

Er hat es nicht getan. Er wollte, daß die Erkenntnisse auch aus der jüngsten Vergangenheit kleinräumig, konkret, in Kenntnis der Beteiligten verarbeitet werden, daß die Diskussion unter Lebenden stattfinde. Die Geschichte kennt keine Schlußstriche.

"Aufarbeitung" mißrät also nicht zur Theorie, nicht zur rechtspolitisch abgehobenen Veranstaltung. Vielmehr erweist sie sich in aktuellen Berichten und eindrucksvollen Ausstellungen, vor allem aber im Gespräch zwischen Tätern und Opfern, so wie dies von den Stasi-Beauftragten der östlichen Länder - Brandenburg hat sich da bemerkenswerterweise ausgenommen und diese Institution gar nicht erst geschaffen - vorbildlich organisiert wird.

Forschung und Publizistik haben insoweit freien Zugang zu allen von staatlichen und kommunalen Stellen archivierten Unterlagen. Dieses Material belegt in manchen Bereichen eine verblüffende Personalkontinuität in Leitungsfunktionen über die Wende hinweg.

Die erwähnte Diplomarbeit stützt sich bei ihren interessanten Ergebnissen weitgehend auf Stasiunterlagen: Sie dokumentieren u. a., wie weitgehend Verlagsmanager, Journalisten und Publizisten Mitarbeiter des MfS waren. Für die Frage, ob personenbezogene Erkenntnisse dieser Art veröffentlicht werden dürfen, enthält das Stasi-Unterlagengesetz überzeugende Regelungen: Informationen über Personen der Zeitgeschichte, Inhaber politischer Funktionen oder Amtsträger, soweit sie volljährige Mitarbeiter und Begünstigte der Stasi gewesen sind, dürfen veröffentlicht werden, wenn dadurch nicht ihre "überwiegenden schutzwürdigen Interessen" beeinträchtigt werden. Eine ähnliche Abwägung schreibt auch das Sächsische Archivgesetz vor. Bei der Auslegung dieses unbestimmten Rechtsbegriffs ist zunächst der formulierte Zweck des Stasi-Unterlagengesetzes zu berücksichtigen, der mehrschichtig ist: Dem Einzelnen wird Zugang zu seinem persönlichen Schicksal gewährt, er soll gleichzeitig vor einem persönlichkeitswidrigen Umgang mit Stasi-Unterlagen geschützt werden. Darüber hinaus wird die historische, politische und juristische Aufarbeitung der Tätigkeit der Stasi gewährleistet und gefördert. Nur zu diesen Zwecken werden öffentlichen und privaten Stellen die erforderlichen Informationen zur Verfügung gestellt. Das Interesse der Allgemeinheit an historischer Aufarbeitung der DDR, insbesondere der Strukturen des Stasiapparates und des Ausmaßes seines Informantensystems, hat im Stasi-Unterlagengesetz gerechte Gestalt gefunden.

Wenn das Gesetz die Veröffentlichung grundsätzlich für zulässig erklärt, so geht es zunächst davon aus, daß die Informationen der Wahrheit entsprechen. Denn die Forschungsfreiheit muß sich - wie jede Freiheit - an der Wahrheit orientieren. Eine urkundlich belegte, wahre Information über früheres amtliches Verhalten beeinträchtigt schutzwürdige Interessen der Täter in der Regel nicht.

Die Verpflichtung zur sorgfältigen, auf vollständige Wahrheit gerichteten Recherche zielt nicht nur auf eine realistische und - endlich - differenzierte Meinungsbildung des

Publikums, sondern auf einen gerechten Ehrenschutz der Betroffenen. Das rechte Maß zwischen Leisetreterei und Schmähkritik, zwischen Legendenbildung und Hartherzigkeit wird von der Wahrheit gegeben. Wer die würdelosen Angriffe des zentralen Machtapparates auf die Meinungsbildung bis an den Familientisch heute in die verklärende Abendsonne der guten armen Zeit taucht, dem sei das Aktenstudium empfohlen.

Eine Sorgfaltspflicht des Wissenschaftlers, über seine Erkenntnis aus Stasiunterlagen mit den dort enttarnten Tätern zu reden, besteht nicht. Dies zum einen, weil die Akten der Stasi in aller Regel sachlich wahr und vollständig sind, zum anderen, weil - ebenfalls nach aller Erfahrung - mit einem Dementi seitens der Täter zu rechnen ist. "Sie lügen bis zum Schafott" heißt es landläufig, weil die Zahl der falschen Erklärungen, der verharmlosenden Ausflüchte so hoch ist. Hier wird deutlich, daß die professionelle Konspiration in Fleisch und Blut übergegangen ist. Der Gesellschaft muß damit aber auch deutlich werden, wie sehr manche Täter sich innerlich schämen. Vielleicht haben die meisten aber nur die begründete Angst davor, ihr spießbürgerliches Gesicht zu verlieren. Sie, die das Vertrauen ihrer Bekannten oder Verwandten mißbraucht haben, merken jetzt erst, was es heißt, deren Vertrauen zu verlieren. Würde die wissenschaftliche Veröffentlichung dokumentierter Wahrheit von einem Placet der Täter abhängig oder mit dem Ballast unerträglicher Halbwahrheiten beschwert, so bliebe die Macht, die Wahrheit zu verschleiern da, wo sie früher war.

Das allgemeine Persönlichkeitsrecht garantiert ein umfassendes, subjektives Recht auf private Achtung und Entfaltung. Aber es wird verfassungsimmanent begrenzt durch die Rechte anderer und durch die verfassungsmäßige Ordnung. Nahezu absoluten Schutz genießt nur die Intimsphäre, das heißt die innere Gedanken- und Gefühlswelt mit ihren äußeren Erscheinungsformen, z. B. in Tagebuchaufzeichnungen. Die sozial geprägte Privat- oder Individualsphäre, die auch die wirtschaftlichen und beruflichen Beziehungen einer Person erfassen, unterliegt nicht diesem absoluten Schutz; die Verarbeitung personenbezogener Daten wird in diesen Fällen durch Rechtsvorschriften geregelt, die dem Grundsatz der Verhältnismäßigkeit genügen müssen: Je tiefer eine Information in den privaten Persönlichkeitsbereich eingreift, um so dringender muß das Anliegen der Gemeinschaft dazu sein und um so klarer muß die Befugnis zur Offenlegung normiert werden. Aber: Wer seinerzeit haupt- oder nebenamtlich für das MfS gearbeitet hat, war Helfer der diktatorischen Staatsmacht, mag er das auch in der Freizeit und noch so im Verborgenen getan haben: Seine Spitzeltätigkeit gehört nicht zu seiner Privat- und Individualsphäre. Deshalb ist die damalige Privatsphäre von heutigen Veröffentlichungen nicht betroffen.

Anders sieht es mit den heutigen Folgen aus, die sich aus der Veröffentlichung früherer MfS-Tätigkeit und ehemaliger Systemnähe ergeben: Es liegt in der Natur der Sache, daß die Mitarbeiter des MfS heute von den Nachwirkungen ihres amtlichen Verhaltens nun voll in ihrer Privat- und Individualsphäre getroffen werden. Wer damals im Auf-

trage staatlicher Institutionen die Menschenrechte verletzt hat, muß sich heute gefallen lassen, daß er dafür zur Rechenschaft gezogen wird. Diesen Grundsatz hat der Gesetzgeber im Stasi-Unterlagengesetz konkretisiert: Je herausgehobener die Funktion und je gemeiner das Verhalten des Mitarbeiters oder Begünstigten im Gefüge des Machtapparates war, je mehr ist von einem Interesse seiner Opfer und der Öffentlichkeit an einer Kenntnisnahme dieser Tatsachen auszugehen. Die - erst in zweiter Linie interessierende - Frage, ob jemand einem anderen geschadet hat, kann auch vom Täter selbst erst beurteilt werden, wenn alles offen zutage liegt.

Allerdings können Jugendlichkeit, besonders tragische Verstrickungen, z. B. Verpflichtungen unter Pressionen und Kompromaten, rechtzeitige und freiwillige Abkehr vom Spitzeldienst oder ernsthafte Bemühungen um Schadensbegrenzung und Wiedergutmachung einer Veröffentlichung im konkreten Fall entgegenstehen.

Ist dies aber nicht der Fall, so können folgende Kriterien Anlaß zu einer Veröffentlichung geben: Die gesellschaftliche oder berufliche Stellung des Täters in der DDR, Art, Umfang und Folgen der Tätigkeit (Zielrichtung, Zielpersonen, Nachhaltigkeit, Methode des Vertrauensgewinns, Art des Vertrauensverhältnisses, Nachteilsabsicht) sowie seine heutige gesellschaftliche oder berufliche Position.

Daß die Täter für sich selbst und vor Gleichgesinnten gute Entschuldigungen, subjektives Verständnis finden, sei ihnen unbenommen. All dies wurde jedoch vom Gesetzgeber als zu leicht befunden, um gegen eine Veröffentlichung zu sprechen. Nach einer Veröffentlichung ist es allerdings geboten, derartige persönliche Argumente mitzuempfinden und mit Gefühl und Nachsicht zu bewerten. Dazu gehört auch der indoktrinierte Glaube an die höheren Werte des Sozialismus und die von Gewissen und Skrupeln unberührte, aber der Staatsdoktrin entsprechende Meinung, man dürfe den Klassenfeind auch mit inhumanen Mitteln unschädlich machen. Wer über sein Gewissen nachdenkt, wird feststellen, daß er es sich nicht selbst verdankt.

Der Freistaat Sachsen hat - ausgehend vom Einigungsvertrag - in seiner Verfassung eine glasklare Regelung für die Feststellung der Verfassungstreue zum öffentlichen Dienst statuiert: In der Regel verdient ein informeller oder hauptamtlicher Mitarbeiter des MfS dieses Vertrauen nicht. Obwohl das Stasiunterlagengesetz die Mitarbeiter des Arbeitsgebietes 1 der DDR-Kriminalpolizei den Mitarbeitern der Stasi ausdrücklich gleichstellt, stehen mehr als 300 von ihnen in sächsischem Polizeidienst. Leider ist auch in Sachsen die Prüfung, wie weit systemnahe Personen, z. B. Auftraggeber der Stasi, ebenfalls für den heutigen öffentlichen Dienst ungeeignet sind, zu spät und nur halbherzig durchgeführt worden. „Sachzwänge“ sind da nicht immer eine hinreichende Erklärung.

Es ist an der Zeit, über den öffentlichen Dienst hinaus die Aufarbeitung der DDR dadurch voranzutreiben, sich - wie von Reichert vorbildlich geschehen - anderen Bereichen des öffentlichen Lebens im Hinblick auf Verantwortungsstrukturen

(darunter eben auch Stasimitarbeit und Verantwortungskontinuität) zuzuwenden: So hat der Verlag Gruner und Jahr für die von ihm übernommenen großen Tageszeitungen ebenfalls die Publikation einer wissenschaftlichen Arbeit von Prof. Kluge in Dresden zu diesem Thema angekündigt. Neben den Medien (auch dem öffentlich-rechtlichen Rundfunk) sollten weiterhin Gewerkschaften, Parteien, Verlage, private Kultureinrichtungen und weitere auf Öffentlichkeit hin orientierte Träger gesellschaftlicher Verantwortung bis hin zu großen Betrieben, Versicherungen und Banken wissenschaftlich erforscht werden. § 32 StUG und das Archivgesetz in Sachsen ermuntern zu solchen Arbeiten. Mich interessiert dabei auch, ob und wie Datensammlungen ihren Besitzer gewechselt haben und wie altes Herrschaftswissen in neu gewandeten Positionen nutzbar ist.

Wenn manche Menschen es schon nicht schaffen, sich zur eigenen Vergangenheit zu bekennen, dann müssen sie halt dulden, erkannt zu werden. Das ist oft mit Verlust von Ansehen, nicht selten mit beruflichen und familiären Einbußen verbunden. Die Gerechtigkeit nimmt dies in Kauf, weil es als Konsequenz der Revolution notwendig ist, die tragende Rolle der Funktionäre in den Machtstrukturen bloßzulegen.

Weil das von den Stasi-Mitarbeitern rechtswidrig gesammelte Wissen in Köpfen und Akten vorhanden ist, gebietet der Datenschutz, es offenzulegen und die Betroffenen über die zu ihrer Person gesammelten Informationen ins Bild zu setzen. Nur die Akteneinsicht durch die Opfer und die Veröffentlichung der Täter verhindert die Entstehung von Herrschaftswissen, so daß es nicht zu persönlichen Pressionen genutzt werden kann.

Dies dient nicht nur der Wahrheit, sondern ermöglicht einen differenzierten, abwägenden und auch barmherzigen Dialog, um den uns die östlichen Nachbarländer ausnahmslos beneiden. Nur in einer offenen Gesellschaft können Ressentiments offenbart und abgebaut und damit Informationen in den Dienst einer Versöhnung gestellt werden. Unsere Gesellschaft dürfte Bekenntnisse nicht wünschen, und die Rechtsordnung dürfte auch Täterschaften nicht offenlegen, wenn damit nicht die Chance auf Verzeihung verbunden wäre. Ein Pranger als schlichtes Rachewerkzeug wäre mit der Menschenwürde nicht vereinbar.

Um es klar zu sagen: Die Wahrheit über die Vergangenheit gehört ohne Wenn und Aber an's Licht. Nur dann kann das Verhalten des Einzelnen nach den Regeln der Verfassung offen, frei und verständnisvoll beurteilt werden. Der Datenschutz ist nicht dazu da, Unrecht zu verschweigen, wenn Opfer und Öffentlichkeit legitime Informationsansprüche haben.

Der mehr und mehr wachsende zeitliche Abstand muß allerdings auch zu der breiten Erkenntnis führen, daß Menschen sich ändern und daß die freiheitliche, auf einen staatlichen Unterdrückungsapparat verzichtende Gesellschaft in Europa solche persönlichen Entwicklungen wünscht, ermöglicht und ernst nimmt.

2 Parlament

Auf seine Bitte habe ich den Bewertungsausschuß des Sächsischen Landtags in der Frage beraten, ob und wieweit Informationen über eine mögliche Stasi-Vergangenheit von Landtagsabgeordneten veröffentlicht werden dürfen. Der Bewertungsausschuß leitet gemäß Art. 118 SächsVerf i. V. m. § 1 des Abgeordnetengesetzes dem Sächsischen Landtag eine Empfehlung zu, darüber zu entscheiden, ob vor dem Verfassungsgerichtshof eine Klage auf Aberkennung des Mandates erhoben wird. Selbstverständlich habe ich nicht - obwohl dies angesonnen wurde - darüber zu entscheiden, ob es verfassungswidriges Verfassungsrecht gibt und ob eine Aberkennung eines Mandats politisch sinnvoll ist. Meine Beratung betraf nur die Frage einer Offenlegung von Daten aus der politischen Vergangenheit; sie hatte sich am Wortlaut der Verfassung und den gesetzlichen Vorschriften zu orientieren. Das Verfahren ist dort im einzelnen geregelt. Demgemäß habe ich dafür votiert, daß der Bewertungsausschuß seine Ermittlungsergebnisse in den gebotenen Einzelheiten, die detaillierte und sicher auch peinliche, also sensible Daten enthalten, allen Abgeordneten (vertraulich und im verschlossenen Umschlag) mitzuteilen hat. Denn die Abgeordneten müssen sich ein lückenloses und abschließendes Bild darüber machen können, zu welchem Entscheidungsergebnis sie bezüglich einer Klage zum Verfassungsgerichtshof gelangen. Ich halte die entsprechende gesetzliche Regelung im Abgeordnetengesetz für geeignet und erforderlich, aber auch zumutbar. Dabei habe ich einkalkulieren müssen, daß vertrauliche Mitteilungen an freie Abgeordnete auch immer wieder publiziert werden.

3 Europäische Union / Europäische Gemeinschaft

Vgl. oben unter 1.

5 Inneres

5.1 Personalwesen

5.1.1 Gemeinsame Verwaltungsvorschrift der Sächsischen Staatskanzlei und der Sächsischen Staatsministerien zur Führung und Verwaltung von Personalakten für Angestellte, Arbeiter und die zur Ausbildung Beschäftigten im öffentlichen Dienst des Freistaates Sachsen

Immer wieder bestehen bei den sächsischen Behörden Unsicherheiten darüber, wie Personalakten von Arbeitnehmern zu führen und aufzubewahren sind. Bei Anfragen und Kontrollen habe ich stets empfohlen, die für den Bereich der Beamten geltende Verwaltungsvorschrift des SMI zur Führung von Personalakten vom 4. November 1993 als Vorbild zu nehmen, sofern kein zwingender rechtlicher Grund für eine Ungleichbehandlung von Arbeitnehmern und Beamten besteht (z. B. in Beihilfeangelegenheiten).

Um ungerechtfertigte Ungleichbehandlungen beim Umgang mit Personaldaten zu vermeiden, habe ich - wie im 4. Tätigkeitsbericht unter 5.1.2 angekündigt - beim SMI angeregt, die §§ 117 ff. SächsBG in § 31 Abs. 1 SächsDSG für entsprechend anwendbar zu erklären (wie dies teilweise in anderen Landesdatenschutzgesetzen vorbildlich geregelt ist). Nach meinem Dafürhalten ist es mit Art. 33 SächsVerf und der Forderung des Bundesverfassungsgerichts (BVerfGE 65, 1 ff.), Eingriffe in das Grundrecht auf informationelle Selbstbestimmung auf klare gesetzliche Grundlagen zu stellen, nicht vereinbar, daß der Umgang mit sensiblen Personalaktendaten im Arbeitnehmerbereich lediglich am Grundsatz der Erforderlichkeit (vgl. § 31 Abs. 1 SächsDSG) zu messen ist. Eine Reaktion auf meine Anregung steht noch aus.

Einen Schritt in die richtige Richtung stellt jedenfalls die o. g. Verwaltungsvorschrift dar, an deren Erarbeitung ich beteiligt war. Hiernach gilt die Verwaltungsvorschrift des SMI vom 4. November 1993 im wesentlichen für den Arbeitnehmerbereich entsprechend.

Gleichwohl halte ich - wie dargelegt - aus verfassungsrechtlichen Gründen und deswegen, weil die Verwaltungsvorschrift die Personalaktenführung lediglich im staatlichen Bereich (also nicht für die Kommunen, die Kammern, die Hochschulen etc.) verbindlich regelt, den Erlaß einer gesetzlichen Grundlage für unerläßlich.

5.1.2 Verwaltungsvorschrift des Sächsischen Staatsministeriums der Finanzen über die Dienstunfalluntersuchung gemäß § 45 Beamtenversorgungsgesetz im Rahmen der Dienstunfallfürsorge

Am Entwurf der o. g. Verwaltungsvorschrift wurde ich frühzeitig beteiligt. Schriftwechsel und konstruktive Gespräche mit dem SMF führten dazu, daß datenschutzrechtliche Defizite erkannt und beseitigt wurden.

Beispielsweise schreibt die Verwaltungsvorschrift die Verwendung eines Vordrucks für den Befundbericht des behandelnden Arztes vor, mit dem sensible Diagnosedaten des Verletzten erfaßt werden sollen. Auf meine Anregung hin wurde ein ausdrücklicher Hinweis für den Arzt aufgenommen, daß Angaben nur im erforderlichen Umfang und nur im Zusammenhang mit der Prüfung, ob ein Dienstunfall vorliegt, gemacht werden dürfen.

5.1.3 Verwaltungsvorschrift der Sächsischen Staatsregierung zur Prüfung der persönlichen Eignung im Beamtenverhältnis - Frage auch nach erfolglosen Anwerbeversuchen

In dem bisher verwendeten amtlich eingeführten Erklärungsbogen zur Prüfung der persönlichen Eignung im Beamtenverhältnis (SächsABl. 1995, S. 40) wird u. a. undifferenziert danach gefragt, ob der Betroffene durch das MfS/AfNS "zur Mitarbeit aufgefordert" wurde. Hierunter fallen auch erfolglose Anwerbeversuche.

Im Hinblick auf die jüngste Rechtsprechung des Bundesarbeitsgerichtes und des Sächsischen Oberverwaltungsgerichtes (BAG-Urt. vom 7. September 1995 - 8 AZR 828/93; SächsOVG Urt. vom 30. Oktober 1996 - 2 S 41/95) halte ich diese Frage für nicht mehr erforderlich. Den Urteilen zufolge besteht kein berechtigtes Interesse des Dienstherren, über erfolglose Anwerbungsversuche unterrichtet zu werden, weil die Frage der persönlichen Eignung für den öffentlichen Dienst hierdurch nicht berührt wird.

Im Interesse der Wahrung des Rechts der Betroffenen auf informationelle Selbstbestimmung habe ich die Behörden gebeten, künftig auf die Erhebung dieses Datums zu verzichten und die betreffende Frage auf den noch unverbrauchten Erklärungsbögen zu streichen.

Die Gespräche mit dem SMI zur Anpassung der Verwaltungsvorschrift dauern noch an.

5.1.4 Personalinformationssysteme

In der öffentlichen Verwaltung wird die Personalverwaltung und Personalwirtschaft zunehmend mit *Personalinformationssystemen* unterstützt. Im Berichtszeitraum wurde ich gemäß § 31 Abs. 7 SächsDSG an der Einführung einer Vielzahl von automatisierten Verfahren beteiligt, zu denen ich meine Stellungnahme abgegeben habe.
Weil in den mir vorgelegten Verfahrenskonzepten vielfach die für eine sachgerechte Prüfung nach § 31 Abs. 7 SächsDSG erforderlichen Unterlagen nicht vollständig waren (siehe meine Bekanntmachung vom 10. Dezember 1992 - SächsABl. 1993, S. 50), sei im folgenden nochmals auf einige Schwerpunkte hingewiesen:

Grundsätzlich dürfen Beschäftigtendaten nur verarbeitet werden, soweit dies zur Eingehung, Durchführung oder Beendigung des Dienst- oder Arbeitsverhältnisses erforderlich ist oder ein Gesetz, ein Tarifvertrag oder eine Dienstvereinbarung dies vorsieht. Dies gilt auch für Daten Dritter, denen Rechte aus dem Dienst- und Arbeitsverhältnis zustehen (§ 31 Abs. 1 SächsDSG).

Der *Verfahrenszweck* muß eindeutig sein und ist schriftlich festzulegen (entweder in der erforderlichen Dienstvereinbarung selbst oder in einer genauen und vollständigen *Verfahrensbeschreibung*, die Bestandteil der Dienstvereinbarung ist). Die Verfahrensbeschreibung muß Aufschluß über *mögliche und tatsächliche Auswertungen* geben und die (in der Regel unzulässige) Verknüpfung mit anderen Verfahren dokumentieren. Dazu gehört auch die genaue *Beschreibung* der für die Speicherung vorgesehenen (personenbezogenen) *Datensätze bis auf Feldebene*, die sich am Grundsatz der Erforderlichkeit auszurichten haben. Auf die strenge *Zweckbindung von Personalaktendate*n, die sich aus § 31 i. V. m. § 12 SächsDSG und § 117 ff. SächsBG (insbesondere § 124 SächsBG) ergibt, weise ich besonders hin. Danach dürfen Personalaktendaten ausschließlich für Zwecke der Personalverwaltung und Personalwirtschaft verwendet werden. Ferner ist bei der Übernahme der Daten auf das Personalinformationssystem zu beachten, daß das Zugangsrecht auf die Beschäftigten zu beschränken ist, die im Rahmen der Personalverwaltung mit der Bearbeitung von Personalangelegenheiten beauftragt sind (§ 117 Abs. 3 SächsBG). Die Berechtigten sind nach § 6 SächsDSG schriftlich auf das Datengeheimnis zu verpflichten (siehe meine Bekanntmachung vom 22. Juli 1993 - SächsABl. S. 970).

Ein Personalverwaltungssystem, das automatisiert Personaldaten verarbeitet, ermöglicht gegenüber der manuellen Personaldatenverwaltung eine erhöhte Verfügbarkeit, Verknüpfbarkeit, schnellere Auswertungsmöglichkeiten der gespeicherten Informationen, bringt aber auch ein erhöhtes Risiko des Datenmißbrauchs mit sich. Daher sind für den Einsatz automatisierter Verfahren die Anforderungen an ein Datenschutz- und Datensicherheitskonzept gemäß § 9 SächsDSG sehr hoch (siehe meine Bekanntmachung vom 30. Juni 1994 - SächsABl. S. 979). Darin ist u. a. festzulegen, welche personellen, technischen und organisatorischen Sicherungsmaßnahmen für den Schutz der zu verarbeitenden Personalaktendaten *sinnvoll, zweckmäßig und ausreichend* sind. Aus datenschutztechnischer Sicht sind die Forderungen nach *der räumlichen Sicherheit, dem Paßwortverfahren, der Vergabe von Zugangs- und Benutzerrechten und der Protokollierung* (vgl. meinen 3. Tätigkeitsbericht unter 14.2) besonders wichtig. Sollten Wartungs- und Pflegearbeiten der Hard- und Software durch Privatfirmen ausgeführt werden, muß (z. B. vertraglich) ausgeschlossen werden, daß das Wartungspersonal dabei auf personenbezogene Daten zugreift. So ist auch in der Testphase der Software zu verfahren. Hier können datenschutzrechtliche Probleme vermieden werden, wenn Testdaten, die zum Beispiel durch eine ausreichende Anonymisierung von Echtdaten erzeugt werden können, zum Testen der Software genutzt werden.

Als Grundlage für die Erstellung des erforderlichen Dateien- und Geräteverzeichnisses gemäß § 10 SächsDSG dient meine Bekanntmachung vom 29. September 1993 (SächsABl. S. 1175). Das Verfahren muß auch so gestaltet werden, daß die Rechte der Beschäftigten auf Einsicht in und Auskunft über ihre gespeicherten Daten (§ 31 Abs. 3 SächsDSG, § 124 Abs. 5 SächsBG) gewahrt bleiben.
Werden für die Erstellung der Verfahrensdokumente "Musterdienstvereinbarungen" zu Hilfe genommen, gebe ich zu bedenken, daß sich das "eigene" Verfahren immer an den *tatsächlichen Gegebenheiten* (z. B. vorhandene Verfahrensorganisation, Hard- und Software) orientieren muß. Werden die einzelnen Maßnahmen aus dem Muster einfach nur übernommen, besteht die Gefahr, daß das Datensicherheitskonzept lückenhaft und die Umsetzung der Maßnahmen zur Gewährleistung des Datenschutzes nach § 9 SächsDSG nicht in ihrer Gesamtheit sichergestellt werden kann. Gemäß § 31 Abs. 7 Satz 2 SächsDSG ist meine Stellungnahme der zuständigen Personalvertretung im Rahmen des personalvertretungsrechtlichen Beteiligungsverfahrens zuzuleiten.

5.1.5 Zeiterfassung mit dem Arbeitsplatzcomputer

Wie in den vergangenen Jahren wurde ich gemäß § 31 Abs. 7 SächsDSG an der Einführung vieler Verfahren der automatisierten Arbeitszeiterfassung beteiligt (siehe dazu auch den vorstehenden Abschnitt).
In einem Fall wurde mir nachträglich ein Verfahren angezeigt, in dem die Behörde die personenbezogenen Daten, die automatisch bei der Systemprotokollierung (An- und Abmeldezeiten am System) am Arbeitsplatzcomputer entstehen, als Arbeitszeitdaten nutzt. Ein zusätzliches Programm macht die Protokolldaten für die Beschäftigten in Form eines "Arbeitszeiterfassungsbogens" lesbar. Der Systemverwalter ist gleichzeitig auch Gleitzeitbeauftragter.
Ich habe der Behörde mitgeteilt, daß personenbezogene Protokolldaten einer besonderen Zweckbindung unterliegen. Gemäß § 12 Abs. 4 SächsDSG dürfen personenbezogene Daten, die ausschließlich zum Zweck der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage gespeichert werden, *nur für diesen Zweck* und hiermit in Zusammenhang stehende Maßnahmen gegenüber Bediensteten genutzt werden. Dies hat zur Folge, daß Protokolldaten nicht für eine Verhaltens- und Leistungskontrolle, die mit einem Zeiterfassungsverfahren verbunden wäre, zweckentfremdet werden dürfen. Die Zweckbindung des § 12 Abs. 4 SächsDSG kann auch durch eine Dienstvereinbarung nicht aufgehoben werden. Abgesehen davon begegnen der praktizierten PC-Lösung auch im Hinblick auf § 117 Abs. 3 SächsBG bezüglich der Doppelfunktion des Systemverwalters datenschutzrechtliche Bedenken (Interessenkollision).

Da außerdem die Erfassung der Arbeitszeit in dem geschilderten Fall am Arbeitsplatz (Arbeitsplatzcomputer) erfolgt, wäre das Verfahren auch an § 15 Abs. 7 BAT-O zu messen gewesen (vgl. BAG-Urteil vom 18. Januar 1990 - 6 AZR 386/89). Danach beginnt und endet die Arbeitszeit an der Arbeitsstelle (z. B. im Eingangsbereich der Behörde).

Ich habe die Einstellung dieses Arbeitszeiterfassungs-Verfahrens gefordert und gebeten, mich bei der Einführung eines neuen und datenschutzgerechten Verfahrens rechtzeitig gemäß § 31 Abs. 7 SächsDSG zu beteiligen.

5.1.6 Löschung von Arbeitszeiterfassungsdaten in automatisierten Verfahren

Den Hinweis in meinem 4. Tätigkeitsbericht (5.1.19), im Interesse einer einheitlichen Behandlung von Arbeitern, Angestellten und Beamten die erfaßten Arbeitszeitdaten maximal *sechs* Monate aufzubewahren (und dann zu löschen), kann ich wegen der in § 16 Abs. 2 Satz 2 ArbZG vorgeschriebenen *zweijährigen Aufbewahrungsfrist* nicht aufrecht erhalten. Die relativ lange Aufbewahrungszeit ist Teil des Arbeitnehmerschutzes und soll die Aufsichtsbehörden (Gewerbeaufsicht) in die Lage versetzen, die Einhaltung der Vorschriften nach dem ArbZG zu kontrollieren. Verstöße gegen die vorgeschriebene Zweijahresfrist können gemäß § 22 Abs. 1 Nr. 9 und Abs. 2 ArbZG i. V. m. § 31 Abs. 2 Nr. 2 OWiG als Ordnungswidrigkeit mit einer Geldbuße bis zu 30.000 DM geahndet werden.

Die Praxis zeigt, daß es mit den automatisierten Arbeitszeiterfassungsverfahren möglich ist, über die reine Zeiterfassung hinaus Auswertungen bezogen auf einzelne Mitarbeiter oder Mitarbeitergruppen unter mehreren Gesichtspunkten zu erstellen. Die umfangreichen Möglichkeiten der eingesetzten Systeme ermöglichen es z. B., aus den Zeitwertdaten Abwesenheits-, Urlaubs- und Krankheitslisten, Listen der "Kernzeitverletzer", Monatslisten und Tagesspiegel zu erstellen und zu speichern.

Deshalb ist in den erforderlichen Dienstvereinbarungen konkret festzulegen, welche Zeitwertdaten der zweijährigen Aufbewahrung nach § 16 Abs. 2 ArbZG unterliegen sollen. Aus datenschutzrechtlicher Sicht empfehle ich, ausschließlich die automatisiert gespeicherten Zeitwertdaten (nicht zuletzt aus Gründen der Datensicherheit und der besseren Speicher- und Abrufkontrolle) zwei Jahre lang im System zu speichern und danach zu löschen. Sonstige Auswertungen (manuelle Auswertungen, z. B. Korrekturlisten und Tagesspiegel) sind nach Aufgabenerledigung (§ 19 Abs. 1 Nr. 2 SächsDSG), spätestens jedoch nach *sechs* Monaten zu vernichten, es sei denn, daß besondere Umstände (z. B. Arbeitsrechtsstreit) eine längere Aufbewahrung im Einzelfall erforderlich machen.

5.1.7 Personaldatenverarbeitung der Innungskrankenkassen durch private Auftragnehmer

Mehrere sächsische Innungskrankenkassen (IKK) haben die Lohn- und Gehaltsrechnung für ihre Beschäftigten bisher (als sogenannte Untermandanten des IKK-Landesverbandes Baden-Württemberg) bei einem privaten Unternehmen für Datenverarbeitung in Stuttgart ausführen lassen. Mit der angestrebten Einzelmandantenlösung haben sich der IKK-Landesverband Sachsen und die Innungskrankenkassen (aus wirtschaftlichen Erwägungen und wegen der Fachkompetenz des Unternehmens) entschieden, die Auftragsdatenverarbeitung nach §

7 SächsDSG mit dem privaten Unternehmen fortzuführen (was nicht per se unzulässig ist). In meiner Stellungnahme habe ich die Kassen jedoch darauf hingewiesen, daß besondere Voraussetzungen zu erfüllen sind, ehe ihrer Natur nach besonders schutzwürdige Beschäftigtendaten durch ein privates Unternehmen, das sich darüber hinaus in einem anderen Bundesland befindet, im Auftrag verarbeitet werden.

Nach § 7 SächsDSG ist der *Auftraggeber* für die Einhaltung des Datenschutzgesetzes und anderer Vorschriften über den Datenschutz verantwortlich. Er hat gemäß § 7 Abs. 2 SächsDSG den Auftragnehmer (das private Datenverarbeitungsunternehmen) unter besonderer Berücksichtigung der Eignung der von diesem getroffenen personellen, technischen und organisatorischen Maßnahmen (vgl. auch § 9 SächsDSG) *sorgfältig* auszuwählen.

Aus den mir übersandten Unterlagen vermochte ich nicht zu erkennen, aufgrund welcher Feststellungen die *sorgfältige* Auswahl der Stuttgarter Firma getroffen worden war. Nur durch ausreichende personelle, technische und organisatorische Maßnahmen, von denen sich der *Auftraggeber* zu überzeugen hat und die darüber hinaus *vertraglich festzulegen* sind, kann eine ordnungsgemäße Auftragsdatenverarbeitung gewährleistet werden. Die mir übersandten Verträge genügten jedenfalls nicht in allen Punkten meiner Bekanntmachung vom 3. November 1993 zur Datenverarbeitung im Auftrag (SächsABl. S. 1304).

Ich habe auf folgende datenschutzrechtliche Schwerpunkte der *Vertragsgestaltung* hingewiesen:

Ein *Datenschutz- und Datensicherheitskonzept* ist vom Auftragnehmer, als Teil des schriftlichen Vertrages, vorzulegen. Da der Auftragnehmer Datenverarbeitung für eine sächsische öffentliche Stelle erledigt, müssen die *Beschäftigten des Auftragnehmers* auf das Datengeheimnis gemäß § 6 SächsDSG schriftlich verpflichtet werden. Die Verarbeitung personenbezogener Daten darf nur nach Weisung der IKK erfolgen. Der Auftraggeber muß im einzelnen und abschließend vertraglich bestimmen, welche Personaldaten dem privaten Unternehmen zur Verfügung zu stellen sind und welche Verarbeitungsschritte dort vorgenommen werden dürfen. Für den Fall, daß Datenschutzvorschriften oder vertragliche Regelungen z. B. mit Schadensfolge verletzt werden, sind Vertragsstrafen zu vereinbaren. Für wichtig halte ich auch die Klausel, daß dem Auftragnehmer bei Datenschutzverstößen die fristlose Kündigung droht.

Ich empfehle, daß der Auftragnehmer sich vertraglich der Kontrolle des Sächsischen Datenschutzbeauftragten unterwirft. Hat zum Beispiel der externe Verarbeiter seinen Sitz in einem anderen Bundesland, oder erfolgt die Datenverarbeitung in unterschiedlichen unternehmenseigenen Rechenzentren (auch Subunternehmen), lassen sich sonst meine Kontrollrechte nur schwer realisieren. In diesen Fällen kommt der Vertragsgestaltung besondere Bedeutung zu. In Abschnitt 5.5.2 des 3. Tätigkeitsberichtes habe ich zusätzliche schriftliche Vereinbarungen für eine datenschutzgerechte Vertragsgestaltung empfohlen.

5.1.8 Verwendung datenschutzgerechter Personalbögen

Das SMI hat den Inhalt des datenschutzgerechten Personalbogens (vgl. 4. Tätigkeitsbericht 5.1.7) überarbeitet. Weil Angaben über Ehegatten und Kinder aus den Unterlagen im Einstellungsverfahren hervorgehen, habe ich angeregt, künftig auf die *Ehegattendaten* im Personalbogen grundsätzlich zu verzichten. Für die *Kinderdaten* sollte eine Fußnote darauf hinweisen, daß hier Angaben nur zu machen sind, sofern die Kinder noch im Haushalt des Bewerbers bzw. Bediensteten leben und soweit sich die Angaben auf Kindergeld und Ortszuschlag auswirken. In solchen Fällen genügt es, das *Geburtsjahr* einzutragen. In allernächster Zeit sollte der überarbeitete Personalbogen für Beamte, Angestellte und Arbeiter durch das SMI bekannt gemacht und dessen Verwendung allgemein empfohlen werden.

Bei der datenschutzrechtlichen Bewertung von Personalbögen anderer Behörden mußte ich immer wieder feststellen, daß die bisher verwendeten oder neu entwickelten Vordrucke mit dem vom SMI konzipierten (und mit mir abgestimmten) und im Sinne von § 31 Abs. 1 SächsDSG datenschutzgerechten Personalbogen für Beamte, Angestellte und Arbeiter, oftmals nicht übereinstimmen.

So werden zum Beispiel in den vom SMJus entwickelten Personalbögen für Beamte (Richter) sowie für Angestellte und Arbeiter für die Eingehung, Durchführung oder Beendigung des Dienst- oder Arbeitsverhältnisses nicht erforderliche Daten des Bewerbers bzw. Bediensteten und dessen Familienangehöriger erhoben (z. B. Fragen nach den Daten *verwitwet seit, geschieden seit, wiederverheiratet seit, Orden und Auszeichnungen, nicht bestandene Prüfungen und Wiederholungsprüfungen).* Die Erhebung solcher Daten habe ich bereits in der Vergangenheit wegen offensichtlich mangelnder Erforderlichkeit beanstandet (vgl. unter 5.1.5 bzw. 5.1.7 im 1. bzw. 4. Tätigkeitsbericht). Nachdrücklich habe ich angeregt, den vom SMI konzipierten Personalbogen analog auch im Bereich der Justiz zu verwenden. Besonderheiten für das Justizpersonal, die ein Abweichen vom SMI-Personalbogen erforderlich machen könnten, vermochte ich nicht festzustellen. Meine Verhandlungen mit dem SMJus dauern noch an.

5.1.9 Datenerhebung vor einer Aufnahme in den Juristischen Vorbereitungsdienst

Vor einer Aufnahme in den juristischen Vorbereitungsdienst werden von den Bewerbern auf einem vom SMJus verbindlich vorgegebenem Formblatt u. a. Angaben zu Ermittlungsverfahren *in der Vergangenheit* und zu bloßen, d. h. erfolglos gebliebenen Anwerbungsversuchen des MfS/AfNS verlangt. Weiterhin wird undifferenziert nach dem derzeitigen Wohnsitz der Eltern gefragt, was verwundert, weil angehende Referendare volljährig sind.

Dem SMJus habe ich mitgeteilt, daß zum einen nach der SächsJAPO für die Frage der Ablehnung eines Bewerbers ausschließlich entscheidend ist, ob gegen ihn *derzeit* ein Ermittlungsverfahren läuft. Zu Ermittlungsverfahren in der Vergangenheit gilt: Entweder ist das Verfahren eingestellt oder es ist eine geringfügige und deshalb unbeachtliche Strafe ergangen, oder es ist eine Vorstrafe im Bundeszentralregister eingetragen, aus dem ohnehin ein Auszug angefordert wird.

Zum andern dürfen aus bloßen Anwerbungsversuchen des MfS/AfNS nach der Rechtsprechung des OVG Bautzen (Urteil vom 13.12.1996, Az: 2 S 41/95) keine Rückschlüsse auf die Nichteignung für eine Beschäftigung im öffentlichen Dienst gezogen werden. Art. 119 Abs. 2 SächsVerf stellt ausdrücklich nur auf die *Tätigkeit* für die genannten Stellen ab.

Schließlich ist bei der Frage nach dem elterlichen Wohnsitz (Angabe des Ortes) zu beachten, daß nach § 38 Abs. 2 Satz 2 SächsJAPO die Aufnahme des Referendardienstes grundsätzlich an einem Ort erfolgen soll, mit dem der Bewerber durch längeren Familienwohnsitz verbunden ist. Dies rechtfertigt allerdings nicht die undifferenzierte Frage nach dem Wohnsitz der Eltern.

Eine abschließende Stellungnahme des SMJus steht noch aus.

5.1.10 Datenschutz und Anhörungsrechte

Die Vorschrift des § 78 Abs. 2 und 3 SHEG (inzwischen außer Kraft) sah zur Frage, ob Hochschullehrer der DDR nach der Wiedervereinigung für eine Weiterbeschäftigung im Hochschuldienst geeignet sind, ein Anhörungsrecht der Betroffenen vor. Ein ehemaliger Hochschullehrer teilte mit, daß die nach dem Hochschulerneuerungsgesetz eingesetzte Personalkommission seine Eignung *ohne Anhörung* verneint habe und bat mich um datenschutzrechtliche Bewertung.

Der mit dem Sachverhalt konfrontierte Mitarbeiter des SMWK hat - im Gegensatz zu früheren Fällen - eine (inhaltliche) Stellungnahme mit dem Hinweis abgelehnt, ich sei für die Kontrolle der Einhaltung gesetzlich gewährter Anhörungsrechte nicht zuständig, weil es sich hierbei nicht um datenschutzrechtliche Vorschriften nach dem Sächsischen Datenschutzgesetz handele. Hier rate ich zum berühmten Blick ins Gesetz; er erleichtert die Rechtsfindung.

Nach Art. 57 SächsVerf wird der Datenschutzbeauftragte zur *Wahrung des Rechts auf Datenschutz* berufen. Dieser verfassungsrechtliche Auftrag erfährt durch § 24 Abs. 1 SächsDSG eine Konkretisierung: Hiernach hat der Sächsische Datenschutzbeauftragte, die Einhaltung des Sächsischen Datenschutzgesetzes und *anderer Vorschriften über den Datenschutz* zu kontrollieren. Die Kontrollkompetenz des Datenschutzbeauftragten ist also keineswegs nur auf die Auffangvorschriften des SächsDSG beschränkt, sondern erstreckt sich auf jeglichen Umgang mit personenbezogenen Daten bei sächsischen öffentlichen Stellen. "Andere Vorschriften über den Datenschutz" sind u. a. auch

die gesetzlich gewährten Anhörungsrechte, also z. B. § 78 Abs. 2 und 3 SHEG (vgl. 1. Tätigkeitsbericht unter 5.1.9). Dies basiert auf folgenden Überlegungen:

Im rechtsstaatlichen Anhörungsverfahren ist dem Betroffenen der aus Sicht der Behörde entscheidungserhebliche Sachverhalt (der stets weitestgehend aus personenbezogenen Daten des Betroffenen besteht) mitzuteilen. Anschließend erhält er das Recht, sich zu dem Sachverhalt zu äußern. Die Behörde ist gegenüber dem Betroffenen verpflichtet, sein Vorbringen bei ihrer Entscheidung zu berücksichtigen (vgl. BVerwGE 66, 114).

Diese Rechte lassen sich nach dem Volkszählungsurteil des Bundesverfassungsgerichts (BVerfGE 65, 1 ff.) unmittelbar aus dem Grundrecht auf informationelle Selbstbestimmung ableiten. Nach dieser für alle öffentlichen Stellen verbindlichen Entscheidung setzt informationelle Selbstbestimmung zwingend voraus, daß der Einzelne die Möglichkeit erhalten muß, zu wissen, welche ihn betreffenden Informationen bei welchen Stellen bekannt sind (vgl. BVerfGE 65, 42 f.). Dies bedeutet die Begründung eines Anspruchs auf Mitteilung des personenbezogenen Sachverhalts (erste Phase des Anhörungsverfahrens). Außerdem ist anerkannt, daß das "Recht auf Information im Anhörungsverfahren" insbesondere durch Akteneinsicht verwirklicht werden kann (vgl. Wassermann, AK zum GG, Art. 103 Rdnr. 25). Unbestritten haben Akteneinsichtsrechte (siehe z. B. § 17 SächsDSG) einen unmittelbaren datenschutzrechtlichen Bezug. Auch dies ist ein Indiz dafür, daß Anhörungsverfahren der Kontrollkompetenz des Sächsischen Datenschutzbeauftragten unterliegen.

Weiterhin kann auch das Recht des Betroffenen auf Äußerung und Berücksichtigung seines Vorbringens bei der behördlichen Entscheidung (zweite und dritte Phase des Anhörungsverfahrens) - wie z. B. auch der Berichtigungsanspruch nach § 18 SächsDSG - aus dem Grundrecht auf informationelle Selbstbestimmung hergeleitet werden. Datenschutzrechtlich ausgedrückt bedeutet dieser Anspruch, daß der Betroffene das Recht hat, auf die Verarbeitung (Nutzung, Verwendung) seiner personenbezogenen Daten klarstellend und entlastend Einfluß zu nehmen (z. B. die entscheidungsbefugte Stelle hält den Betroffenen zunächst für ungeeignet, ändert ihre Meinung aber aufgrund der Anhörung).

Nach alledem bleibt festzuhalten, daß eine unterlassene Anhörung immer das Recht auf informationelle Selbstbestimmung beeinträchtigt und daher die Einhaltung gesetzlich vorgeschriebener Anhörungsrechte vom Sächsischen Datenschutzbeauftragten kontrolliert werden kann.

5.1.11 Anhörung vor Aufnahme ungünstiger Bewertungen in die Personalakte

Bei Einsicht in seine Personalakte stellte ein Beamter fest, daß sein Vorgesetzter mit Bleistift auf der Rückseite einer zur Personalakte genommenen Beschwerde das Wort „Querulant“ vermerkt hatte.

Unabhängig davon, ob eine solche allgemeine und nicht näher begründete Bewertung überhaupt zulässig ist, lag auf jeden Fall ein Verstoß gegen § 119 SächsBG vor. Hiernach ist der Beamte zu Bewertungen, die für ihn ungünstig sind oder ihm nachteilig werden können, vor deren Aufnahme in die Personalakte zu hören.

Der Betroffene hat mir inzwischen mitgeteilt, daß sein Vorgesetzter das Wort ausradiert und zugesagt hat, die Rechtslage künftig zu beachten.

5.1.12 Datenerhebung im Vorstellungsgespräch

Die immer wiederkehrende Frage, welche personenbezogenen Daten eine Behörde im Vorstellungsgespräch von Stellenbewerbern erheben darf, veranlaßten mich, auf folgendes hinzuweisen:

Art. 33 Abs. 2 GG, Art. 91 Abs. 2 SächsVerf nennen drei Kriterien für den Zugang zu öffentlichen Ämtern, nämlich: *Eignung, Befähigung* und *fachliche Leistung*. Daher sind nur solche Fragen zur Eingehung eines Beschäftigungsverhältnisses erforderlich i. S. v. § 31 Abs. 1 SächsDSG, die Rückschlüsse auf diese drei Kriterien zulassen oder - wie es das Bundesarbeitsgericht ausdrückt - an denen der mögliche Arbeitgeber ein objektiv gerechtfertigtes Interesse zur Beurteilung des Bewerbers hat (vgl. BAG CR 1987, 372). Es bestehen daher keine Bedenken gegen Fragen zu abgelegten Prüfungen, beruflichen Kenntnissen oder zur Schul- und Berufsausbildung. Auch Fragen nach Allgemeinwissen oder psychologischer Test sind erlaubt, letztere natürlich nur in der gebotenen Achtung des Persönlichkeitsrechts. Grundsätzlich zulässig ist ebenfalls die Frage nach einer Schwerbehinderung (vgl. BAG NJW 1994, 1363 ff.). Im Lichte des Art. 119 SächsVerf sogar geboten sind Fragen nach MfS-/AfNS-Mitarbeit und systemnahen Tätigkeiten in der DDR.

Die Frage nach der Schwangerschaft ist nur ausnahmsweise zulässig: Sie ist erlaubt, wenn sie objektiv dem gesundheitlichen Schutz des ungeborenen Kindes dient (z. B. bei Bewerberinnen für eine Stelle im Krankenhaus, wenn die Arbeit den Umgang mit infektiösem Material erfordert - vgl. BAG NJW 1994, 148 f.) oder wenn die Schwangerschaft der Ausübung der Arbeit objektiv entgegensteht (z. B. Berwerbung als Tänzerin für den Zeitraum eines Jahres). Von solchen Ausnahmefällen abgesehen ist die Frage nach einer Schwangerschaft unerlaubt.

Wegen des sehr weiten Begriffs der Eignung (er erfaßt die ganze Person mit ihren körperlichen und charakterlichen Eigenschaften) ist es nicht möglich, einen abschließenden Katalog von Daten zu nennen, die zulässigerweise im Vorstellungsgespräch erhoben werden dürfen.

Für die Begründung eines Beschäftigungsverhältnisses generell nicht erforderlich und daher unzulässig sind Fragen nach bevorstehender Heirat, Intimleben oder Partei- bzw. Gewerkschaftszugehörigkeit.

Zur Frage nach Vorstrafen und Ermittlungsverfahren siehe 3. und 4. Tätigkeitsbericht jeweils unter 5.1.3.

5.1.13 Regelbeurteilung von Angestellten

Im Berichtszeitraum hat das SMF eine Verwaltungsvorschrift über die dienstliche Beurteilung der Angestellten im Geschäftsbereich des SMF erlassen, die (analog zur Beurteilung der Beamten) eine regelmäßige Beurteilung der Angestellten im Abstand von drei Jahren vorsieht.

Hiergegen habe ich keine datenschutzrechtlichen Bedenken erhoben.

Zwar habe ich in der Vergangenheit Zweifel an der Zulässigkeit von Regelbeurteilungen für Angestellte geäußert (vgl. 4. Tätigkeitsbericht 5.1.14). Ein intensiver Meinungsaustausch mit dem SMF und die Rechtsprechung des Bundesarbeitsgerichts (Urteil vom 10. März 1989 - 5 AZR 927/79, BAGE 38, 141) haben mich jedoch davon überzeugt, daß die regelmäßige Beurteilung von Angestellten mit dem Erforderlichkeitsgrundsatz vereinbar ist. Ausschlaggebend für diese (neue) Auffassung war insbesondere das Argument, daß der Anspruch des ausscheidenden Angestellten auf Erteilung eines qualifizierten Zeugnisses (vgl. § 630 Satz 2 BGB) nur erfüllt werden kann, wenn sich aus der Personalakte die dienstliche Entwicklung des Angestellten erkennen läßt. Verläßliche und belegbare Aussagen zu dieser Entwicklung sind nur möglich, wenn die Betroffenen in vernünftigen zeitlichen Abständen beurteilt werden.

5.1.14 Verwendung von Erklärungen über den Ortszuschlag ("OSA" - Erklärung)

Der Ortszuschlag (künftig Familienzuschlag) ist für Beschäftigte im öffentlichen Dienst Bestandteil der Vergütung. Für die Zuordnung zu einer Stufe des Ortszuschlags sind die Familienverhältnisse maßgebend. Verheirateten Beschäftigten steht lediglich die Hälfte des Ortszuschlags zu, wenn der Ehegatte ebenfalls im öffentlichen Dienst tätig ist. Um dies feststellen zu können, werden die Beschäftigten von der jeweiligen Bezügestelle aufgefordert, in "OSA"- Erklärungen Namen und Anschrift des Arbeitgebers des Ehegatten mitzuteilen. Die Bezügestelle setzt sich dann per Formblatt (sog. Vergleichsmitteilung) mit dem Arbeitgeber des Ehegatten in Verbindung, um festzustellen, ob er Vergütungen nach dem BAT-O leistet. Dabei werden in den Vergleichsmitteilungen alle Beschäftigtendaten, die der Ortszuschlagsberechnung zugrunde liegen (z. B. detaillierte Angaben über Namen, Vornamen, Geburtsdatum des Beschäftigten, über das Arbeitsverhältnis, Wochenstunden, Erziehungsurlaub) an den Arbeitgeber des Ehegatten übermittelt, und zwar auch dann, wenn es sich bei diesem um ein Privatunternehmen handelt. So erhielten in einem Fall nicht nur der private Arbeitgeber Kenntnis von den personenbezogenen Daten des Bediensteten, sondern auch dessen Mitarbeiter und der Steuerberater des Unternehmens.

Dem SMF und dem LfF machte ich deutlich, daß sich dieses Verfahren mit § 31 Abs. 2

Satz 1 SächsDSG und § 121 Abs. 2 SächsBG (danach ist eine Übermittlung der Daten von öffentlich Bediensteten an Personen oder Stellen außerhalb des öffentlichen Bereiches nur auf gesetzlicher Grundlage oder mit Einwilligung der Betreffenden zulässig) wohl kaum vereinbaren läßt, und ich habe als milderes Mittel vorgeschlagen, von den Betroffenen eine Bestätigung des Arbeitgebers des jeweiligen Ehegatten beibringen zu lassen, aus der hervorgeht, ob Vergütung nach BAT-O bezahlt wird oder nicht.

Das SMF lehnte diesen Vorschlag mit dem Hinweis ab, daß das kritisierte Vergleichsmitteilungsverfahren aufgrund einer Verwaltungsvorschrift des Bundes bundeseinheitlich durchzuführen sei und eine Änderung der Praxis deshalb in die Zuständigkeit des BMI fiele.

Meinen Feststellungen zufolge steht die Verwaltungsvorschrift des Bundes jedoch meinem Vorschlag nicht entgegen. In ihr ist geregelt, daß Vergleichsmitteilungen *erst* in den Fällen bestehender Anspruchskonkurrenz auszutauschen sind, wenn also bereits *feststeht*, daß auch dem Ehegatten des Betroffenen der (halbe) Ortszuschlag zustehen würde.

Eben diese Feststellung kann durch die Beibringung der von mir vorgeschlagenen Bescheinigung getroffen werden, um sodann das Vergleichsmitteilungsverfahren in Gang zu setzen. Hierfür ist jedoch eine Rechtsgrundlage erforderlich (die Verwaltungsvorschrift reicht nicht aus), die den Grundsätzen des Volkszählungsurteils (BVerfGE 65, 1 ff.) entspricht. Danach bedürfen Einschränkungen des Rechts auf informationelle Selbstbestimmung nach Art. 2 Abs. 1 GG einer (verfassungsmäßigen) gesetzlichen Grundlage, aus der sich die Voraussetzungen und der Umfang der Beschränkungen klar und für den Bürger erkennbar ergeben und die damit dem rechtsstaatlichen Gebot der Normenklarheit entspricht. Dabei muß der Grundsatz der Verhältnismäßigkeit beachtet werden. Dieser mit Verfassungsrang ausgestattete Grundsatz folgt bereits aus dem Wesen der Grundrechte selbst, die als Ausdruck des allgemeinen Freiheitsanspruchs des Bürgers gegenüber dem Staat von der öffentlichen Gewalt jeweils nur soweit beschränkt werden dürfen, als es zum Schutz öffentlicher Interessen *unerläßlich* ist.

Das SMF hat die Problematik dem BMI vorgetragen, damit sich der Arbeitskreis für Besoldungsfragen, der unter der Federführung des BMI steht, um eine gesetzliche Regelung für das Vergleichsmitteilungsverfahren bemüht.

Ich setzte mich dafür ein, daß bis zur Schaffung der erforderlichen Rechtsgrundlage für das Vergleichsmitteilungsverfahren meinem o. a. Vorschlag entsprechend verfahren wird.

5.1.15 Übermittlung personenbezogener Lehrerdaten von den Oberschulämtern an das SMK

Ein Lehrerhauptpersonalrat teilte mit, daß das SMK wegen der rückläufigen

Schülerzahlen an den Grundschulen beabsichtige, durch Aufhebungsverträge den Personalüberhang sozialverträglich zu mindern. In diesem Zusammenhang seien die Oberschulämter angewiesen worden, dem SMK in bestimmten Zeitabständen die Anzahl der ausgeschiedenen Lehrkräfte unter Angabe folgender Daten zu melden: Staatliches Schulamt, Schule, Name, Geschlecht, Lebensalter, Fächerkombination, Schuljahre, Höhe der Abfindungssumme, Zeitpunkt des Ausscheidens.

Unter Hinweis auf § 31 Abs. 1 SächsDSG (danach dürfen öffentliche Stellen Beschäftigtendaten nur verarbeiten, soweit dies zur Eingehung, Durchführung oder Beendigung des Dienst- oder Arbeitsverhältnisses *erforderlich* ist oder ein Gesetz, ein Tarifvertrag oder eine Dienstvereinbarung dies vorsieht), habe ich das SMK gebeten, mir mitzuteilen, weshalb hier eine personenbezogene Datenübermittlung (Name, Geschlecht, Lebensalter usw. der ausgeschiedenen Lehrkraft) für *erforderlich* gehalten werde. Meines Erachtens reichen nämlich für die Unterrichtung des SMK statistische Werte aus. Außerdem sind die Oberschulämter die personalverwaltenden Stellen und nicht das SMK.

Das SMK teilte daraufhin mit, daß auf personenbezogene Daten der betroffenen Lehrer verzichtet werde. Die Oberschulämter seien deshalb angewiesen worden, nur anonymisierte Daten an das SMK zu melden. Sollten dennoch personenbezogene Daten übermittelt worden sein, sei eine unverzügliche Löschung erfolgt.

Für die demnach ausschließlich statistischen Zwecken dienende Verarbeitung personenbezogener Daten ergaben sich allerdings zusätzlich Einschränkungen aus dem Statistikrecht; dazu unten Abschnitt 5.7.12.

5.1.16 Übermittlung personenbezogener Haushaltsüberwachungslisten durch das Landesamt für Finanzen an mittelbewirtschaftende Dienststellen

Ein Betroffener machte mich darauf aufmerksam, daß das LfF im monatlichen Turnus an die mittelbewirtschaftenden Stellen (die nicht mit den personalverwaltenden Stellen identisch sind) personenbezogene Haushaltsüberwachungslisten mit detaillierten Bezügedaten zu "Kontrollzwecken" übermittelt.

Dem von mir zur Stellungnahme aufgeforderten SMF teilte ich mit, daß für die Aufgabenerfüllung der mittelbewirtschaftenden Dienststellen lediglich die Gesamtsummen pro Haushaltsstelle - also ohne Personenbezug - erforderlich sind (was übrigens auch die Auffassung des SRH ist).

Nach längerem Hin und Her schloß sich das SMF dieser Auffassung an und veranlaßte - entsprechend meinen Vorstellungen - beim LfF die Änderung der Übermittlungspraxis. Die mittelbewirtschaftenden Dienststellen, denen bis dahin die nicht erforderlichen personenbezogenen Haushaltsüberwachungslisten zugegangen sind, wurden gebeten, die Unterlagen entweder an die personalverwaltenden Dienststellen abzugeben oder zuverlässig zu vernichten.

5.1.17 Prüfung von Personalausgaben durch die Staatlichen Rechnungsprüfungsämter beim Landesamt für Finanzen im Onlineverfahren

Der Sächsische Rechnungshof fragte an, unter welchen Voraussetzungen den Staatlichen Rechnungsprüfungsämtern ein *permanenter* Lesezugriff auf die beim LfF vorhandenen Bezügedaten sämtlicher Staatsbediensteter im Onlineverfahren gestattet werden könnte. Man dachte daran, durch Änderung der SHO eine entsprechende Rechtsgrundlage zu schaffen. Außerdem berief sich der Rechnungshof auf ein in Bayern bereits zwischen dem dortigen Obersten Rechnungshof und der Bezügestelle der Bezirksdirektion praktiziertes Verfahren.

In meiner Stellungnahme machte ich dem Rechnungshof deutlich, daß ich der Absicht, den Staatlichen Rechnungsprüfungsämtern Chemnitz, Dresden und Leipzig einen permanenten (lesenden) Online-Zugriff auf die Bezügedaten beim LfF durch eine Änderung der SHO zu ermöglichen, kritisch gegenüberstehe. Den Hinweis, daß in Bayern bereits ein solches Verfahren zwischen dem Obersten Rechnungshof und der Bezügestelle der Bezirksfinanzdirektion praktiziert würde, habe ich zum Anlaß genommen, beim Bayerischen Datenschutzbeauftragten nachzufragen. Mir wurde mitgeteilt, daß das dortige Verfahren ohne sein Wissen und entgegen der § 124 Abs. 1 Satz 3 SächsBG entsprechenden Vorschrift des Bayerischen Beamtengesetzes eingeführt worden ist.

Mein bayerischer Kollege teilt die Auffassung, daß zum einen mit automatisierten Abrufverfahren, die tendenziell den Grundsätzen des Volkszählungsurteils (BVerfGE 65, 1, 43, 44, 45) entgegenstehen (der Bürger weiß nicht mehr, wer was wann und bei welcher Gelegenheit über ihn weiß), stets erhebliche Gefährdungen des Persönlichkeitsrechts der Betroffenen verbunden sind. Zum anderen ist es der Stelle, welche die Daten zum Abruf bereithält, nicht möglich, die Zulässigkeit der Datenübermittlungen im Einzelfall zu überprüfen, was ebenfalls zu Lasten des Persönlichkeitsrechts der Betroffenen geht.

Anders als im Kommunalbereich, wo unter bestimmten Voraussetzungen ein *temporärer* (nicht also ein permanenter) Online-Zugriff des (kommunalen) Rechnungsprüfungsamtes gemäß § 8 Abs. 2 SächsDSG zulässig sein kann (vgl. unten Abschnitt 5.5.7), sehe ich für das ins Auge gefaßte Verfahren keinen Raum. Sogenannte Visaprüfungen (permanente Prüfung aller Vorgänge), die auch ein automatisiertes Abrufverfahren zuließe, sind ohne besonderen Grund unverhältnismäßig und daher unzulässig. Einer Ergänzung der Sächsischen Haushaltsordnung i. S. v. § 8 Abs. 1 SächsDSG, § 124 Abs. 1 Satz 3 SächsBG stehe ich deshalb ablehnend gegenüber. Selbstverständlich bestehen weder gegen die stichprobenartige Überprüfung der Bezügedaten beim Landesamt für Finanzen Bedenken noch gegen eine prüfende Auswertung ganzer Dateien, wenn dies der konkrete Prüfungsauftrag vorsieht.

Bei dieser Bewertung verkenne ich nicht, daß das Verfassungsgebot einer Finanzkontrolle durch den Rechnungshof andere verfassungsrechtlich geschützte Rechtspositionen einschränken kann (vgl. Heuer, Kommentar zur Bundeshaushaltsordnung, § 95, Rdnr. 1 m.w.N.). Andererseits ist in der Rechtsprechung und Literatur anerkannt (vgl. OVG Lüneburg DVBl. 1984, 837; v. Köckritz/Ermisch/Maatz, Kommentar zur Bundeshaushaltsordnung, § 95, Anm. 2), daß Eingriffe in das Persönlichkeitsrecht des einzelnen durch den Rechnungshof nur dann verhältnismäßig sind, wenn es keine andere - das Persönlichkeitsrecht weniger belastende - Möglichkeit gibt, die benötigten Informationen zu erlangen. Das traditionelle Prüfverfahren ist eine solche weniger belastende Möglichkeit.

Ich gehe davon aus, daß die durch den Rechnungshof diskutierte Onlineprüfung nicht mehr weiterbetrieben wird.

5.1.18 Feststellung des Jubiläumsdienstalters

Ende Februar 1997 erfuhr ich, daß in den staatlichen Dienststellen - konkret im SMS - gegenwärtig zur Feststellung des Jubiläumsdienstalters Daten über den lückenlosen Werdegang aus den Personalakten sowie unmittelbar bei den Bediensteten auf einem zweiteiligen Fragebogen erhoben werden; er ist identisch mit dem Formular, mit dem das Besoldungsdienstalter erstmals im Beitrittsgebiet ernannter Beamter festgestellt wird.

Während der erste Teil des Erhebungsbogens mit Angaben, die der Personalakte entnommen wurden, an das LfF zu schicken ist, verbleibt Teil 2 bei der Dienststelle (Personalstelle). Diesen Teil 2 mußten die Bediensteten des SMS ausfüllen. In Spalte 5 wird - wie bereits anläßlich der Festsetzung des Besoldungsdienstalters - nach Funktionen in einer Partei und sonstigen gesellschaftlichen Organisationen gefragt. Da dieser Teil 2 nicht für das LfF bestimmt ist, lag die Vermutung nahe, daß die Angaben in Spalte 5 für die Festsetzung des Jubiläumsdienstalters nicht erforderlich sind und daher nicht erhoben werden dürfen (vgl. § 31 Abs. 1 SächsDSG, § 117 Abs. 4 SächsBG).

Ich habe deshalb beim SMS angeregt, auf Beantwortung der Frage in Spalte 5 zu verzichten und inzwischen vorliegende Antworten zu löschen. Dies ist inzwischen geschehen.

5.1.19 Behandlung von Bescheiden des BStU bei inzwischen aus dem Dienstverhältnis ausgeschiedenen Beschäftigten

Problematisch ist die Behandlung von Bescheiden des BStU für den Fall, daß die Betroffenen zwischenzeitlich aus dem öffentlichen Dienst ausgeschieden sind oder bei einer anderen Behörde beschäftigt werden. In solchen Fällen würden die Bescheide des BStU von einer inzwischen nicht mehr zuständigen Behörde geöffnet und nunmehr unzulässigerweise zur Kenntnis genommen.

Ich habe deshalb angeregt, daß die Behörden den BStU unverzüglich unterrichten, für welche angefragten Personen die Antwort wegen Ausscheidens aus dem öffentlichen Dienst nicht mehr erforderlich ist bzw. (nach Abstimmung mit dem neuen öffentlich-rechtlichen Arbeitgeber) an welche Behörden die Antworten nunmehr geschickt werden sollen.

Dies setzt selbstverständlich eine sorgsame Sachbehandlung der Stasi-Anfragen und deren Rücklaufes voraus.

5.1.20 Veröffentlichung nicht erforderlicher Beschäftigtendaten in Geschäftsverteilungsplänen, Telefonverzeichnissen, Hausmitteilungen usw.

Meinen Feststellungen zufolge enthielten behördliche Publikationen personenbezogene Informationen z. B. über

1. Teilzeitbeschäftigung
2. befristetes Arbeitsverhältnis
3. Mutterschutz
4. Erziehungsurlaub
5. BAT-Eingruppierungen, Höhergruppierung
6. Bewährungsaufstieg
7. Beamtenbeförderung
8. Dienstjubiläum
9. Ordensverleihung

Eine Veröffentlichung solcher Daten ohne Einwilligung der Betroffenen ist mit § 31 SächsDSG und § 121 Abs. 2 SächsBG nicht zu vereinbaren. Sie mögen zwar für die Kollegen interessant sein, sind aber für einen geordneten Dienstbetrieb nicht nötig.
Statt der unter 1 bis 4 genannten Date3n genügen – falls nötig – neutrale Angaben zur Erreichbarkeit („Frau Müller ist nur von 8-13 Uhr erreichbar“).
Die Information über 5 bis 7 ist nicht erforderlich; sie wird durch die natürlich erlaubten und sinnvollen Angaben zur dienstlichen Funktion („Sachgebietsleiter“, „Sekretärin“, „Referent“ etc.) und zur übertragenen Aufgabe („Einbürgerung A-K“, „Bürosachbearbeitung“, „Aufsicht über kommunale Abwasserzweckverbände“) ersetzt. Ob jemand nach BAT VIII oder VII bezahlt wird, ob jemand Oberinspektor oder Amtmann ist, kann dahinstehen.

Allenfalls kommt eine Veröffentlichung der unter 7 bis 9 genannten Ereignisse mit (ausdrücklicher) Einwilligung der Betroffenen in Frage.

Auch in anderen personenbezogenen Aufstellungen, wie beispielsweise Geschäftsverteilungspläne (einschließlich der Änderungen bei den

Funktionszuweisungen) sowie Telefonverzeichnisse für den Dienstgebrauch sind die oben kritisierten Zusatzinformationen nicht erforderlich. Mit dem SMI wird derzeit über eine einheitliche Handhabung im staatlichen Bereich beraten..

Publikationen, die zwar ihrem Wesen nach nur für den Dienstgebrauch erstellt werden, jedoch erfahrungsgemäß immer auch den Weg nach "außen" finden, müssen unbedingt auf das für die Zweckerfüllung unerläßliche Maß beschränkt bleiben.

5.1.21 Veröffentlichung von Personalnachrichten im "Jahrbuch der Staatlichen Kunstsammlungen"

Aus einer Eingabe habe ich erfahren, daß es bisher üblich war, im „Jahrbuch der Staatlichen Kunstsammlungen“ ohne Einwilligung der Betroffenen Personalnachrichten zu veröffentlichen. Eine solche Verfahrensweise halte ich im Hinblick auf § 31 Abs. 2 Satz 1 SächsDSG, wonach die Übermittlung (dazu zählt auch die Veröffentlichung im Jahrbuch) von Beschäftigtendaten an den nichtöffentlichen Bereich (Leser des Jahrbuches) nur auf gesetzlicher Grundlage oder mit Einwilligung der Betroffenen zulässig ist, für unzulässig.

Die Staatlichen Kunstsammlungen, denen ich meine Rechtsauffassung mitgeteilt habe, haben mir schriftlich versichert, daß personenbezogene Daten von aktiven und ehemaligen Beschäftigten künftig nur mit deren Einwilligung veröffentlicht werden.

5.1.22 Datenschutzrechtliche Kontrolle der Personalaktenführung in einer Mittelschule

Bei der Kontrolle der Personalaktenführung in einer Mittelschule mußte ich feststellen, daß in einigen Nebenakten vollständige Kopien von Zeugnissen (Diplomen) mit Zensurenspiegel abgeheftet waren. Mit der Schulleiterin habe ich Einigung erzielt, daß diese Daten in der Personalnebenakte nicht erforderlich i. S. d. § 31 Abs. 1 SächsDSG sind und die Speicherung dieser Daten daher unzulässig ist. Mir wurde zugesagt, die Zensurenspiegel in der Nebenakte zu schwärzen.

Das SMK habe ich gebeten, dies in der Verwaltungsvorschrift über die Führung und Verwaltung von Personalakten von Lehrkräften im Angestelltenverhältnis (noch im Entwurf) klarzustellen und generell den Umgang mit personalaktenrelevanten Unterlagen in Dienststellen, die nicht gleichzeitig personalaktenverwaltende Stellen sind, zu regeln.

5.1.23 Zulässigkeit behördlicher Organisations- und Arbeitsplatzuntersuchungen

In der sächsischen Verwaltung werden zunehmend Organisations- und Arbeitsplatzuntersuchungen u. a. durch Befragung der Stelleninhaber durchgeführt, entweder durch die Behörde selbst oder durch ein beauftragtes Unternehmen.

Auf der Grundlage eines Umfrageergebnisses (Stellungnahmen der Datenschutzbeauftragten der anderen Bundesländer zur datenschutzrechtlichen Einschätzung von Organisations- und Arbeitsplatzuntersuchungen) fand im Oktober 1996 eine gemeinsame Erörterung mit den Staatsministerien des Innern und der Finanzen statt. Dabei wurde Konsens erzielt, daß Organisations- und Arbeitsplatzuntersuchungen schon wegen des haushaltsrechtlichen Grundsatzes der Sparsamkeit und Wirtschaftlichkeit aus vordergründig datenschutzrechtlichen Gründen nicht verhindert werden dürfen.

Auch waren wir uns einig, daß zur Herstellung der Rechtssicherheit eine Anpassung von § 31 Abs. 1 SächsDSG an entsprechende Regelungen anderer Bundesländer, wo Organisationsuntersuchungen ausdrücklich zugelassen werden, vorzusehen sei. In § 117 Abs. 4 SächsBG ist dies ohnehin schon der Fall.

Der Sächsische Landtag hat nunmehr am 7. April 1997 eine entsprechende Änderung des § 31 Abs. 1 SächsDSG beschlossen (GVBl. S. 350).

Eine Mitwirkungspflicht der Beamten ergibt sich aus § 73 SächsBG, wonach sie ihre Vorgesetzten zu beraten und zu unterstützen, ihre Anordnungen auszuführen und damit auch Fragen im Rahmen von Organisationsuntersuchungen zu beantworten haben. Die Mitwirkungspflicht der Arbeitnehmer ergibt sich als individualrechtliche Nebenpflicht aus dem Arbeitsvertrag. Nach dem rechtskräftigen Urteil des LAG Frankfurt vom 26. Januar 1989 - 9 SaGa 1583/88, CR 4/1990, 274 ist unter Beachtung des auch das Arbeitsverhältnis bestimmenden Grundsatzes von Treu und Glauben davon auszugehen, daß der Arbeitgeber berechtigt ist, vom Arbeitnehmer zu verlangen, daß dieser bei einer Überprüfung der Wirtschaftlichkeit und Organisation der Verwaltung mitwirkt. Das LAG führt aus, daß dazu auch die Beantwortung entsprechender Fragen betreffend den Arbeitsplatz und die Umstände der persönlichen Arbeitsleistung gehört, soweit daran ein sachlich begründetes Interesse besteht und die Beantwortung dem Arbeitnehmer unter Beachtung insbesondere seines grundgesetzlich geschützten Persönlichkeitsrechts zumutbar ist.

Im Unterschied zu Organisationsuntersuchungen, in deren Mittelpunkt eine Analyse der Aufbau- und Ablauforganisation steht, sind reine Mitarbeiterbefragungen, in denen es (vorwiegend oder ausschließlich) um die subjektive Bewertung des Arbeitsumfeldes geht (wo also der Sachbezug wie bei einer Organisationsuntersuchung fehlt), nur auf *freiwilliger* Basis zulässig.

Wichtig ist jedenfalls, daß die Zweckbindung der Daten beachtet wird (keine Verwendung für andere Zwecke), daß sie zum frühestmöglichen Zeitpunkt anonymisiert werden oder, soweit ein Personenbezug herstellbar bleibt, daß sie zum frühestmöglichen Zeitpunkt gelöscht werden.

5.1.24 Mitarbeiterbefragung im Zusammenhang mit einem von der Bertelsmann-Stiftung initiierten Städtevergleich

Ein Mitglied des Landtages informierte mich, daß Beschäftigte einer Stadtverwaltung seines Wahlkreises im Rahmen eines interkommunalen Wettbewerbs einen umfangreichen Fragebogen ausfüllen sollten.

Bei meinen Ermittlungen stellte ich fest, daß es bei allen neun beteiligten Städten, die ich nach der
- verantwortlichen Stelle innerhalb der Stadt,
- Freiwilligkeit der Angaben,
- Anonymisierung,
- Löschung,
- Übermittlung der Ergebnisse an die Bertelsmann-Stiftung

fragte, keinen Anlaß zu einer datenschutzrechtlichen Beanstandung gab.

Dem Abgeordneten konnte ich deshalb mitteilen, daß
- die Projektleitung durchweg bei Personen lag, die nicht an Personalentscheidungen mitwirken,
- die Freiwilligkeit der Mitarbeiterbefragung gesichert war,
- die Löschung der Fragebogen nach anonymisierter Auswertung erfolgte,
- eine Datenübermittlung der anoymisierten Ergebnisse an die Bertelsmann-Stiftung nicht erfolgte; vielmehr wurden die anonymisierten Ergebnisse der für den interkommunalen Leistungsvergleich federführenden Stadt mitgeteilt.

5.1.25 Informations- und Führungsunterstützungssystem (IFS) des SMU

Das SMU hat ein Informations- und Führungsunterstützungssystem (IFS) eingerichtet und die Staatlichen Umweltfachämter aufgefordert, ihm quartalsweise Übersichten über Zahl und Bearbeitungsstand der von ihnen zu erledigenden Stellungnahmen zu übersenden. Als Grundlage für die Meldungen ans SMU dienen von den Umweltfachämtern zu führende "Vorgangsbegleitblätter", aus denen u.a. auch die jeweiligen Sachbearbeiter ersichtlich sind.

Meine anfänglichen Bedenken, die “Vorgangsbegleitblätter” könnten für eine umfassende Leistungskontrolle der jeweiligen Bearbeiter zweckentfremdet werden (was mit § 31 Abs.1 SächsDSG nicht ohne weiteres zu vereinbaren gewesen wäre), wurden anläßlich einer eingehenden Erörterung mit dem SMU zerstreut. Die erhobenen Daten liefern zweckgebunden einen nach Fachbereichen gegliederten Überblick über die Anzahl der von den Staatlichen Umweltfachämtern zu bearbeitenden Stellungnahmen. Sie werden nicht beim jeweiligen Vorgesetzten, sondern beim jeweiligen Vorgang aufbewahrt, so daß eine Kontrolle der Leistungen der Bearbeiter zwar theoretisch möglich ist, jedoch wegen des unverhältnismäßigen Aufwandes, den eine personenbezogene Zusammenführung der Einzelvorgänge verursachen würde, unterbleibt.

5.1.26 Mitarbeiterbezogene Leistungsstatistiken aus dem automatisierten Wohngeldverfahren (Liste WG 07)

Bei der Überprüfung der Verträge zwischen den kommunalen Datenverarbeitungszweckverbänden und den Gemeinden über die automatisierte Wohngeldbearbeitung habe ich festgestellt, daß das Wohngeldberechnungsprogramm u.a. den Ausdruck einer Leistungsstatistik (Liste WG 07) zuläßt, aus der ersichtlich ist, wieviele Wohngeldfälle der einzelne Wohngeldsachbearbeiter erledigt hat. Zumindest zwei sächsische Gemeinden ließen sich die Liste WG 07 regelmäßig ausdrucken.
Wäre ich ordnungsgemäß nach § 31 Abs. 7 SächsDSG beteiligt worden, hätte ich die betreffenden Gemeinden bereits im Vorfeld auf die Unzulässigkeit des Verfahrens hingewiesen.
Da die Liste WG 07 ausschließlich der Leistungs- und Verhaltenskontrolle der Wohngeldsachbearbeiter dient und durch den ständigen Überwachungsdruck in unverhältnismäßiger Weise in das Persönlichkeitsrecht der Betroffenen eingegriffen wird, ist das SMI meiner Bitte nachgekommen, alle Wohngeldstellen in Sachsen auf die Unzulässigkeit des Verfahrens hinzuweisen. Inzwischen habe ich erfahren, daß die Funktion “Erstellen der Liste WG 07” aus dem Programm herausgenommen und bisher angefallene Vorgänge gelöscht worden sind.

5.1.27 Ressortübergreifende Fortbildung: Beurteilung der Seminare und Dozenten durch Kursteilnehmer (Evaluation)

Seit Jahren habe ich mich bemüht, beim SMI datenschutzgerechte Lösungen bei der Erhebung und Auswertung von Evaluationsdaten zu erreichen (siehe schon unter 5.1.8 im 3. Tätigkeitsbericht). Insbesondere habe ich kritisiert, daß die Beurteilung der Dozenten durch die Seminarteilnehmer (Datenerhebung bei Dritten) zunächst ohne Einwilligung der Betroffenen vorgesehen war.

Nach wiederholten Gesprächen hat das SMI eine m. E. datenschutzfreundliche Regelung in den Dozentenvertrag aufgenommen, die nunmehr den Anforderungen an eine wirklich freiwillige Einwilligung entspricht.

5.1.28 Novellierung der Arbeitskampfrichtlinien 1992

Sensibilisiert durch das Streikgeschehen im öffentlichen Dienst habe ich mich mit den Arbeitskampfrichtlinien der Tarifgemeinschaft deutscher Länder (TdL) befaßt. Sie sollen den Dienststellen Hinweise zur verwaltungsmäßigen Abwicklung von Arbeitskampfmaßnahmen geben. Aus aktuellem Anlaß wurden die Arbeitskampfrichtlinien von der TdL überarbeitet. Vom SMF wurde ich gebeten, die Neufassung datenschutzrechtlich zu prüfen.

Im großen und ganzen halte ich die Richtlinien datenschutzrechtlich für unbedenklich.

Allerdings ist eine Dokumentation über den gesamten Ablauf der jeweiligen Arbeitskampfmaßnahme vorgesehen, die an die vorgesetzte Behörde weitergeleitet werden soll. Einzelheiten dazu, wie diese Dokumentation zu erstellen ist, sind einem Hinweisblatt zu entnehmen, wonach außer der Schilderung der Vorgeschichte der Arbeitskampfmaßnahme auch Unterlagen wie Protokolle und Vermerke über mit Arbeitnehmern, dem Personal- bzw. Betriebsrat geführte Verhandlungen, Pläne über zum Notdienst bestellte Arbeitnehmer u. ä. beizufügen sind.
Zwar wurde mir vom SMF mitgeteilt, daß die Erstellung der Dokumentation über die Arbeitskampfmaßnahme laut TdL *nicht zum Ziel habe*, der vorgesetzten Behörde einzelne streikende Arbeitnehmer zu benennen, gleichwohl ist es jedoch denkbar, daß die vorgesetzte Behörde durch die Übersendung der der Dokumenation beizufügenden Vermerke und Protokolle personenbezogene Daten einzelner am Streikgeschehen beteiligter Arbeitnehmer erhält.

Die Erkenntnis, daß das Verhalten der Arbeitnehmer bei Arbeitskampfmaßnahmen möglicherweise dokumentiert und an die vorgesetzte Behörde übermittelt wird, kann letztendlich zu einem Verzicht des aus der verfassungsrechtlichen Tarifautonomie abgeleiteten Streikrechts führen. Denn wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. Wer damit rechnet, daß etwa die Teilnahme an einer Versammlung oder an einer Bürgerinitiative oder eben an einem Streik behördlich registiert wird und daß ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte (Art. 8, 9 GG) verzichten. Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist (BVerfGE 65, 1, 43).

Gerade weil die Erstellung der Dokumentation laut TdL nicht zum Ziel hat, Daten über das Streikverhalten einzelner Arbeitnehmer an die vorgesetzte Behörde weiterzuleiten, sollte auf personenbezogene Vermerke und Verhandlungsprotokolle als Dokumentationsunterlagen verzichtet werden. Ich halte daher eine Klarstellung der Formulierungen in dem Hinweisblatt nach wie vor für unerläßlich.

5.2 Personalvertretung

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

In Abschnitt 5.2.5 des 4. Tätigkeitsberichts habe ich wegen möglicher Irritationen, die durch o. a. Bestimmungen entstehen könnten, die ersatzlose Streichung des § 77 Nr. 4 SächsPersVG gefordert. Das SMI konterte in seiner Stellungnahme überzeugend und für alle Rechtsanwender klarstellend, daß § 80 Abs. 3 Nr. 16 SächsPersVG als lex specialis der Auffangvorschrift des § 77 Nr. 4 SächsPersVG vorgeht. Deshalb konnte ich meine Forderung nach Streichung der Vorschrift nicht aufrechterhalten.

5.2.2 Dürfen beim Personalrat Personalnebenakten entstehen?

Ein Oberschulamt teilte mit, daß Personalunterlagen, die von der personalverwaltenden Stelle im Rahmen der Mitwirkungs- und Mitbestimmungsverfahren zur Verfügung gestellt wurden, vom Personalrat nach Abschluß seiner Entscheidung zu seinen Akten genommen wurden. Auf diese Weise entstanden dort Personalnebenakten.

Schon in meinem 4. Tätigkeitsbericht (5.2.1) habe ich u. a. festgestellt, daß beim Personalrat keine zweite Personalakte - auch nicht in verkürzter Form - entstehen darf.

Dies ergibt sich bereits aus § 117 Abs. 2 SächsBG, wonach Nebenakten nur geführt werden dürfen, wenn die personalverwaltende Behörde nicht zugleich Beschäftigungsbehörde ist oder wenn mehrere personalverwaltende Behörden für den Bediensteten zuständig sind. Der Personalrat ist weder personalverwaltende Behörde noch Beschäftigungsbehörde, so daß von ihm Nebenakten nicht geführt werden dürfen. Dieses Verbot stützt sich außerdem auf § 117 Abs. 3 SächsBG, wonach Zugang zur Personalakte nur Beschäftigte haben dürfen, die im Rahmen der Personal*verwaltung* mit der Bearbeitung von Personalangelegenheiten beauftragt sind. Dem Personalrat, der nicht mit Personalverwaltungsaufgaben betraut ist, steht der Zugang zur Personalakte nur unter den in § 73 Abs. 2 Satz 3 SächsPersVG genannten Voraussetzungen - also nur mit Zustimmung des Beschäftigten und nur zur Lösung eines Einzelfalles - zu. Auch dies ist ein Indiz dafür, daß Personalunterlagen beim Personalrat auf Dauer nichts zu suchen haben.

Aus alledem folgt, daß der Personalrat nach Abschluß des personalvertretungsrechtlichen Verfahrens die ihm (temporär) zur Verfügung gestellten Unterlagen entweder an die personalverwaltende Stelle zurückzugeben oder - falls es sich um keine Originale handelt - zuverlässig zu vernichten hat.

Die Aktenführung (einschließlich der automatisierten) der Personalräte werde ich verstärkt kontrollieren.

5.3 Einwohnermeldewesen; Paß- und Personalausweiswesen

5.3.1 Rechtliche Entwicklung: Entwurf eines Gesetzes zur Änderung des Sächsischen Meldegesetzes

Im März 1997 hat der Landtag eine Novellierung des Meldegesetzes beschlossen. Dankenswerterweise wurde ich in die Vorarbeiten so frühzeitig eingebunden, daß ich zu den mir übersandten Gesetzentwürfen umfassend Stellung nehmen konnte. Größtenteils wurden meine Anregungen berücksichtigt.

In folgenden Bereichen konnte ich mich nicht durchsetzen:

5.3.1.1 Novellierungsbedürftigkeit von §§ 18 Abs. 2, 19 Abs. 1 SächsMG

Entgegen § 16 Abs. 2 Satz 1, 2. Halbsatz MRRG sehen §§ 18 Abs. 2, 19 Abs. 1 SächsMG - wie bisher - auch für Deutsche eine Pflicht vor, sich gegenüber dem Leiter der Beherbergungsstätte oder seinem Beauftragten durch Vorlage eines Identitätsdokuments zu identifizieren. Ich habe zum Gesetzentwurf der Staatsregierung - wie auch schon früher (vgl. 3. Tätigkeitsbericht 5.3.1.2, unter c) - ausgeführt, daß § 16 Abs. 2 Satz 1, 2. Halbsatz MRRG, der eine Identifizierungspflicht nur für Ausländer vorsieht, eine unmittelbar geltende und abschließende Einzelvorschrift i. S. v. Art. 75 Abs. 2 GG ist. Dies ergibt sich - abgesehen vom Wortlaut der Vorschrift - daraus, daß der Gesetzgeber in der Vorschrift diejenigen Bereiche, die durch Landesrecht näher geregelt werden dürfen, ausdrücklich genannt hat (z. B. § 16 Abs. 2 Satz 3 MRRG: "... nach Maßgabe des Landesrechts" ...; Absatz 4: "... soweit durch Bundes- oder Landesrecht nichts anderes bestimmt ist".). Die Erweiterung der Identifizierungspflicht auch auf Deutsche ist hier nicht vorgesehen und daher wohl rahmenrechtswidrig.

5.3.1.2 Erweiterung des Datenkatalogs in § 29 Abs. 1 SächsMG

Der Datenkatalog des § 29 Abs. 1 SächsMG ist um die Daten:
- "16. erwerbstätig/nicht erwerbstätig" und
- "17. Zugehörigkeit zu einer öffentlich-rechtlichen Religionsgesellschaft"

erweitert worden. Damit ist die Übermittlung dieser Daten an andere öffentliche Stellen zulässig, wenn dies zur Erfüllung der Aufgaben des Empfängers *erforderlich* ist. Demgegenüber schreibt § 18 Abs. 2 MRRG verbindlich vor, daß diese Daten (weil sie nicht in Absatz 1 genannt sind) nur dann übermittelt werden dürfen, wenn der Empfänger ohne Kenntnis der Daten zur Aufgabenerfüllung *nicht in der Lage wäre* und eine Datenerhebung beim Betroffenen ausnahmsweise nicht in Betracht kommt. Diese strengen Voraussetzungen bleiben in der Gesetzesänderung unbeachtet.

Das SMI teilt meine Auffassung und hat zugesagt, auf die Streichung der Daten in Nr. 16 und 17 der Vorschrift hinzuwirken.

5.3.1.3 Kostenerhebung für das Eintragen von Auskunftssperren bei Gefahr für Leben, Gesundheit, persönliche Freiheit oder ähnliche schutzwürdige Belange

§ 23 Abs. 1 Satz 2 SächsMG sieht weiterhin die Möglichkeit der Kostenerhebung für das Eintragen von Auskunftssperren bei Vorliegen o. g. Voraussetzungen vor. Mit dem SMI hatte ich nach intensivem Schriftwechsel und Gesprächen bereits Einigung erzielt, daß das Eintragen solcher Auskunftssperren kostenfrei sein soll. Auch der Gesetzentwurf der Staatsregierung sah die Möglichkeit einer Kostenerhebung nicht mehr vor. Der Landtag hat jedoch anders entschieden.

5.3.2 Abgleich des Schwerbehindertendatenbestandes der Ämter für Soziales mit den Melderegistern

In Sachsen sind bei den Ämtern für Soziales annähernd 300.000 Schwerbehinderte registriert. Trotz einer Mitteilungspflicht der Betroffenen werden infolge Sterbefällen und Wegzügen die Datenbestände der Ämter vielfach fehlerhaft.

Frühzeitig wurde ich vom SMS über Bestrebungen, regelmäßige Datenabgleiche mit den Melderegistern zum Zwecke der Bereinigung des Schwerbehinderten-Datenbestandes einzuführen, unterrichtet. Jedoch lassen weder die rechtlichen Voraussetzungen (fehlende Regelung in einer Meldedatenübermittlungsverordnung) noch ein mir vorgelegtes Konzept über die beabsichtigte technische Abwicklung zum gegenwärtigen Zeitpunkt solche Datenabgleiche zu.

Die weitere Entwicklung werde ich im Auge behalten.

5.3.3 Erteilung von Melderegisterauskünften über das Internet

Mit dem SMI erörterte ich die Frage, ob die Meldebehörden den zur Erteilung "einfacher" Melderegisterauskünfte (§ 32 Abs. 1 SächsMG) erforderlichen Teil des Melderegisters ins Internet stellen dürfen.

Wir waren uns einig, daß nach § 1 Abs. 2 Satz 1 SächsMG die Meldebehörden - und nur diese - zur Erfüllung ihrer Aufgaben das Melderegister zu führen haben. Da das Melderegister (auch in verkürzter Form) kein öffentliches Register ist, scheidet eine Einstellung ins Internet, wo die Meldedaten der Öffentlichkeit ohne Einschränkung zur Verfügung stünden, von vornherein aus, zumal eine Prüfung, ob schutzwürdige Belange des Betroffenen beeinträchtigt werden könnten (§ 22 SächsMG), nicht möglich wäre. Außerdem verbietet § 32 Abs. 3 SächsMG eine Einstellung ins Internet, weil Melderegisterauskünfte über eine Vielzahl nicht namentlich bezeichneter Einwohner (Gruppenauskunft) nur erteilt werden dürfen, soweit sie im öffentlichen Interesse liegen. Eine Prüfung dieser Voraussetzung kann vor einer Abfrage über das Internet nicht erfolgen.

Auch sind regelmäßige Datenübermittlungen an Private oder automatisierte Abrufe durch Private im Sächsischen Meldegesetz nicht vorgesehen (nach §§ 29 Abs. 5, 36 Nr. 4 SächsMG sind solche Datenübermittlungen oder Abrufe nur an bzw. durch Behörden oder sonstige öffentliche Stellen unter den dort genannten Voraussetzungen möglich).

Gegen die Einstellung des (verkürzten) Melderegisters ins Internet spricht auch § 33 SächsMG; die Widersprüche nach § 33 Abs. 4 SächsMG blieben wirkungslos.
Abgesehen von der Kostenfrage (Melderegisterauskünfte sind kostenpflichtig) spricht zuletzt noch gegen die Einstellung des (verkürzten) Melderegisters ins Internet, daß eine Aktualisierung des Datenbestandes einen unverhältnismäßigen Aufwand erfordern würde.

5.4 Personenstandswesen

5.4.1 Rechtliche Entwicklung

Im Juli 1996 erhielt ich vom SMI den Vorentwurf eines Fünften Gesetzes zur Änderung des Personenstandgesetzes (5. PStÄndG; Stand: 25. März 1996), zu dem ich - wie andere Datenschutzbeauftragte - ausführlich Stellung genommen habe.

Vor dem Hintergrund, daß der Bund seit annähernd zwölf Jahren an dem Gesetzentwurf „bastelt“, der den Grundsätzen des Volkszählungsurteils vom 15. Dezember 1983 (BVerfGE 65, 1, 42, 44) entsprechend für normenklare Datenschutzregelungen im Personenstandswesen sorgen soll, sind die nach wie vor vorhandenen zahlreichen und erheblichen Defizite unerklärlich. Es würde den Rahmen dieses Berichtes sprengen, sämtliche Mängel aufzuzählen. Deshalb begnüge ich mich mit der abstrakten Darstellung einiger Schwerpunkte.

So sind die Regelungen über technische und organisatorische Maßnahmen zur Gewährleistung des Datenschutzes, gerade im Hinblick auf die zunehmende Automation des Personenstandswesens völlig unzureichend.

Insbesondere entsprechen auch die zahlreichen Mitteilungspflichten des Standesamtes gegenüber anderen Behörden und umgekehrt nicht dem Gebot der Normenklarheit.

Unbefriedigend geregelt werden aus meiner Sicht die Einsichtnahme in Personenstandsbücher und Auskünfte aus Personenstandsbüchern an private Dritte, aber auch an andere Behörden. Endlich werden die Bücher zugunsten der genealogischen Forschung geöffnet (Voraussetzung, daß seit dem Tod des Betroffenen mindestens 30 Jahre, oder falls der Todestag nicht bekannt ist, seit der Geburt mindestens 120 Jahre vergangen sind). Mit Einwilligung der noch Lebenden oder der Hinterbliebenen sollte das aber auch jederzeit gestattet sein.

Dem humanitären Auftrag verschiedener nationaler und internationaler Organisationen (z. B. Internationaler Suchdienst Arolsen, Suchdienst des Deutschen Roten Kreuzes, Volksbund Deutsche Kriegsgräberfürsorge e. V.) ist nicht ausreichend Rechnung getragen. Diese Institutionen benötigen zur Erfüllung ihrer Aufgaben nicht nur Daten von längst Verstorbenen, sondern insbesondere auch von noch lebenden Hinterbliebenen, um diese auf bestehende Entschädigungsansprüche oder z. B. über Ort und Lage von Grabstätten im Kriege Gefallener zu unterrichten. Das geforderte Vorliegen eines „rechtlichen Interesses“ dürfte im Falle der Hinterbliebenenermittlung nicht erfüllt sein. Ich habe deshalb eine Einwilligungslösung vorgeschlagen.

Für Behörden sollen Einsicht oder Auskunft nur noch zur Erfüllung *hoheitlicher* Aufgaben erlaubt sein. Da jedoch Personenstandsdaten auch bei der Erfüllung sonstiger öffentlicher Aufgaben von Bedeutung sein können (z. B. Ermittlung von Verstorbenendaten für eine öffentliche Ehrung durch die Behörde), habe ich auch hier eine Einwilligungsregelung angeregt, falls von der Beschränkung auf „hoheitliche“ Aufgaben nicht abgegangen werden sollte.

Defizite weist auch die an und für sich begrüßenswerte Regelung zugunsten der wissenschaftlichen Forschung auf. So sollten Ausnahmen vom Grundsatz der Einwilligung, die Verwendung der erhobenen Daten für andere Forschungsvorhaben, die Anonymisierung und Löschung der Daten etwa an § 30 SächsDSG angepaßt werden.

Die Reaktion des Bundesgesetzgebers auf die zahlreichen Stellungnahmen der Datenschutzbeauftragten bleibt abzuwarten.

5.4.2 Datenschutzrechtliche Einordnung des Volksbundes Deutsche Kriegsfürsorge e. V. (Volksbund)

Im 4. Tätigkeitsbericht (5.4.1) habe ich mich im Ergebnis dahingehend geäußert, daß die humanitäre Arbeit des Volksbundes (hier: Unterrichtung der Angehörigen von Kriegstoten über Ort und Lage der Grabstätten im Ausland) nicht durch das PStG behindert werden darf.

Die rechtlichen Grenzen des § 61 Abs. 1 PStG (gegenwärtige Fassung) haben mich deshalb zu Auslegungsüberlegungen veranlaßt, die ich dem Volksbund mitgeteilt habe.

Um die nächsten Angehörigen von Kriegstoten über die (neue) Lage von Grabstätten informieren zu können, bittet die „Abteilung Gräbernachweis und Angehörigenbetreuung“ des Volksbundes bei Städten und Gemeinden um Auskünfte u. a. aus den Standesamtsbüchern. Entscheidend für die Zulässigkeit solcher Auskünfte ist die datenschutzrechtliche Einordnung des Volksbundes entweder als Behörde oder als nicht-öffentliche Stelle.

Unter den verwaltungsverfahrensrechtlichen Behördenbegriff fallen außer den

Verwaltungsbehörden im organisatorischen Sinn und den kraft Gesetzes beliehenen Unternehmen auch alle sonstigen Einrichtungen, die aufgrund von Vorschriften des öffentlichen Rechts mit der Befugnis zu sonstigem nach öffentlichem Recht zu beurteilenden Handeln (auch z. B. schlicht hoheitliches Handeln) ausgestattet sind (vgl. BGH, DVBl 1987, 1266).

Als eine solche Vorschrift des öffentlichen Rechts wird auch „Gewohnheitsrecht“ anerkannt (vgl. Kopp, Rdnr. 21 zu § 1 VwVfG). Gewohnheitsrecht entsteht durch längere und gleichmäßige Übung sowie die Überzeugung der Beteiligten, daß diese Übung rechtlich geboten sei (Maurer, Allgemeines Verwaltungsrecht, § 4 Rdnr. 19). Diese Voraussetzungen liegen m. E. bei dem Volksbund, der bereits seit 1919 die Kriegsgräberfürsorge betreibt, vor.

Nach diesen Überlegungen und nach Auswertung des mir vom Auswärtigen Amt zur Verfügung gestellten Materials ist der Volksbund - obwohl privatrechtlich organisiert - nach meinem Dafürhalten in Erfüllung seiner öffentlichen Aufgabe „Kriegsgräberfürsorge“ als Behörde zu behandeln. Datenübermittlungen aus den Personenstandsbüchern an den Volksbund halte ich daher im Freistaat Sachsen nach § 61 Abs. 1 Satz 1 und 2 PStG für zulässig. Dem humanitären Auftrag des Volksbundes kann somit m. E. in Sachsen Rechnung getragen werden. Denkbar ist allerdings, daß man durch das in Vorbereitung befindliche 5. PStÄndG zu einer noch klareren Lösung gelangt (vgl. vorstehend unter 5.4.1).

5.4.3 Erhebung personenbezogener Daten durch ein Standesamt bei "vermuteter Scheinehe”

Der Verband binationaler Familien und Partnerschaften (*iaf e.V.*) fragte, ob es zulässig sei, daß ein Standesbeamter bei einem deutsch-ausländischen Paar die Entgegennahme der für die Eheschließung erforderlichen Unterlagen von der Unterzeichnung einer eidesstattlichen Versicherung abhängig machen darf, um sicherzugehen, daß keine “Scheinehe” geschlossen wird.

Meine Ermittlungen ergaben, daß das Standesamt von der Deutschen Botschaft im Heimatstaat des Bräutigams konkrete Hinweise auf Vorliegen einer “Scheinehe” zur Erlangung einer Aufenthaltsgenehmingung erhalten hatte. Das betreffende Standesamt war bisher noch nie mit dem Thema “Scheinehe” bei einer Aufgebotsniederschrift konfrontiert gewesen. Um nichts falsch zu machen und um sich abzusichern, verlangte der Standesbeamte die eidesstattliche Versicherung. § 382 DA regelt, unter welchen Voraussetzungen sich der Standesbeamte eine eidesstattliche Versicherung geben lassen darf. Im Zusammenhang mit “Scheinehen” besteht keine solche Möglichkeit, so daß ich das Standesamt auf die Unzulässigkeit des Verfahrens hinweisen mußte. Es wurde mir versichert, daß sich ein derartiger Vorgang nicht widerholen werde.

Weil die Problematik im Hinblick auf die geplante Rückführung bosnischer Bürgerkriegsflüchtlinge ebenfalls von aktueller Bedeutung ist (die Eheschließung mit

einem deutschen Partner steht einer Rückführung entgegen), habe ich das SMI zu der grundsätzlichen Frage, wie sich Standesbeamte bei Hinweisen auf Vorliegen einer “Scheinehe” zu verhalten haben, um Stellungnahme gebeten.

Nachstehende Ausführungen des SMI dürften für alle Standesämter bedeutsam sein:

"Der Begriff der Scheinehe ist ebenso wie der Begriff der Ehe gesetzlich nicht definiert. Jede unter Mitwirkung eines Standesbeamten geschlossene Ehe ist zunächst gültig.

Die Rechtsprechung läßt die Ablehnung der Eheschließung durch den Standesbeamten nur in sog. evidenten Mißbrauchsfällen zu (vgl. OLG Frankfurt vom 23.2.1995, StAZ 1995, 139, OLG Hamburg vom 22.01.1996, StAZ 1996, 139, OLG Düsseldorf vom 2.2.1996, StAZ 1996, 138). Somit wird der Nachweis einer 'Scheinehe' in der Praxis sehr schwierig, denn der ehefremde Zweck der Eheschließung muß ausschließlich, offenkundig und nachweisbar sein.

Der bloße Verdacht einer beabsichtigten 'Scheinehe', weil sich die Verlobten erst kurz kennen oder sich nicht verständigen können, der ausländische Beteiligte Asylbewerber ist oder ihm aufenthaltsbeendende Maßnahmen drohen, reicht für die Ablehnung der Eheschließung nicht aus. Zwar kann der Standesbeamte durch Befragung der Verlobten prüfen, ob sich seine Vermutung bestätigen läßt, dies ist jedoch nur in beschränktem Umfang möglich. Insbesondere Ermittlungen vom Amts wegen durch den Standesbeamten sind durch Art. 1 GG i. V. m. Art. 2 Abs. 1 GG von vornherein enge Grenzen gesetzt. So sind etwa Fragen, die die Intimsphäre der Beteiligten betreffen, ausgeschlossen. Die Fragen dürfen sich nur auf den nach außen allgemein erkennbaren Teil der ehelichen Lebensgemeinschaft beziehen. Kann der Standesbeamte seine Zweifel daran, daß eine eheliche Lebensgemeinschaft beabsichtigt ist, nicht ausräumen, kann er eine Entscheidung des Amtsgerichts nach § 45 Abs. 2 PStG herbeiführen. Kommt er dagegen zu der Überzeugung, daß eine 'Scheinehe' beabsichtigt ist, lehnt er die Anordnung des Aufgebots oder die Vornahme der Eheschließung ab. Auf Verlangen erläßt er einen schriftlichen Bescheid mit Rechtsmittelbelehrung.

Dieses Recht des Standesbeamten, die Bestellung des Aufgebots und die Eheschließung abzulehnen, wird allerdings wegen der Eheschließungsfreiheit des Art. 6 Abs. 1 GG und auch deshalb, weil das Eherecht ein Mißbrauchsrecht nicht kennt, nur sehr restriktiv anerkannt."

Diesen Ausführungen ist nichts hinzuzufügen.

5.4.4 Datenschutz bei Übersetzungen ausländischer Personenstandsurkunden

Einer öffentlich bestellten Übersetzerin für die russische Sprache fiel bei der Übersetzung von Aussiedlerdokumenten auf, daß auf russischen Sterbeurkunden stets auch die *Todesursache* angegeben ist. Da die Todesursache auf deutschen Sterbeurkunden nicht vorgesehen ist, fragte sie, ob sie bei der Übersetzung aus datenschutzrechtlichen Gründen diese Angabe auslassen dürfe.

In meiner Stellungnahme habe ich zunächst deutlich gemacht, daß Daten von Verstorbenen grundsätzlich nicht unter den Schutzbereich der Datenschutzgesetze fallen. Gleichwohl können Informationen über Verstorbene Auswirkungen auf die Hinterbliebenen entfalten. So könnten Angaben über die Todesursache zu Spekulationen und damit zur Beeinträchtigung des Persönlichkeitsrechts der Hinterbliebenen führen.

Dennoch kann es nicht der Disposition des Übersetzers überlassen bleiben, in Urkunden - auch unter datenschutzrechtlichen Gesichtspunkten - etwas wegzulassen oder nicht. Sollten die übersetzten Urkunden zur Vorlage bei deutschen Behörden dienen, so dürfen diese, dem Grundsatz der Erforderlichkeit gehorchend, die "überschüssigen" (hier: Todesursachen-) Daten nicht nutzen. Für sächsische Behörden gilt § 20 Abs. 2 SächsDSG, wonach nicht für die Aufgabenerfüllung der Behörde erforderliche Daten zu *sperren* sind. Sperren bedeutet nach § 3 Abs. 2 Nr. 7 i. V. m. § 20 Abs. 4 SächsDSG die Einschränkung der weiteren Verarbeitung der nicht erforderlichen Todesursachendaten insofern, als eine weitere Nutzung grundsätzlich nur mit Einwilligung der betroffenen Hinterbliebenen zulässig wäre. Ohne Einwilligung der Betroffenen dürfen gesperrte Daten nur verarbeitet werden, wenn

1. es zur Behebung einer dringenden Beweisnot in einem gerichtlichen oder Verwaltungsverfahren oder zu Aufsichts- oder Kontrollzwecken unerläßlich ist *und*

2. die Daten hierfür übermittelt oder genutzt werden dürften, wenn sie nicht gesperrt wären.

Diese Ausnahme dürfte nach meinem Dafürhalten für die von der Übersetzerin problematisierten Todesursachendaten nicht in Frage kommen.

5.5 Kommunale Selbstverwaltung

5.5.1 Datenschutzprobleme im Kreistag

Ein Landrat informierte mich, daß
- eine in nichtöffentlicher Sitzung gefällte Personalentscheidung im anschließenden öffentlichen Sitzungsteil bekanntgegeben wurde,
- einem Kreisrat die Mehrfertigung der Niederschrift über die nichtöffentliche Sitzung

ausgehändigt wurde,
- der Kreisrat diese Niederschrift einem Gericht als Beweismittel in einem Zvilprozeß vorgelegt hat und
- dieser Kreisrat seine Kenntnisse über die Abmahnung einer Kreisbediensteten der Presse mitgeteilt hat,

und bat mich um datenschutzrechtliche Bewertung.

Zu den im Landratsamt entstandenen "Rechtsfragen im Zusammenhang mit der ehrenamtlichen Tätigkeit von Kreisräten" nahm ich wie folgt Stellung:

1. Bekanntgabe von in nichtöffentlichen Sitzungen gefaßten Beschlüssen

Bereits in meinem 1. Tätigkeitsbericht habe ich mich unter 5.5.2 mit dem Konflikt, Öffentlichkeitsgrundsatz bei Gemeinderatssitzungen einerseits, Recht auf informationelle Selbstbestimmung der Betroffenen andererseits, auseinandergesetzt. Immer dann, wenn das Recht auf informationelle Selbstbestimmung berührt ist (das ist bei Personalentscheidungen stets der Fall), wenn also berechtigte private Interessen einzelner es gebieten, ist die Öffentlichkeit gemäß § 33 Abs. 1 Satz 1 SächsLkrO auszuschließen. In nichtöffentlicher Sitzung gefaßte Beschlüsse mit personenbezogenem Inhalt dürfen aus dem gleichen Grund gemäß § 33 Abs. 1 Satz 3 SächsLkrO *nicht* in öffentlicher Sitzung bekanntgegeben und erst recht nicht veröffentlicht werden. Allenfalls käme eine Bekanntgabe in anonymisierter Form - also nicht personenbeziehbar - in Frage (vgl. auch Abschnitt 5.5.1 meines 4. Tätigkeitsberichts).

Die Bekanntgabe des in nichtöffentlicher Sitzung gefaßten Beschlusses im nachfolgenden öffentlichen Teil der Sitzung nahm hierauf keine Rücksicht. Der Personenbezug ist trotz Abkürzung des Namens der Betroffenen ("Frau X, Sozialdezernentin und Außenstellenleiterin des Y-Kreises") eindeutig gegeben. Daß durch die Bekanntgabe in öffentlicher Sitzung schutzwürdige Interessen der Betroffenen berührt sind, ergibt sich bereits aus § 31 Abs. 1 und 2 SächsDSG. Die Bekanntgabe der Personalmaßnahme war weder zur Eingehung, Durchführung oder Beendigung des Arbeitsverhältnisses *erforderlich* noch gab es eine ausreichende gesetzliche Grundlage, geschweige denn eine Einwilligung der Bediensteten.

2. Behandlung des Protokolls der nichtöffentlichen Sitzung

Nach § 36 Abs. 2 Satz 3 SächsLkrO dürfen Mehrfertigungen von Niederschriften über nichtöffentliche Sitzungen nicht ausgehändigt werden. Damit soll verhindert werden, daß nichtöffentlich behandelte Themen an die Öffentlichkeit gelangen. So verbietet § 36 Abs. 2 Satz 5 SächsLkrO auch die Einsichtnahme in Protokolle über nichtöffentliche Sitzungen durch die Einwohner, und zwar auf Dauer.

Der Landrat hätte demnach das Protokoll nicht an den Kreisrat herausgeben dürfen.

3. Verschwiegenheitspflichten des Kreistages

Nach § 17 Abs. 1 SächsLkrO haben die ehrenamtlich tätigen Kreisräte die ihnen übertragenen Aufgaben *uneigennützig* und *verantwortungsbewußt* zu erfüllen. Hierauf sind sie nach § 31 Abs. 1 Satz 2 SächsLkrO ausdrücklich zu verpflichten. Hierzu gehört auch die Pflicht zur Verschwiegenheit in allen Angelegenheiten, deren Geheimhaltung gesetzlich vorgeschrieben, besonders angeordnet oder ihrer Natur nach erforderlich ist.

Unter die Verschwiegenheitspflicht fallen auch alle in nichtöffentlicher Sitzung behandelten Angelegenheiten, und zwar so lange, bis der Kreistag den Kreisrat im Einvernehmen mit dem Landrat von der Schweigepflicht entbindet (§ 33 Abs. 2 SächsLkrO).

Dem Schreiben des Landrats entnahm ich, daß eine solche förmliche Entbindung des Kreisrats nicht erfolgt war, so daß das Verwertungsverbot des § 17 Abs. 2 Satz 2 SächsLkrO eingriff. Danach ist die Verwertung von Sachverhalten, die der Verschwiegenheitspflicht unterliegen (hier aus nichtöffentlicher Sitzung) z. B. dann untersagt, wenn der zur Verschwiegenheit verpflichtete Kreisrat (hier als privater Prozeßbeteiligter) Maßnahmen unter Ausnutzung seiner Kenntnisse - also in eigennütziger Weise - trifft (hier die unbefugte Verwertung einer unzulässigerweise erhaltenen Sitzungsniederschrift in einem Zivilprozeß).

Eine solche - nicht verantwortungsbewußte - Handlungsweise, die sowohl gegen § 17 Abs. 1 SächsLkrO als auch gegen § 17 Abs. 2 SächsLkrO verstößt, kann mit einem Ordnungsgeld bis zu 1.000,- DM geahndet werden (§ 17 Abs. 4 SächsLkrO).

4. Information der Presse/der Öffentlichkeit durch den Kreisrat

Die Ausführungen unter 3 treffen im wesentlichen auch auf diese Handlungsweise zu. Hinzu kommt, daß sich die Verschwiegenheitspflicht des Kreisrats nicht nur auf die in nichtöffentlicher Sitzung behandelten Gegenstände (§ 33 Abs. 2 SächsLkrO), sondern gemäß § 17 Abs. 2 SächsLkrO auf *alle* Angelegenheiten bezieht, die ihm bei seiner ehrenamtlichen Tätigkeit bekannt geworden sind (sie brauchen jedoch diese Tätigkeit nicht selbst betreffen). Die Vorschrift geht nach der allgemeinen Lebenserfahrung davon aus, daß Personen, die sich im amtlichen Bereich bewegen, mitunter von Angelegenheiten Kenntnis erlangen, die nicht unmittelbar mit ihrer Tätigkeit zusammenhängen (hier Kenntnisse über die Abmahnung einer Landkreisbediensteten).

Neben dem Ordnungsgeld nach § 17 Abs. 4 SächsLkrO kommt möglicherweise auch die Anwendung des § 203 Abs. 2 und 5 StGB in Betracht, da ein Kreisrat Amtsträger i. S. v. § 11 Abs. 1 Nr. 2 Buchst. b StGB ist. Auch die §§ 32, 33 SächsDSG könnten als Sanktionsmöglichkeit in Frage kommen.

Nach alledem kam ich zu dem Ergebnis, daß dem Datenschutz im Kreistag insgesamt mehr Bedeutung beizumessen ist. Ich habe den Landrat gebeten, meine Stellungnahme dem Kreistag zur Kenntnis zu bringen, und unter dieser Voraussetzung von einer förmlichen Beanstandung nach § 26 SächsDSG abgesehen.

5.5.2 Datenschutz im Gemeinderat: Behandlung von Steuerangelegenheiten

Eine Stadtverwaltung hatte Zweifel, ob Steuerangelegenheiten (hier der Erlaß bzw. die Niederschlagung von Steuerschulden) von den Stadträten in ihren Sitzungen erörtert werden dürfen.

Die Stadtverwaltung vertrat die Auffassung, daß einer Behandlung von Steuerangelegenheiten im Gemeinderat das Steuergeheinmis entgegensteht, selbst wenn darüber in nichtöffentlicher Sitzung verhandelt werden würde. Weil in der Hauptsatzung dem Stadtrat Abgabenangelegenheiten, insbesondere auch Erlaß und Niederschlagungen, zur Aufgabenerledigung zugewiesen sind, waren die Stadträte hingegen der Meinung, daß Steuerangelegenheiten in ihre uneingeschränkte Zuständigkeit fielen und sie somit das Recht hätten, die erforderlichen ins einzelne gehenden Angaben zu den betreffenden Steuerpflichtigen mitgeteilt zu bekommen. Nur so könne sachgemäß entschieden werden.
In Anbetracht der häufig auftretenden Problematik bat mich die Stadtverwaltung um Stellungnahme, insbesondere auch zu der Frage, ob die Stadträte Amtsträger im Sinne der Abgabenordnung seien.

Ich habe der Stadtverwaltung folgendes mitgeteilt:

Da Stadträte in einem öffentlichen Amtsverhältnis stehen, fallen sie unter den Amtsträgerbegriff nach §§ 7 Nr. 3 AO, 11 Abs. 1 Nr. 2 Buchst. b StGB und haben somit das Steuergeheimnis (§ 30 Abs. 1 AO) zu wahren. Hierauf sind die Stadträte ausdrücklich hinzuweisen.
Deshalb bestehen keine Bedenken, wenn die Stadträte im Rahmen ihrer Aufgabenzuweisung über Steuerangelegenheiten im Gemeinderat beraten. Um eine Verletzung des Rechts auf informationelle Selbstbestimmung der Betroffenen auszuschließen, muß darüber allerdings in *nichtöffentlicher* Sitzung verhandelt werden.

Zwar sind nach § 37 Abs. 1 SächsGemO Gemeinderatssitzungen grundsätzlich öffentlich abzuhalten, soweit jedoch Beratungsgegenstände das Recht auf informationelle Selbstbestimmung und damit die schutzwürdigen Belange eines Betroffenen beeinträchtigen können, ist die Öffentlichkeit auszuschließen. Dies ist insbesondere bei Steuerangelegenheiten, aber auch z. B. bei Personalangelegenheiten, Grundstücksangelegenheiten, Erörterungen persönlicher oder wirtschaftlicher Verhältnisse, bei Zuschußgewährung an einzelne Personen sowie Rechtsstreitigkeiten zwischen Stadt und Bürger der Fall.

Deshalb scheidet auch die Bekanntgabe der in nichtöffentlicher Sitzung gefaßten

Beschlüsse auf Dauer immer dann aus, wenn durch Bekanntgabe personenbezogener Sachverhalte schutzwürdige Interessen der Betroffenen beeinträchtigt werden können. Allenfalls könnten die gefaßten Beschlüsse in anonymisierter Form, also ohne Personenbezug, veröffentlicht werden.

5.5.3 Nochmals: Tonband- und Videoaufnahmen in öffentlichen Gemeindratssitzungen

Im 4. Tätigkeitsbericht (5.5.2) habe ich vertreten, daß vor Tonband- und Videoaufzeichnungen in öffentlichen Gemeinderats- und Kreistagssitzungen (z. B. zu Protokollzwecken oder durch die Presse) die Einwilligung der Redner (die durch Handheben erklärt werden kann) eingeholt werden muß.

Die Frage, ob die Einwilligung dann entbehrlich ist, wenn die Geschäftsordnung solche Tonband- und Videoaufzeichnungen zuläßt, habe ich aus folgenden Gründen bejaht:

Das gesprochene Wort darf auf ein Tonband aufgenommen und eine Person mit einer Videokamera nur dann aufgezeichnet werden, wenn eine *Rechtsvorschrift* dies (unter Angabe des Zwecks) ausdrücklich erlaubt oder der Betroffene eingewilligt hat (vgl. BVerfG NJW 1973, 891; BGH NJW 1995, 1955, jeweils m.w.N.). Nach der Auffassung des Bundesverwaltungsgerichts (NVwZ 1988, 1119), die ich teile, haben auch die Geschäftsordnungen kommunaler Vertretungsorgane die Qualität von Rechtsvorschriften, weil sie verbindlich und abstrakt-generell die Rechte und Pflichten der Mitglieder dieser Organe regeln. Der Eingriff in das Persönlichkeitsrecht ist - davon hat mich ein Abgeordneter des Landtages überzeugt - auch kaum noch spürbar, weil er als sozialadäquat empfunden wird. Man denke auch an anwesende Pressevertreter oder an örtliche TV-Sender.

Läßt also die gemeindliche Geschäftsordnung Tonband- und Videoaufnahmen in öffentlichen Gemeinderatssitzungen zu, bedarf es einer Einwilligung der Redner nicht.

5.5.4 Veröffentlichung personenbezogener Daten in kommunalen Mitteilungsblättern

Ein Kommunalamt machte mich auf die Veröffentlichung personenbezogener Jubiläumsdaten und daneben von Gewerbetreibendendaten im Amtsblatt einer sächsischen Stadt aufmerksam und bat mich um datenschutzrechtliche Bewertung.

Nach § 33 Abs. 2 SächsMG darf die Meldebehörde Namen, Doktorgrad, Anschriften, Tag und Art des Jubiläums u. a. von *Altersjubilaren* (Altersjubilare sind Einwohner, die den 70. oder einen höheren Geburtstag begehen) veröffentlichen und an Presse, Rundfunk oder andere Medien zum Zwecke der Veröffentlichung übermitteln.
Die gilt nicht, soweit die Betroffenen für eine Justizvollzugsanstalt, für ein Krankenhaus, Pflegeheim oder eine ähnliche Einrichtung i. S. v. § 20 Abs. 1 SächsMG gemeldet sind (besondere Meldeverhältnisse), eine Auskunftssperre besteht oder die

Betroffenen der Auskunftserteilung, der Veröffentlichung oder der Datenübermittlung widersprechen (§ 33 Abs. 4 Satz 1 SächsMG). Auf das Widerspruchsrecht hat die Meldebehörde bei der Anmeldung (§ 33 Abs. 4 Nr. 1 SächsMG) und mindestens einmal jährlich durch öffentliche Bekanntmachung (§ 33 Abs. 4 Nr. 3 SächsMG) hinzuweisen.
Im vorliegenden Fall wurden von der Stadt Jubiläumsdaten auch der unter 70jährigen veröffentlicht, was nur mit deren Einwilligung hätte erfolgen dürfen (§ 4 Abs. 1 Nr. 2 und Abs. 2 und 3 SächsDSG).

Bei der Veröffentlichung von *Gewerbedaten* muß § 14 Abs. 8 Satz 1 GewO beachtet werden. Danach dürfen der Name, die betriebliche Anschrift und die angezeigte Tätigkeit des Gewerbetreibenden an Private nur bei Vorliegen eines berechtigten Interesses übermittelt werden. Von einem solchen berechtigten Interesse konnte im vorliegenden Fall wohl schon deshalb nicht ausgegangen werden, weil es bereits an einem entsprechenden Auskunftsbegehren mangelte. Die Daten der Gewerbetreibenden hätten allenfalls mit deren Einwilligung gemäß § 4 Abs. 1 Nr. 2 und Abs. 2 und 3 SächsDSG veröffentlicht werden dürfen.

Die Stadtverwaltung wird dafür sorgen, daß im Mitteilungsblatt zukünftig nur noch die Jubilare ab dem 70. Geburtstag genannt und die Einwohner auf das Widerspruchsrecht nach § 33 Abs. 4 SächsMG hingewiesen werden. Daten von Gewerbetreibenden werden im Mitteilungsblatt künftig nicht mehr veröffentlicht.

5.5.5 Einwohneranhörung in Gemeinden, deren Gemeindegebiet durch Gesetz geändert werden soll

Das SMI hat die Umlandgemeinden Dresdens, deren Gemeindegebiet durch Gesetz geändert werden soll, per Erlaß u. a. angewiesen, schriftlich und personenbezogen festzuhalten, welche Einwohner in den öffentlich auszulegenden Gesetzentwurf mit Begründung und die dazugehörigen Karten Einsicht genommen haben. Erst durch zähes Verhandeln konnte ich das SMI überzeugen, daß eine solche personenbezogene Datenerhebung nicht erforderlich ist und eine (anonyme) Strichliste zur Feststellung des Einwohnerinteresses am Gemeindegeschehen völlig ausreicht. In einer ergänzenden Weisung wurden die betroffenen Gemeinden vom SMI schließlich aufgefordert, "von einer Kenntlichmachung der in den Gesetzentwurf einsichtnehmenden Personen aus datenschutzrechtlichen Gründen abzusehen". Warum man nicht in klarem Deutsch schreibt, *daß die Namen nicht notiert werden dürfen, weil dazu die nötige Rechtsgrundlage fehlt*, lasse ich offen.

5.5.6 Stärkung der Stellung der behördlichen Datenschutzbeauftragten im Kommunalbereich

§ 9 Abs. 2 Nr. 10 SächsDSG schreibt vor, daß öffentliche Stellen ihre innere Organisation so zu gestalten haben, daß sie den besonderen Anforderungen des Datenschutzes gerecht werden. Hierunter fällt auch die Bestellung eines behördlichen Datenschutzbeauftragten. Das Gesetz enthält zwar keine Pflicht dazu, ich rate aber in allen größeren Behörden zu dieser Maßnahme, zumal die EG-Datenschutzrichtlinie ab 1999 nur dann von Meldepflichten dispensiert, wenn eine interne und externe Datenschutzkontrolle gesichert ist.

Nach §§ 64 Abs. 1 und 3 SächsGemO, 60 Abs. 1 und 4 SächsLkrO sind Beauftragte in Ausübung ihrer Tätigkeit *unabhängig* und können an den Sitzungen des Gemeinderats bzw. des Kreistags und der für ihren Aufgabenbereich zuständigen Ausschüsse mit beratender Stimme teilnehmen.

Es dürfte symptomatisch für viele sächsische Kommunalbehörden sein, daß - wie ich in verschiedenen Landratsämtern und Städten feststellen mußte - Beschäftigte in untergeordneter Funktion zwar mit Datenschutzaufgaben betraut wurden, jedoch wegen der damit verbundenen Unabhängigkeit eine förmliche Bestellung nach §§ 64 SächsGemO, 60 SächsLkrO unterblieb. Die abhängige Stellung, in der sich die Betroffenen befinden, führt vielfach zu Defiziten im kommunalen Datenschutz. So wurde z. B. einem "Datenschutzkoordinator" untersagt, sich in Datenschutzfragen selbständig mit mir in Verbindung zu setzen. Dafür habe ich kein Verständnis, es sei denn, man hat etwas zu verbergen.

Ich habe das SMI als oberste Kommunalaufsichtsbehörde gebeten, die sächsischen Kommunalbehörden unter Hinweis auf die Verpflichtungen aus § 9 Abs. 2 Nr. 10 SächsDSG aufzufordern, unabhängige behördliche Datenschutzbeauftragte gemäß §§ 64 SächsGemO, 60 SächsLkrO formell zu bestellen. Die Landratsämter und Gemeinden sind gut beraten, so zu verfahren.

5.5.7 Online-Anbindung städtischer Rechnungsprüfungsämter am Beispiel „Zugriff auf Kfz-Zulassungsdaten“

Eine kreisfreie Stadt fragte, ob es zulässig sei, dem Rechnungsprüfungsamt (RPA) einen *permanenten* Online-Zugriff auf personenbezogene Daten im Kfz-Zulassungsverfahren zu gestatten. Sie hatte im Hinblick auf Abschnitt 5.11.3 meines 3. Tätigkeitsberichts, wo ich den abschließenden Charakter des § 36 Abs. 1 und 2 StVG für automatisierte Abrufe aus dem örtlichen und dem zentralen Fahrzeugregister herausgestellt habe, Zweifel an der Rechtmäßigkeit des Vorhabens.

In meiner Stellungnahme verwies ich zunächst auf § 18 Abs. 1 KomPrO, wonach sich die Rechnungsprüfung grundsätzlich auf Stichproben erstrecken soll (Ausnahme: Kassenbestandsaufnahme). Eine sog. Visaprüfung (permanente Prüfung aller

Vorgänge) wäre schon wegen ihrer Unverhältnismäßigkeit unzulässig. Dies gilt insbesondere auch für die Einrichtung einer *permanenten* Online-Anbindung für das RPA, die - da es sich um eine innerstädtische Angelegenheit handelt - an den in § 8 Abs. 2 SächsDSG genannten Voraussetzungen zu messen wäre (so daß nicht nach § 8 Abs. 1 SächsDSG ein besonderes Gesetz erforderlich wäre) und außerdem meiner Beteiligung bedürfte (§ 8 Abs. 3 SächsDSG).

Gleichwohl kann eine *temporäre* Online-Anbindung des RPA zur Erfüllung eines *konkreten Prüfungsauftrags* unter folgenden Voraussetzungen als angemessen angesehen werden:

- Herr der Daten bleibt die speichernde Stelle (Zulassungsstelle),
- die Zeitdauer der Online-Anbindung ist vorher festzulegen (für die Dauer des Prüfungsauftrags), also keine permanente Zugriffsberechtigung,
- nach Erledigung des Prüfungsauftrags ist die Zugriffsberechtigung zu löschen (Benutzercode, Paßwort),
- nur Leseberechtigung für das RPA (also keine Schreibrechte),
- Sicherstellung im RPA, daß nur der zuständige Rechnungsprüfer auf die für die Prüfung erforderlichen Daten zugreifen darf,
- Sicherstellung im RPA, daß Auswertungen (z. B. Bildschirmausdrucke) datenschutzgerecht zusammen mit den übrigen Prüfungsunterlagen sicher aufbewahrt werden und, sobald sie entbehrlich sind, datenschutzgerecht vernichtet werden (z. B. Reißwolf, DIN 32757),
- Protokollierung der Abrufe, damit zumindest stichprobenweise festgestellt werden kann, wer wann auf welche Daten zugegriffen hat,
- weiteres dazu in meiner Bekanntmachung zur Zulässigkeit automatisierter Abrufverfahren (§ 8 SächsDSG) vom 29. Juni 1994 (SächsABl. S. 976).

Nach § 17 Abs. 2 KomPrO haben die Gemeinden den Prüfer zu unterstützen. Der Prüfer kann (ähnlich wie der Sächsische Datenschutzbeauftragte nach § 25 SächsDSG) *alle* Auskünfte und Unterlagen verlangen sowie eigene Erhebungen vornehmen, die zur Erfüllung seiner Aufgaben erforderlich sind. Hierzu kann auch eine Online-Anbindung dienlich sein.

§ 36 StVG ändert nichts an der Zugriffsberechtigung des RPA auf das Fahrzeugregister (unter den vorstehenden Voraussetzungen). Die Zweckbestimmung der Fahrzeugregister (Kraftfahrtbundesamt, örtliches Fahrzeugregister) ist in § 32 StVG geregelt. Demzufolge kann sich § 36 StVG auch nur im Rahmen dieser Zweckbestimmung (und zwar abschließend) bewegen. Für (Prüfungs-)Befugnisse außerhalb der Zweckbestimmung des § 32 StVG gilt nach § 46 StVG das SächsDSG mit der Folge, daß die Online-Anbindung des RPA an das örtliche Fahrzeugregister an § 8 Abs. 2 SächsDSG zu messen ist. Ferner liegt bei der Nutzung der Fahrzeugregisterdaten durch das RPA keine Zweckänderung vor (§ 12 Abs. 3 SächsDSG).

5.5.8 Drohende Obdachlosigkeit - Mitteilungen der Wohnungsbaugesellschaften an das Amt für Wohnungswesen

In die vertraglichen Vereinbarungen zwischen der Landeshauptstadt Dresden und den städtischen Wohnungsbaugesellschaften ("Wobas") über Belegungsrechte sollte folgender neue Passus aufgenommen werden:
"Vor Ausspruch einer beabsichtigten fristlosen Mietvertragskündigung ist das Amt für Wohnungswesen seitens des Wohnungsunternehmens unverzüglich zu konsultieren."

Die beteiligten Stellen, einschließlich der Datenschutzaufsichtsbehörde für den nichtöffentlichen Bereich interpretierten diese Vertragsregelung als Verpflichtung zu einer Übermittlung *personenbezogener* Daten durch die Woba an das Amt für Wohnungswesen.

Dieser Ansicht hielt ich entgegen, daß die beabsichtigte Vertragsänderung, nämlich die Einführung einer Pflicht, vor Ausspruch einer fristlosen Kündigung das Amt für Wohnungswesen zu *konsultieren*, keinesfalls - dem Erforderlichkeitsgrundsatz folgend - zwingend eine Übermittlung personenbezogener Daten der zu Kündigenden zur Folge haben muß. Vielmehr hat die Woba nach meinem Verständnis dem Amt für Wohnungswesen lediglich die Tatsache (also ohne Namen) mitzuteilen, daß einer bestimmten Anzahl von Mietern fristlos gekündigt werden soll und zu fragen, ob das Amt für Wohnungswesen eine Möglichkeit sieht, die Betroffenen vor drohender Obdachlosigkeit zu bewahren. Sollte vom Amt für Wohnungswesen der entsprechende Wohnraum zur Verfügung gestellt werden können, kann die Woba die zu Kündigenden auffordern, sich mit dem Amt für Wohungswesen zwecks Zuweisung einer Unterkunft in Verbindung zu setzen. Hierfür könnte eine entsprechende Bescheinigung über die bevorstehende fristlose Kündigung zur Vorlage beim Amt für Wohnungswesen dienlich sein.

Sollten die Betroffenen von einem solchen Angebot - aus welchen Gründen auch immer - nicht Gebrauch machen wollen, ist dies eine Entscheidung, die die Woba wohl akzeptieren müßte. Jedenfalls sehe ich für eine Datenübermittlung gegen den Willen der Betroffenen keine Grundlage.

Das Amt für Wohnungswesen hat mir mitgeteilt, daß personenbezogene Datenübermittlungen von den Wohnungsbaugesellschaften nicht (mehr) verlangt würden.

5.5.9 Videoüberwachung der Standorte von Wertstoffcontainern

Ein Landratsamt fragte mich, ob die Standorte von Wertstoffcontainern mit Videokameras überwacht werden dürfen, um Verstöße gegen die Abfallentsorgungssatzung des Landkreises festzustellen. Häufig würden Reststoffe in die falschen Container geworfen oder einfach neben den Behältern abgelagert. Dabei entstünden Dreckecken und zusätzliche Kosten.

Videoüberwachung im öffentlichen Bereich ist ein Eingriff in das Grundrecht auf informationelle Selbstbestimmung, der einer tragfähigen Rechtsgrundlage bedarf.

Ordnungswidrig handelt nach § 66 Abs. 1 SächsLKrO, wer vorsätzlich oder fahrlässig einer aufgrund von § 3 Abs. 1 oder § 12 SächsLKrO erlassenen Satzung zuwiderhandelt, soweit die Satzung für einen bestimmten Tatbestand auf diese Bußgeldvorschrift verweist. Die vorliegende Abfallentsorgungssatzung nennt solche Tatbestände, z. B. vorschriftswidriges Behandeln, Bereitstellen, Benutzen und Aufstellen der Abfallbehälter und gibt an, wer dafür haftet (Anschlußpflichtige oder Verursacher).

Für den Vollzug des 1. Gesetzes zur Abfallwirtschaft und zum Bodenschutz im Freistaat Sachsen (EGAB) sind die Landkreise als untere Abfallbehörden zuständig (§ 13 Abs. 2 Nr. 3 EGAB und § 13 Abs. 3 i. V. m. § 1 Abs. 1 der Zuständigkeitsverordnung ABoZUV). In diesem Rahmen trifft der zuständige Landkreis Maßnahmen, die ihm erforderlich erscheinen. Die Ermittlung zur Feststellung von Ordnungswidrigkeiten kann das zuständige Landratsamt auch selbst durchführen; nach § 64 Abs. 1 Satz 4 SächsPolG sind die Landratsämter zugleich Kreispolizeibehörden.

Für eine Videoüberwachung zur Ermittlung von Ordnungswidrigkeiten existiert aber keine spezialgesetzliche Grundlage. Nur wenn die Ermittlung einer Ordnungswidrigkeit der Polizei übertragen wird, greifen die Datenschutznormen des Sächsischen Polizeigesetzes (§§ 37 ff. SächsPolG).

So bleibt nur das Sächsische Datenschutzgesetz als Rechtsgrundlage:
In jedem Einzelfall sind Geeignetheit, Erforderlichkeit und Angemessenheit der datenverarbeitenden Maßnahme zu prüfen. Die Videoüberwachung muß also ein geeignetes Mittel sein, um Ordnungswidrigkeiten zu verhindern oder aufzuklären. Sie darf im Einzelfall z. B. den Bürger nicht vertreiben und veranlassen, seine Wertstoffe unbeobachtet in das nächste Gebüsch zu werfen. Es muß klar geregelt sein, wie durch Videobilder der Täter identifiziert werden soll, sonst ist die Videoüberwachung sinnlos.

Die Videokamera muß so eingestellt sein, daß sie Unbeteiligte, die sich in angrenzenden Bereichen aufhalten, nicht aufnimmt. Falls eine abschreckende Stichprobenkontrolle (zeitweilige Einschaltung der Kamera) für die Zweckerfüllung

genügt, hat man sich auf sie als das mildere Mittel zu beschränken.

Die Videoüberwachung muß dem Ermittlungszweck angemessen sein, d. h. "das Maß der den Einzelnen [...] treffenden Belastung [muß] in einem vernünftigen Verhältnis zu dem der Allgemeinheit erwachsenden Vorteil stehen" (BVerfGE 76, 1, 51). Anders ausgedrückt: Das geprüfte Mittel darf nicht außer Verhältnis zu dem verfolgten Zweck stehen (BVerfGE 70, 278, 286; vgl. auch § 3 Abs. 3 SächsPolG). So wäre eine Videoüberwachung an einem Standort mit einer Häufung massiver Ordnungswidrigkeiten („Ordnungswidrigkeitsschwerpunkt“) zulässig, so daß die Unbeteiligten - im Interesse der Allgemeinheit - einen Eingriff in ihr Recht auf informationelle Selbstbestimmung beim Abliefern ihres Abfalls hinnehmen müßten.

Bei der Beurteilung der Frage, ob die Verwertung von Videoaufnahmen in einem Bußgeldverfahren zulässig ist, muß ein gegenüber dem Eingriff in das Recht auf informationelle Selbstbestimmung überwiegendes Interesse der Allgemeinheit an der Verfolgung des einzelnen Verstoßes feststehen. Weiter muß die Verwertung der Aufnahmen für die Ermittlung der Ordnungswidrigkeit verhältnismäßig sein (vgl. BVerfGE NJW 1990, 563).

Vor dem videoüberwachten Bereich sollte ein deutliches Hinweisschild angebracht sein. Es "hilft" jedem, sich richtig zu verhalten.

Zum Schutz des Rechts auf informationelle Selbstbestimmung kommen weitere Maßnahmen in Betracht:

a) technische Maßnahmen:
- griffsichere Anbringung der Videokamera
- präzise Einstellung des Bildausschnittes
- Aufzeichnung nur im unbedingt erforderlichen Umfang (zeitlich eingeschränkt)
- sichere Löschung nicht benötigter Datenträger bzw. automatisches Überschreiben

b) organisatorische Maßnahmen:
- Dienstanweisung über den zweckgebundenen Umgang mit den Bildaufnahmen
- Regelungen darüber, wann die als Beweismittel für Ordnungswidrigkeitsverfahren nicht benötigten Aufnahmen zu löschen sind (spätestens nach 48 Stunden), wie Verstöße und Täter zu identifizieren sind und wann geprüft wird, ob die Anlage abzubauen ist, weil ihr Zweck erreicht und sie deswegen nicht mehr erforderlich ist (vgl. § 3 Abs. 4 SächsPolG)
- Aufnahme der Geräte in das Datei- und Geräteverzeichnis nach § 10 Abs. 1 SächsDSG
- Vertrag mit einem Wartungsunternehmen, der den Anforderungen an eine Auftragsdatenverarbeitung (vgl. § 7 SächsDSG) genügt.

c) personelle Maßnahmen:
- Auswahl, Belehrung und schriftliche Festlegung der Personen, die mit der Auswertung, Verarbeitung und Löschung betraut werden
- Festlegung des davon ausgeschlossenen Personenkreises, der eben keinen Zugriff hat (Problem: Wartungskräfte, Reinigungskräfte).

Also: Sowohl der einmalige als auch der laufende Aufwand für den ordnungsgemäßen Betrieb einer Videoüberwachungsanlage ist hoch. Im Regelfall dürfte er so teuer sein, daß er sich nicht lohnt. Besser ist es, den Containerstandort gut zu beleuchten, ihn zum Verkehrsraum zu öffnen und regelmäßig zu reinigen.

Wenn hinreichend positive praktische Erfahrungen mit der Videoüberwachung vorliegen, könnte das Verfahren in die Abfallentsorgungssatzung eingearbeitet werden.

5.6 Baurecht / Wohnungswesen

In diesem Jahr nicht belegt. Vgl. unter 5.7.11 und 5.7.13.

5.7 Statistikwesen

5.7.1 VO über die Frauenförderungs-Statistik

Im letzten Tätigkeitsbericht (5.7.2) habe ich darauf hingewiesen, daß die erste Anordnung einer sächsischen Landesstatistik in Gestalt der Sächsischen Frauenförderungsstatistikverordnung vom 22. August 1995 aus datenschutzrechtlicher Sicht fehlgeschlagen ist.

Die Leitstelle für die Gleichstellung hat auf der Grundlage dieser Verordnung eine Verwaltungsvorschrift erarbeitet (SächsABl. 1996 S. 644). Sie schreibt den nach der Verordnung berichtspflichtigen Dienststellen die Benutzung bestimmter Erhebungsbögen vor.

Verwaltungsvorschriften werden durch die Organisations- und Weisungsbefugnis der sie erlassenden Instanz bestimmt und begrenzt (Maurer, Allgemeines Verwaltungsrecht, 9. Aufl. 1994, § 24 Rdnr. 18). Daraus folgt auch, daß die Verwaltungsvorschriften nur innerhalb eines Verwaltungsträgers verbindlich sind, es sei denn, daß ausnahmsweise auch Organe anderer Verwaltungsträger der *Fachaufsicht* der die Verwaltungsvorschrift erlassenden Behörde unterliegen (vgl. Maurer a. a. O.). An eben jener Fachaufsicht der Staatsministerin gegenüber den nicht-staatlichen Stellen fehlt es jedoch. Die Staatsministerin ist im Verhältnis zu ihnen weder vorgesetzte Frauenförderungsbehörde noch Frauenförderungsstatistikbehörde.
Es steht außer Frage, daß solche nicht-staatlichen Einrichtungen zur Erstellung eines Frauenförderplanes und zur Durchführung einer Frauenförderungsstatistik gemäß §§ 4, 5 SächsFFG verpflichtet sind. Es hätte jedoch nicht der Eindruck erweckt werden dürfen, als sei die Anordnung der Verwendung bestimmter Erhebungsbögen gegenüber dem nicht-staatlichen Bereich von der Organisations- und Weisungsbefugnis der Staatsministerin umfaßt.

Auch hinsichtlich des statistischen Meldeweges ist die Verwaltungsvorschrift der rechtswidrigen Regelung der Verordnung gefolgt. Sie sieht vor, daß die Dienststellen des nachgeordneten Geschäftsbereiches sowie der Landtag und der Rechnungshof, aber auch die der Aufsicht des Freistaates unterstehenden juristischen Personen des öffentlichen Rechts wie namentlich die Kommunen und die Hochschulen, die ausgefüllten Erhebungsbögen auf dem Dienstweg dem jeweils zuständigen Ressort bzw. der obersten Rechtsaufsichtsbehörde bzw. der Staatskanzlei zu überlassen haben. Erst dann werden sie dem Statistischen Landesamt übermittelt. Wie im 4. Tätigkeitsbericht (unter 5.7.2, zu Buchstabe b) dargelegt, handelt es sich um einen Verstoß gegen das statistikrechtliche Grundgebot der frühestmöglichen

Anonymisierung, eine Ausprägung des verfassungsrechtlichen Grundsatzes der Verhältnismäßigkeit.

Ich habe mir in diesem Fall ganz besondere Mühe gegeben, gangbare Wege aufzuweisen, z. B. angeregt, eine Verwendungsempfehlung für die Erhebungsvordrucke mit den Kommunalen Spitzenverbänden abzustimmen. Dazu ist es aber bisher nicht gekommen.

Vgl. weiter dazu auch unter 5.7.5.

5.7.2 Empirische Mietspiegel als Kommunalstatistik

Bis Ende des Jahres gelten für die Höhe des Mietzinses für Wohnraum noch die Sonderregeln des *Gesetzes zur Überleitung preisgebundenen Wohnraums im Beitrittsgebiet in das allgemeine Miethöherecht* vom 6. Juni 1995 (BGBl. I S. 748). Mit dem Auslaufen dieses sog. Mietenüberleitungsgesetzes gilt ab 1. Januar 1998 auch in den neuen Bundesländern das in Westdeutschland vor rund 25 Jahren eingeführte *Vergleichsmietensystem*. Es schreibt ein bestimmtes Verfahren für die Begründung einer Mieterhöhung in Anpassung an die ortsübliche Vergleichsmiete vor. Zum Nachweis dafür, wie hoch die ortsübliche Miete für die betreffende Wohnung ist, sind in § 2 Abs. 2 MHRG drei Mittel zugelassen: Neben der Benennung dreier ähnlicher Wohnungen oder der Vorlage des Gutachtens eines öffentlich bestellten oder vereidigten Sachverständigen kann der Vermieter sich auch auf einen sog. Mietspiegel berufen, das ist nach dem Gesetz (§ 2 Abs. 2 Satz 2, 1. Halbsatz MHRG) eine *von der Gemeinde oder von Interessenvertretern der Vermieter und der Mieter gemeinsam erstellte oder anerkannte Übersicht über die üblichen Entgelte* (nach Maßgabe des § 2 Abs. 1 Nr. 2 MHRG).

Es liegt auf der Hand, daß es einfach und insbesondere kostengünstig und streitvermeidend sein kann, wenn den Mietvertragsparteien und den Gerichten ein Mietspiegel zur Verfügung steht.

Mietspiegel erstellen entweder die Gemeinde oder die Interessenvertreter der Mietvertragsparteien oder beide im Zusammenwirken. Es ist die Gemeinde, die zu entscheiden hat, ob sie einen Mietspiegel erstellen will, auf welcher Datengrundlage sie das tun will und in welcher Weise sie die örtlichen Interessenvertreter (Haus- und Grundbesitzerverein einerseits, Mieterverein andererseits) beteiligt.

Soweit die Gemeinde selbst empirische Einzeldaten für die Erstellung des Mietspiegels verarbeiten will und insbesondere sie die Daten neu bei einzelnen Mietvertragsparteien erheben will, handelt es sich um die Verarbeitung personenbezogener Daten durch eine öffentliche Stelle.
Immerhin wird nach Ausprägungen der Merkmale Art, Größe, Ausstattung, Beschaffenheit und Lage der Wohnung gefragt (§ 2 Abs. 1 Nr. 2 MHRG), und ebenso natürlich nach der Höhe der Miete.

Besondere Rechtsvorschriften über diese Datenerhebung fehlen. Zwar ermächtigt § 2 Abs. 5 Satz 4 MHRG die Bundesregierung, durch Rechtsverordnung mit Zustimmung des Bundesrates Vorschriften über den näheren Inhalt und das Verfahren zur Aufstellung und Anpassung von Mietspiegeln zu erlassen, aber davon ist bisher kein Gebrauch gemacht worden. Ein besonderes Mietspiegelgesetz, wie teilweise verlangt, hält die Bundesregierung, wie sie unlängst erklärt hat, für nicht erforderlich.

Die für die Erstellung eines empirischen Mietspiegels erforderliche Erhebung und Weiterverarbeitung von Daten findet gleichwohl nicht in einem rechtlich weitgehend ungeregelten Raum statt. Diese beruhigende Feststellung kann man allerdings nur dann treffen, wenn man der von mir aufgegriffenen Auffassung des namhaften Gelsenkirchener Mietrechtlers Ulf Börstinghaus (zum Mietspiegelrecht zuletzt NJW 1997, 977) folgt und die Datenverarbeitung zum Zwecke der Erstellung eines Mietspiegels als Statistik im Rechtssinne auffaßt.
Auch das SMI hat sich bisher mir gegenüber zustimmend zu dieser Auffassung geäußert. Ich hoffe, inzwischen auch das Statistische Landesamt von ihrer Richtigkeit überzeugt zu haben. Akzeptiert ist meine Auffassung von den drei großen Städten Sachsens, die mich gemäß § 8 Abs. 3 SächsStatG an der Erarbeitung von Satzungen über die Mietspiegel-Datenerhebung beteiligt haben.

Es sind folgende Gründe, die dafür sprechen, auch die Erstellung empirischer Mietspiegel (durch Gemeinden) als (amtliche) *Statistik im Rechtssinne* anzusehen:
Die definitionsähnlichen Bestimmungen in § 1 Abs. 1 und 2 SächsStatG (wie auch in § 1 BStatG) passen zwanglos auf die Erstellung empirischer Mietspiegel. Werden doch zur Deckung des Informationsbedarfs von Gesellschaft und Wirtschaft (Mieter und Vermieter) und auch Ländern (als den Rechtsträgern der für Mietstreitigkeiten zuständigen Tatsachen-Gerichte) Daten über Massenerscheinungen erhoben, gesammelt, aufbereitet und dargestellt.
Zudem trifft auf den Mietspiegel sicherlich zu, daß er zu den Voraussetzungen einer bestimmten am Sozialstaatsprinzip des Grundgesetzes orientierten Politik gehört, nämlich der Gestaltung der Beziehungen zwischen Mietern und Vermietern von Wohnraum, wie sie durch das geltende Recht reguliert wird.
Auch die allgemeinen Gebote, die § 1 Abs. 2 SächsStatG für die Statistik aufstellt, passen gut auf die Erstellung von Mietspiegeln.

Demgegenüber fallen die Besonderheiten, welche die Mietspiegel gegenüber dem klassischen Bereich der amtlichen Statistik aufweisen, wenig ins Gewicht:
Bei der Erstellung eines Mietspiegels werden die Einzel-Daten für die Gewinnung eines ganz bestimmten Tabellenwerkes, also einer - zu veröffentlichenden, § 2 Abs. 5 Satz 5 MHRG - ganz bestimmten, feststehenden Auswertung verwendet. Die Einzeldaten werden anders als im klassischen Kernbereich der amtlichen Statistik nicht für eine Fülle möglicher, nicht von vornherein feststehender Daten benutzt; vielmehr ist mit der Veröffentlichung des Mietspiegels die Auswertung der Einzeldaten vollständig beendet, eine Nutzung zu einer andersgearteten tabellarischen Aufbereitung

der erhobenen Einzeldaten scheidet aus. Es handelt sich um eine Statistik mit von vornherein beschränkter Funktion.
Eine weitere Besonderheit besteht darin, daß hier das Bundesrecht (Mietrecht) den Gemeinden eine Aufgabe auf dem Gebiet der Statistik überträgt.

Beide Besonderheiten sind aber vom Wortlaut der Statistikgesetze her kein Hindernis für eine Einordnung als Statistik im Rechtssinne. Und sie sind es auch nicht von den datenschutzrechtlich allein interessierenden *Rechtsfolgen* her:

Unter dem Gesichtspunkt des verfassungsrechtlichen Bestimmtheitsgebotes für alle Rechtsvorschriften, die einen Eingriff in Grundrechte wie dasjenige auf informationelle Selbstbestimmung erlauben dürfen, ist die Anwendung des Statistikrechtes auf die Erstellung empirischer Mietspiegel wohltuend: Durch § 2 Abs. 1 Nr. 2 MHRG ist das Erhebungsprogramm für einen empirischen Mietspiegel nur sehr grob umrissen. Über eine Satzung läßt sich das Erhebungsprogramm - und überhaupt der Grundrechtseingriff, z. B. eine mit der Gewinnung einer repräsentativen Stichprobe verbundene Nutzung schon vorhandener personenbezogener Daten - mit der nötigen Bestimmtheit regeln. Es ist sinnvoll, die Ermächtigung zu einer solchen Statistik nicht in der allgemeinen Satzungsermächtigung des § 4 SächsGemO, sondern in der Ermächtigung zum Erlaß von Satzungen über die Durchführung von Kommunalstatistiken in § 8 SächsStatG zu suchen. Dies zeigt sich an folgenden Besonderheiten dieser Vorschrift:
- Es gilt das Gebot vorrangiger Datenbeschaffung beim Statistischen Landesamt (§ 8 Abs. 2 SächsStatG), mit dem dazugehörigen Gebot, das Statistische Landesamt bei der Vorbereitung zu beteiligen, § 8 Abs. 3 SächsStatG. Diese Regel hat ihre Grundlage im verfassungsrechtlichen Grundsatz der Verhältnismäßigkeit.
- Die für Eingriffe in das Grundrecht auf informationelle Selbstbestimmung gebotene Schutzvorkehrung einer Beteiligung des Datenschutzbeauftragten (BVerfGE 65, 1, 46) wird konkret durch das Gebot des § 8 Abs. 3 SächsStatG sichergestellt; stützte man sich stattdessen auf die Satzungsermächtigung des § 4 SächsGemO, wäre dies naturgemäß nicht der Fall.

Ein weiterer Gesichtspunkt auf der Rechtsfolgen-Seite kommt hinzu:
Nach dem kraft Verfassungsrechtes zu beachtenden Grundsatz der informationellen Gewaltenteilung (Wahrung der grundsätzlichen Zweckbindung der bei öffentlichen Stellen vorhandenen personenbezogenen Daten) müßte, wenn man die Erstellung empirischer Mietspiegel nicht dem Statistikrecht unterwürfe, der Mietspiegel durch eine eigene Stelle im funktionellen Sinne, eben die *kommunale Mietspiegelstelle*, erstellt werden. Nur diese Stelle dürfte die Einzeldaten erheben, sammeln und Miethöhetabellen aggregieren.
Bei der Einordnung der Erstellung empirischer Mietspiegel als Statistik kann diese Aufgabe dagegen von einer bereits vorhandenen kommunalen Statistikstelle erledigt werden. Sofern die betreffende Gemeinde noch nicht über eine kommunale Statistikstelle verfügt, ist es ziemlich gleichgültig, ob sie nun für die Zwecke der Erstellung eine kommunale Statistikstelle oder eine eigene Mietspiegelstelle einrichtet.

Beide müssen in gleicher Weise nach den Geboten der informationellen Gewaltenteilung räumlich, personell, organisatorisch und durch Maßnahmen des technischen Datenschutzes von der übrigen Gemeindeverwaltung abgeschottet sein. Beide Stellen, kommunale Statistikstelle und kommunale Mietspiegelstelle, brauchen keine Dauereinrichtungen zu sein, worauf meine Behörde auf Veranstaltungen zur Mietspiegelerstellung nachdrücklich hingewiesen hat. Daneben gibt es die Möglichkeit einer Privatisierung der Durchführung dieser Statistik (vgl. allgemein zu deren Voraussetzungen Abschnitt 5.7.3 meines 4. Tätigkeitsberichts).

Diese rechtliche Einordnung der Erstellung empirischer Mietspiegel als Bestandteil der amtlichen Statistik führt zwar zu zusätzlichem Arbeitsanfall in meiner Behörde. Daß diese Arbeit geleistet werden muß, zeigen jedoch die vielen Verbesserungen, die ich bei den Dresdner, Leipziger und Chemnitzer (in zeitlicher Reihenfolge; jede mit bemerkenswert eigenständigen Lösungen!) Mietspiegelsatzungen bewirken konnte. Es müssen auch erst Erfahrungen mit den speziellen Anforderungen gesammelt werden, die an einen ersten und an spätere Mietspiegel unter den besonderen wohnungswirtschaftlichen Bedingungen in den größeren Gemeinden der neuen Bundesländer zu stellen sind. Hinzu kommt, daß die Anforderungen der Rechtsprechung der Zivilgerichte an Mietspiegel streng sind, was datenschutzrechtlich auf die Beurteilung der Erhebung personenbezogener Daten unter dem Gesichtspunkt der *Geeignetheit* (Erfordernis nach dem Grundsatz der Verhältnismäßigkeit) ohne weiteres durchschlägt. Für den letzten Münchener Mietspiegel (1994) ist rechtskräftig festgestellt worden, daß er kein geeignetes Erkenntnismittel im Mieterhöhungsprozeß ist. Das sollte in Sachsen vermieden werden.

5.7.3 Grundsatzfrage: Sofortaggregierung

Eine kleine sächsische Gemeinde beabsichtigte, zu Planungszwecken die Anzahl der in einem bestimmten Zeitraum eine bestimmte Straße befahrenden Kraftfahrzeuge festzustellen, und zwar durch Beobachtung des Verkehrs und entsprechende Eintragungen in eine Strichliste.
Die Gemeinde fragte bei mir an, ob sie für diese Verkehrszählung eine Statistiksatzung erlassen müsse und ob ich ihr ein Musterbeispiel für eine solche Satzung zur Verfügung stellen könne.

Für eine derartige Verkehrszählung bedarf es keiner Satzung und auch keiner kommunalen Statistikstelle.
Der Grund dafür und damit für den Unterschied zu der in meinem 4. Tätigkeitsbericht unter 5.7.7 dargestellten Verkehrserhebung liegt in Folgendem: Bei einer derartigen Verkehrszählung wird keinerlei individualisierendes Merkmal des betreffenden Kraftfahrzeuges erfaßt. Die Erhebung beschränkt sich darauf, die Eigenschaft des sich bewegenden Gegenstandes, Kraftfahrzeug zu sein, sowie die Tatsache der Bewegung über einen bestimmten Straßenpunkt in Gestalt eines reinen Zählvorganges festzuhalten. Es handelt sich um die Erhebung eines von vornherein personenbezugsfreien Umstandes.

Deswegen bedarf eine solche Datenerhebung keiner in den Bereich des allgemeinen Datenschutzrechtes oder bereichsspezifischer datenschutzrechtlicher Regelungen fallenden Erlaubnis.
Allerdings gewährt das Statistikrecht in Randbereichen einen über das allgemeine Datenschutzrecht hinausgehenden Schutz der persönlichen und geschäftlichen Sphäre. Insbesondere ist der Begriff der Einzelangabe im Statistikrecht weiter als der datenschutzrechtliche Grundbegriff des „personenbezogenen Datums“ (vgl. § 3 Abs. 1 SächsDSG). Das Statistikrecht erfaßt immer auch Datenerhebungen mit von vornherein äußerst hohem Anonymisierungsgrad.
Gleichwohl läßt eine sich auf einen bloßen Zählvorgang beschränkende Erhebung, die von vornherein mit Sicherheit einen Mindestzahlenwert erwarten läßt, der weit über der statistikrechtlichen Tabellenfelduntergrenze von 3 liegt, Einzelangaben gar nicht erst entstehen, insbesondere keine Einzelangaben, hinsichtlich deren vollständiger Anonymität irgendwelche Zweifel begründet wären.

Dieser bereits im Zusammenhang mit der im 4. Tätigkeitsbericht erwähnten Verkehrserhebung von mir geäußerten, seinerzeit aber nicht veröffentlichten Meinung ist das SMI damals beigetreten: Erhebungen von Massendaten in der Form der Sofortaggregierung fallen zumindest im Falle der schlichten Verkehrszählung nicht unter das Sächsische Statistikgesetz.

Bei dem Versuch, diese Ausnahme-Regel auf andersgeartete Sachverhalte zu übertragen, ist allerdings Vorsicht geboten.

5.7.4 Grenzen kommunaler Statistiken

Manche von sächsischen Gemeinden beschäftigten Statistiker können sich mit den Anforderungen, die das Sächsische Statistikgesetz und letztlich die Verfassungsordnung an die statistische Tätigkeit der Kommunen stellt, nicht abfinden.

Am weitesten geht insoweit die Stadt Leipzig. Sie mag nicht einsehen, daß im Freistaat Sachsen nach geltendem Recht - wie übrigens nach dem Recht des Bundes sowie etlicher Bundesländer - amtliche Statistiken auch dann einer Rechtsvorschrift als Grundlage bedürfen, wenn sie ohne Auskunftspflicht durchgeführt werden (vgl. § 6 Abs. 6, § 11 Abs. 1 SächsStatG, § 15 Abs. 1 Satz 1 BStatG). Dies entspricht der Rechtsentwicklung zur Einwilligung im allgemeinen Datenschutzrecht, also zur Einwilligung als Tatbestandsmerkmal von Datenverarbeitungs-Erlaubnisnormen.

Die Kommunen dürfen als Träger öffentlicher Gewalt Daten auch zu statistischen Zwecken nur innerhalb der durch den Verfassungsgrundsatz der Verhältnismäßigkeit gesetzten Grenzen sammeln. Das sich aus den einzelnen Erhebungsmerkmalen einer Kommunalstatistik zusammensetzende Erhebungsprogramm muß in allen seinen einzelnen Teilen rechtmäßig, nämlich zur Aufgabenerfüllung geeignet, erforderlich und angemessen sein.

Dementsprechend begrenzt das Sächsische Statistikgesetz die statistische Tätigkeit auch der kommunalen Körperschaften auf den (objektiven) "Informationsbedarf" (§ 1 Abs. 1 Satz 1) und speziell in § 8 Abs. 1 auf die Tätigkeit der kommunalen Körperschaften "zur Wahrnehmung ihrer Aufgaben".

Entgegen einer von der Stadt Leipzig mir gegenüber noch sechs Jahre nach der Wiedervereinigung vertretenen Auffassung hat die öffentliche Gewalt in Sachsen keinen "umfassenden Planungs- und Gestaltungsauftrag zur Daseinsvorsorge". Die kommunale Selbstverwaltung umfaßt keineswegs "alle Lebens- und Daseinsbereiche der Bewohner bzw. Nutzer der Einrichtungen einer Stadt". Ganz bewußt ist der umfassende Aufgabenkatalog der früheren Kommunalverfassung in der SächsGemO aufgegeben worden. Es gibt deshalb keine Vermutung für eine Erforderlichkeit von Informationen, weder was den Gegenstandsbereich noch was die Eingriffstiefe (Intimität) des Datums betrifft.
Art. 82 Abs. 2 SächsVerf ("im Rahmen der Gesetze") ist zu beachten. Jedes wesentliche Handeln der Verwaltung bedarf einer gesetzlichen Grundlage - so die Rechtsprechung des Bundesverfassungsgerichts (Wesentlichkeitstheorie). Daher enthält § 2 Abs. 1 der Sächsischen Gemeindeordnung die Einschränkung auf die *erforderlichen öffentlichen Einrichtungen*. Wie alle Ausübung öffentlicher Gewalt ist auch das grundsätzlich gewährte "Aufgabenfindungsrecht" der Gemeinde - neben der Gebietsgrenze, dem Bezug zur (gesamten) örtlichen Gemeinschaft und dem Vorrang der Gesetze - auch und vor allem durch den Grundsatz der Erforderlichkeit begrenzt.

Was zum traditionellen eigenverantwortlichen Aufgabenkreis - zumindest im Sinne eines Kernbereichs - der Gemeinden gehört, bestimmt sich nicht nach den Verhältnissen im vormundschaftlichen allsorgenden Staat, sondern nach der Verfassungsordnung des sich aus ordnungspolitischen Gründen zurückhaltenden und privater Initiative den Vortritt gewährenden, also freiheitlichen und sozialen Rechtsstaates.

Dies hat schließlich Folgen für die Art und Weise, in der meine Behörde gemäß § 8 Abs. 3 SächsStatG bei der Vorbereitung der Satzungen, in den Kommunalstatistiken anzuordnen sind, zu beteiligen ist: Es ist nicht pauschal, sondern Erhebungsmerkmal für Erhebungsmerkmal, eben mit rechtsstaatlicher Genauigkeit statt mit Phrasen, darzulegen, zur Erledigung welcher der Gemeinde nach der Rechtsordnung zustehenden Aufgabe die zu erhebende Information über Massenerscheinungen benötigt wird. Denn ohne eine solche konkrete Darlegung ist die rechtliche Prüfung durch eine nicht mit den Details städtischer Planung vertraute Stelle wie den unabhängigen Datenschutzbeauftragten (BVerfGE 65, 1, 46) nicht möglich.
Rechtsstaat bedeutet, außer in Randbereichen geringer Bedeutung, eine genaue Darlegungs- und Begründungs-Last bzw. -Pflicht. Wenn dies nicht schon zur Selbstkontrolle der handelnden Stelle geschieht, dann muß es jedenfalls zum Zwecke der rechtlich vorgeschriebenen Fremdkontrolle geschehen, also zur Verwirklichung des Grundsatzes der Gewaltenteilung.

Manchen mögen diese Fragen zunächst unbedeutend erscheinen. In Wahrheit stehen jedoch Grundfragen unseres Gemeinwesens auf dem Spiel. Ich werde in diesem Punkt nicht locker lassen und demnächst wohl förmliche Beanstandungen gegenüber der Stadt Leipzig, aber auch gegenüber der Stadt Dresden, aussprechen müssen.

5.7.5 Fehler bei der Privatisierung von Statistiken

Gegen die im 4. Tätigkeitsbericht unter 5.7.3 ausführlich dargestellten Regeln für eine Privatisierung amtlicher Statistiken ist in einzelnen Fällen verstoßen worden.

(1) In einem Fall ging der Verstoß von einer obersten Landesbehörde aus, obwohl man sich vorher eingehend von mir über die Voraussetzungen einer rechtmäßigen Durchführung des Vorhabens hatte beraten lassen, nämlich der „Untersuchung über die Situation der kommunalen Gleichstellungsbeauftragten im Freistaat Sachsen“, welche die Sächsische Staatskanzlei durch die Staatsministerin für Fragen der Gleichstellung von Frau und Mann bei einer sächsischen Fachhochschule in Auftrag gegeben hat.

Die Fachhochschule ist allen meinen Empfehlungen gefolgt und hat in dem den Fragebögen beigefügten Anschreiben alles vermieden, was als Hinweis auf eine Auftraggebereigenschaft des Freistaates hätte verstanden werden können. Dem Text war weder zu entnehmen, wer die Studie finanziert, noch auch, daß diese einen politikberatenden Zweck haben sollte.
Nach anfänglichen Zweifeln auf Seiten der Hochschule bestand auch Klarheit darüber, daß es nicht etwa einen Verhaltenskodex gibt, welcher im Bereich der empirischen Sozialwissenschaften dem Forscher gebietet, gegenüber dem Befragten ggf. den Auftraggeber der betreffenden Untersuchung zu nennen.

Im weiteren Verlauf war es dann nicht die Hochschule, sondern die Leitstelle für Fragen der Gleichstellung von Frau und Mann, die den amtlichen Hintergrund der Erhebung offengelegt und damit die vom Recht gesetzten Grenzen für die private Durchführung der Untersuchung überschritten hat: Als sich unter Landräten eine Ablehnung der Teilnahme ihrer Kreisverwaltungen an der Umfrage verbreitete, wandte sich die Leitstelle an den Sächsischen Landkreistag, gab die Staatsministerin als Auftraggeber der Untersuchung zu erkennen und bat um Unterstützung durch den Landkreistag, wozu sie erläuterte, sie habe mit diesem Schritt bisher gezögert, weil der Sächsische Datenschutzbeauftragte die Auffassung vertrete, daß die Auftragserteilung durch die Staatskanzlei nicht erkennbar werden dürfe.
Wohlgemerkt: Einwände gegen meine Rechtsauffassung hatte die Leitstelle nicht geltend gemacht.

Dem Sächsischen Landkreistag habe ich auf seine Anfrage hin mitgeteilt, daß ich seine Rechtsauffassung teilte, wonach die Untersuchung aus datenschutzrechtlichen - hier statistikrechtlichen - Gründen rechtswidrig geworden ist, als die Sächsische Staatskanzlei als Interessent, ja sogar als Auftraggeber der Studie ihm gegenüber - als einem Dritten - aufgetreten ist.

Ich habe die Rechtslage der Ministerin dann in einem persönlichen Gespräch noch einmal dargelegt und bin auf Verständnis für mein Anliegen gestoßen.

(2) Bei Kommunen fand in einzelnen Fällen, die mir durch Eingaben oder Zeitungsberichte bekannt wurden, eine ähnlich mißglückte - nämlich *halbe* - Privatisierung einer eigentlich amtlichen Statistik statt.
In einem Fall konnte für die durch Schüler für ein von der Kommune beauftragtes Planungsbüro durchgeführte Sammlung von Daten über die Wohnsituation noch eine Satzung nachgeschoben werden, nachdem die Spitze der Stadtverwaltung in der Tagespresse die Datenerhebung als im städtischen Auftrag stattfindend ausführlich erläutert und in ihrer Bedeutung für das planerische Handeln der Stadt dargestellt hatte.

(3) Nachdem es aber auch gelungene Beispiele für solche Privatisierungen kommunaler Einzel-Statistiken gibt und nachdem die Staatsregierung in ihrer Stellungnahme zu meinem 4. Tätigkeitsbericht zu erkennen gegeben hat, daß sie an die Privatisierung kommunaler Statistiken nicht weniger strenge Anforderungen gestellt wissen will als ich, gehe ich davon aus, daß die Erfüllung dieser Anforderungen im kommunalen Bereich allmählich gesicherte Praxis werden wird.

5.7.6 Auslegung des Anonymisierungserfordernisses in § 9 Abs. 6 SächsStatG

Die Stadt Chemnitz legte mir den Entwurf einer kommunalen Statistiksatzung gemäß § 9 Abs. 6 Satz 3 SächsStatG über die regelmäßige Weitergabe personenbezogener Daten aus den Fachämtern der Stadt an die kommunale Statistikstelle zur Prüfung vor. Der Entwurf enthielt Vorschriften über die Übermittlung von Daten aus dem Gewerbeamt, der Meldebehörde sowie der Baugenehmigungsbehörde an die kommunale Statistikstelle. So sollten z. B. für die Durchführung einer Statistik über den Bevölkerungsbestand monatlich Angaben zur Anschrift (Straßenschlüssel und Hausnummer), zum Status der Anschrift (Hauptwohnung/Nebenwohnung), zum Tag der Geburt, zum Geschlecht, zum Familienstand, zur Staatsangehörigkeit, zur Zugehörigkeit zu einer öffentlich-rechtlichen Religionsgesellschaft sowie zur Erwerbstätigkeit eines jeden Einwohners an die kommunale Statistikstelle übermittelt werden.

Es drängt sich zunächst auf, darin einen Verstoß gegen die Vorschrift des § 9 Abs. 6 Satz 1 SächsStatG zu sehen, der zufolge Daten aus anderen Verwaltungsstellen der Gemeinde nur *anonymisiert* an die kommunale Statistikstelle übermittelt werden dürfen. Gemäß § 3 Abs. 2 Nr. 4 SächsDSG ist „anonymisieren“ das Verändern personenbezogener Daten in der Weise, daß sie nicht mehr einer bestimmten oder bestimmbaren Person zugeordnet werden können. Diesen Anforderungen genügte der mir vorgelegte Entwurf nicht: Denn die Kombination von Erhebungsmerkmalen, z. B. der Anschrift mit dem Tag der Geburt und dem Geschlecht, ermöglicht oft auch ohne die Nennung von Namen einen Rückschluß auf eine bestimmte Person. Wäre mit der in § 9 Abs. 6 Satz 1 SächsStatG geforderten „anonymisierten Weitergabe“ eine solche

Anonymisierung i. S. v. § 3 Abs. 2 Nr. 4 SächsDSG gemeint, so müßten die zu übermittelnden Daten bereits in den anderen Verwaltungsstellen der Gemeinde unter Ausschluß von Feldgrößen kleiner als 3 aggregiert (d. h. in Tabellen zusammengefaßt) und erst danach an die kommunale Statistikstelle übermittelt werden.

Eine solche Auslegung gäbe der Vorschrift jedoch einen unsinnigen Inhalt. Es ist nicht nötig, besonders zu erlauben, durch Aggregierung anonymisierte Daten, d. h. statistische Tabellen mit genügend großen Tabellenfeldwerten, an die besonders abgeschottete kommunale Statistikstelle zu übermitteln. Denn solche nicht mehr personenbezogenen Daten dürften auch an jede andere Stelle der Gemeinde, ja auch an jedermann ohne weiteres übermittelt werden. Außerdem wären weitere in § 9 Abs. 6 SächsStatG enthaltene Forderungen, etwa nach der Beachtung gesetzlicher Weitergabeverbote bei der Übermittlung von Daten an die kommunale Statistikstelle, überflüssig.

Höchst sinnvoll wird die Vorschrift hingegen, wenn man das Wort "anonymisiert" in einem weiteren, weniger anspruchsvollen Sinne versteht, der sich ergibt, wenn man den verfassungsrechtlichen Grundsatz der Verhältnismäßigkeit auf den besonderen Regelungsgegenstand anwendet, womit man zugleich dem statistikrechtlichen Grundgebot der frühestmöglichen - statistikzweckunschädlichen - Anonymisierung (§ 1 Abs. 2, a. E., SächsStatG) konkrete Geltung verschafft.
Man gelangt dann zu folgender Auslegung des Tatbestandsmerkmals „anonymisiert“ in § 9 Abs. 6 SächsStatG, der sich auch das SMI angeschlossen hat:

Sowohl die Entstehungsgeschichte als auch der Zweck der Vorschrift sowie ein Wertungsvergleich mit § 8 Abs. 1 SächsStatG gebieten es im Hinblick auf die verfassungsrechtliche Garantie der kommunalen Selbstverwaltung, den Ausdruck „anonymisiert“ in § 9 Abs. 6 Satz 1 SächsStatG *weiter* auszulegen als den Ausdruck „anonymisieren“ in § 3 Abs. 2 Nr. 4 SächsDSG. Für die Anonymisierung i. S. v. § 9 Abs. 6 Satz 1 SächsStatG genügt es, wenn der Datensatz keine Angaben zum Namen des Betroffenen enthält; es genügt, anders ausgedrückt, eine *oberflächliche, schwache* Anonymisierung. Es ist somit nicht erforderlich, daß ein vollständiger Grad an Anonymisierung bereits von der Fachbehörde herbeigeführt wird, die gemäß § 9 Abs. 6 SächsStatG in ihrem Verwaltungsvollzug angefallene Daten der kommunalen Statistikstelle für ausschließlich statistische Zwecke übermittelt. (Diese Anonymisierung ist auch schwächer als die nach § 3 Abs. 7 BDSG, der bekanntlich eine weniger strenge Begriffsbestimmung normiert als § 3 Abs. 2 Nr. 4 SächsDSG.)

Führt man diese am Grundsatz der Verhältnismäßigkeit ausgerichtete Überlegung fort, so stellt sich sofort die andere Frage, welcher Anonymisierungsgrad dann für die langfristige Speicherung der Daten durch die kommunale Statistikstelle geboten ist. Nach dem mir vorgelegten Satzungsentwurf sollten als individualisierende Angaben u. a., wie oben aufgeführt, Straßenschlüssel und Hausnummer übermittelt werden. Da in diesen Fällen der Name des Betroffenen nicht übermittelt werden sollte, hielt sich der Entwurf insoweit in den Grenzen des gemäß § 9 Abs. 6 Satz 1 SächsStatG Gebotenen.

Nach einer Kontrolle der Plausibilität der übermittelten Daten wirkt sich jedoch das Gebot der frühestmöglichen Anonymisierung gemäß § 1 Abs. 2 SächsStatG aus: Als Hilfsmerkmale werden die betreffenden individualisierenden Angaben, also etwa Straßenschlüssel und Hausnummer, nicht mehr benötigt; aggregationsfähig sind diese Daten nur insoweit, als sie eine Zuordnung des Einzelangaben-Datensatzes zu einem bestimmten räumlichen Aggregationsbereich (Stadtplanungsbezirk, Blockseite) ermöglichen. Individualisierende Daten sind demzufolge unverzüglich zu ersetzen durch eine Kennung, welche den Einzelangaben-Datensatz einem bestimmten räumlichen Aggregationsbereich zuordnet. Gründe, die eine *adressenscharfe* Speicherung von Einzelangaben-Datensätzen in der kommunalen Statistikstelle notwendig machen, hat man mir bisher nicht dargelegt.

5.7.7 Organisationsuntersuchungen als amtliche Statistik?

Im Berichtszeitraum war ich mehrere Male mit der Frage befaßt, ob sog. Organisationsuntersuchungen in öffentlichen Stellen im Rechtssinne Statistik sind oder nicht. Mit solchen Untersuchungen will man, wie schon länger für Unternehmen und Betriebe üblich, auch in Verwaltungen Rationalisierungsreserven aufdecken und überhaupt die Zweckmäßigkeit der Arbeitsabläufe überprüfen.
In den Geschäftsbereichen des SMI, des SMWK und des SMS sollten sog. harte Organisationsfaktoren untersucht werden, also das, was man messen oder nachlesen kann, wie Zuständigkeitsabgrenzungen von Organisationseinheiten und überhaupt schriftliche Dienstanweisungen, Erledigungszahlen und -zeiten und dergleichen. Dazu müssen zum Teil auch Betroffenendaten aus den Vorgängen, mit deren Erledigung die betreffende öffentliche Stelle beschäftigt ist, sowie bei der Dienststelle vorhandene Beschäftigtendaten durch beauftragte Unternehmensberater genutzt werden.
In einem anderen Fall wollte man Teilnehmer eines Fortbildungskurses die Organisation des Landesjugendamtes, was die sog. weichen Organisationsfaktoren - also den Führungsstil, informelle Verhaltensregeln usw. - betrifft, durch Interviews mit Beschäftigten der Behörde untersuchen lassen. In solchen Fällen werden ausschließlich Beschäftigtendaten verarbeitet.

Die in solchen Untersuchungen gewonnenen Erkenntnisse über einzelne Verwaltungsvorgänge oder über einzelne Bedienstete könnten als Erkenntnisse über 'Massenerscheinungen' aufzufassen sein. Im Hinblick auf § 1 Abs. 1 Satz 1 SächsStatG stellt sich daher datenschutzrechtlich die Frage, ob für Organisationsuntersuchungen Vorgaben des Statistikrechtes zu beachten sind.

Die Untersuchungen harter Organisationsfaktoren - mögen sie sich auch Methoden bedienen, die im sozialwissenschaftlichen Sinne statistische Methoden sind - sind keine (amtliche) Statistik im Rechtssinne, zumindest nicht in datenschutzrechtlicher Hinsicht. Dies ergibt sich aus der Entgegensetzung der Begriffe "Organisationsuntersuchung" und "statistischen Zwecken" in § 12 Abs. 3 Satz 1 SächsDSG: Die Vorschrift unterscheidet zwischen den beiden - privilegierten - Zweckänderungen bzw. Annex-Zwecken in der Weise, daß Organisations-

untersuchungen nicht ein Unterfall der Verfolgung statistischer Zwecke sind.
Dieselbe Entgegensetzung weist auch das Bundesrecht auf: § 8 BStatG enthält zumindest implizit die allgemeine Ermächtigung für Verwaltungsstellen des Bundes, *Statistiken im Verwaltungsvollzug* durchzuführen, also die Erlaubnis, Daten des Verwaltungsvollzuges im Wege der privilegierten Zweckänderung der statistischen 'Selbstversorgung' zuzuführen. Dadurch, daß § 14 Abs. 3 Satz 1 BDSG - wie § 12 Abs. 3 Satz 1 SächsDSG - die Verwendung von Daten Betroffener aus dem Verwaltungsvollzug für *Organisationsuntersuchungen* eigens als privilegierten Zweckänderungstatbestand nennt, werden die Organisationsuntersuchungen der Statistik im Verwaltungsvollzug entgegengesetzt, die ja schon durch das Bundesstatistikgesetz (in dessen Neufassung, die im Zeitpunkt des Erlasses des BDSG 1990 bereits galt) geregelt war.

Für die Untersuchung der "weichen" Organisationsfaktoren ist die Heranziehung von Betroffenendaten aus dem Verwaltungsvollzug nicht erforderlich. Es werden aber Beschäftigtendaten erhoben. Soweit - wie üblich - die Untersuchung ausschließlich einzelne Stellen bzw. deren organisatorische Verhältnisse zum Gegenstand haben, handelt es sich nicht um die Erhebung und Weiterverarbeitung von Daten über Massenerscheinungen, sondern über ein einzelnes organisatorisches Gebilde und dessen einzelne Teile. Statistik im Rechtssinne könnte allenfalls eine Umfrage z. B. zum Führungsstil in vielen verschiedenen öffentlichen Stellen sein, wenn die Ergebnisse der Umfrage nur aggregiert ausgewertet würden.

Allerdings sind jeweils die Vorschriften über die Erhebung und Weiterverarbeitung von Beschäftigtendaten - etwa § 31 SächsDSG - zu beachten! Dazu näher oben unter 5.1.23.

5.7.8 Wahrung des Statistikgeheimnisses

Immer noch ist das Statistikgeheimnis keine Selbstverständlichkeit. Das zeigte sich, als ein Lebensmittelüberwachungs- und Veterinäramt mir gegenüber sein Unverständnis dafür ausdrückte, daß es nicht auf Einzelangaben aus der amtlichen Agrarstatistik zugreifen dürfe, um bisher unbekannte Tierhalter, insbesondere kleinere tierhaltende Betriebe in seinem örtlichen Zuständigkeitsbereich ausfindig zu machen. Zur Erfüllung seiner Aufgaben sei es auf die Kenntnis der Daten über Tierhalter aus der amtlichen Statistik angewiesen; die amtliche Statistik sei auch, soweit ersichtlich, der einzige Bereich, der über die entsprechenden Daten verfüge.

Ich habe dem Lebensmittelüberwachungs- und Veterinäramt, soweit es um den Zugriff auf Einzelangaben aus der Agrarstatistik ging, folgendes mitgeteilt:

Einer Übermittlung von Einzelangaben über persönliche und sachliche Verhältnisse, die für statistische Zwecke gemacht worden sind, steht das Statistikgeheimnis, § 16 BStatG, § 18 SächsStatG, entgegen. Diese Geheimhaltung, d. h. die Nicht-Übermittlung von Einzelangaben aus dem Bereich der amtlichen Statistik in den Bereich des Verwaltungsvollzugs, bildet seit jeher das Fundament der amtlichen Statistik. Bereits in Schriften über die Volkszählung in Bayern im Jahre 1834 steht ein Passus, daß die erhobenen Daten "nur für statistische Zwecke" benutzt und nicht an Polizeibehörden weitergegeben werden dürfen (zitiert nach Dorer/Mainusch/Tubies, Bundesstatistikgesetz mit Erläuterungen, München 1988). Aus Sicht des Staates dient die statistische Geheimhaltung u. a. der Erhaltung des Vertrauensverhältnisses zwischen den Befragten und den statistischen Behörden sowie der Gewährleistung der Zuverlässigkeit der gemachten Angaben sowie der Berichtswilligkeit der Befragten. Aus Sicht der Betroffenen ist der Schutz ihrer Privatsphäre, also der Schutz ihrer informationellen Selbstbestimmung vor neugierigen Fragen des Staates, ein Grundrecht, in das nur auf einer klaren gesetzlichen Grundlage eingegriffen werden darf.

Gegenstand des Statistikgeheimnisses sind zunächst die "Erhebungsmerkmale", d. h. diejenigen Angaben über persönliche und sachliche Verhältnisse, die zur statistischen Verwendung bestimmt sind (§ 10 Abs. 1 Satz 2 BStatG, § 12 Abs. 2 Satz 1 SächsStatG). So ist beispielsweise die Zahl der in einem landwirtschaftlichen Betrieb gehaltenen Rinder ein Erhebungsmerkmal gemäß § 20 AgrStatG und unterliegt deshalb der statistischen Geheimhaltung. Darüber hinaus erstreckt sich das Statistikgeheimnis aber jedenfalls dann auch auf die sog. Hilfsmerkmale (§ 10 Abs. 1 Satz 3 BStatG, § 12 Abs. 3 Satz 2 SächsStatG), d. h. die zur technischen Durchführung von Statistiken dienenden Angaben (etwa Name und Anschrift eines Tierhalters), wenn mit deren Offenbarung zugleich ein eigenes Erhebungsmerkmal, hier die Eigenschaft des Befragten, Tierhalter zu sein, übermittelt würde. Deshalb unterliegen Informationssammlungen wie z. B. das im Bereich der Agrarstatistik gemäß § 97 AgrStatG geführte Betriebsregister, die sowohl Hilfs- als auch Erhebungsmerkmale enthalten, ebenfalls der statistischen Geheimhaltung.

Nur ganz ausnahmsweise und nur, sofern dies gesetzlich besonders bestimmt ist, dürfen Einzelangaben aus der amtlichen Statistik an andere Einrichtungen übermittelt werden. So sieht z. B. § 16 Abs. 5 BStatG unter bestimmten Voraussetzungen die Übermittlung von Einzelangaben vom Statistischen Bundesamt und den statistischen Ämtern der Länder an die zur Durchführung statistischer Aufgaben zuständigen Stellen der Gemeinden und Gemeindeverbände vor. Ferner sieht § 16 Abs. 6 BStatG unter bestimmten Voraussetzungen die Übermittlung von Einzelangaben vom Statistischen Bundesamt und den statistischen Ämtern der Länder an Hochschulen oder sonstige Einrichtungen mit der Aufgabe unabhängiger wissenschaftlicher Forschung für die Durchführung wissenschaftlicher Vorhaben vor. Entsprechende Vorschriften über die Übermittlung von Einzelangaben aus dem Bereich des Statistischen Landesamtes finden sich in § 19 Abs. 3 und 5 SächsStatG.

Im Bereich der Agrarstatistik ist die Übermittlung von Einzelangaben, soweit ersichtlich, lediglich in zwei Fällen gesetzlich erlaubt: Zum einen dürfen gemäß § 98 AgrStatG im Rahmen von § 16 Abs. 4 BStatG Einzelangaben für die Verwendung gegenüber den gesetzgebenden Körperschaften und für Zwecke der Planung, jedoch nicht für die Regelung von Einzelfällen, offenbart werden. Zum anderen besteht mit § 16 Abs. 4 SächsAGTierSG eine "besondere Rechtsvorschrift" im Sinne des § 16 Abs. 1 Satz 1 BStatG, welche die Übermittlung von Tierhalterdaten an die Sächsische Tierseuchenkasse erlaubt. Weitere Übermittlungsbefugnisse sind in diesem Bereich nicht ersichtlich. Daher können Einzelangaben aus der Agrarstatistik, insbesondere aus dem Betriebsregister gemäß § 97 AgrStatG, nicht an ein LÜVA übermittelt werden.

Wenn ein unabweisbarer Bedarf besteht, ist der Gesetzgeber aufgerufen (aber nicht die Exekutive), die Datenübermittlung normenklar zu regeln.

5.7.9 Kommunale Fremdenverkehrsstatistiken

Erfreulich frühzeitig hat das SMWA mich an der Erarbeitung einer Mustersatzung über die Erhebung einer Kurtaxe durch Fremdenverkehrsgemeinden (Kurtaxe-Satzung) beteiligt. Der Musterentwurf enthielt u. a. Vorschriften über die Durchführung einer Fremdenverkehrsstatistik durch die jeweilige Gemeinde. Nach einem ersten Entwurf sollten neben den zur Ermittlung der Kurtaxepflicht unter Klarnamen erforderlichen Angaben auf einem separaten Erhebungsblatt auch „kurtaxerechtlich nicht erhebliche“ Angaben zur Motivation bei der Auswahl des Reiseziels, zur Informationsquelle, zur Aufenthaltsdauer, zum Verkehrsmittel und zum Alter des Gastes und der mitreisenden Personen auf freiwilliger Grundlage erhoben werden dürfen. In einem späteren Entwurf war vorgesehen, daß die Fremdenverkehrsgemeinden "weitere Angaben für Marketing- und Werbezwecke" sollten erheben dürfen. Auch einzelne Fremdenverkehrsgemeinden haben sich wegen solcher Datenerhebungen an mich gewandt.

Werden Daten über Gäste einer Fremdenverkehrsgemeinde für Zwecke der Planung,

des Marketings oder der Werbung erhoben und zusammengeführt (aggregiert), so handelt es sich um Statistik. Wird diese von einer öffentlichen Stelle, hier der Gemeinde, durchgeführt, so handelt es sich um *amtliche* Statistik, nämlich um eine Kommunalstatistik gemäß § 8 SächsStatG. Diese ist nur zulässig, wenn die Massendaten, die erhoben werden sollen, für die Wahrnehmung einer Aufgabe der betreffenden öffentlichen Stelle benötigt werden. Eine Gemeinde darf im Wege der amtlichen kommunalen Statistik nur nach solchen Umständen fragen, deren Vorliegen erheblich für die (über Einzelfallregelungen hinausgehende) Erfüllung der ihr nach der Rechtsordnung zustehenden Aufgaben ist. Ferner muß die Kommunalstatistik durch (Statistik-)Satzung, die die Anforderungen von § 6 Abs. 2 bis 4 und 6 SächsStatG erfüllen muß, angeordnet worden sein und gemäß § 9 SächsStatG ausschließlich von der für die Durchführung statistischer Aufgaben zuständigen Stelle der Gemeinde (kommunale Statistikstelle) durchgeführt werden. Schließlich müssen die übrigen in §§ 8, 9 SächsStatG genannten Voraussetzungen erfüllt sein.
Ich habe dem SMWA deshalb empfohlen, den Fremdenverkehrsgemeinden nahezulegen, die Statistiken nicht selbst, sondern durch die jeweiligen örtlichen oder regionalen Fremdenverkehrsvereine als Private durchführen zu lassen. Auf die strengen Anforderungen des Sächsischen Statistikgesetzes käme es dann nicht mehr an, sofern die Voraussetzungen einer rein privaten Statistik eingehalten werden (vgl. 4. Tätigkeitsbericht unter 5.7.3, Fallgruppe 1). Dann werden beide Erhebungen getrennt voneinander durchgeführt: Ein Durchschreibesatzverfahren, bei dem der Gast auf ein und dem selben Blatt neben den Pflicht-Angaben für die Kurtaxenerhebung freiwillige Angaben zum Zwecke der Durchführung einer Fremdenverkehrsstatistik machen sollte, scheidet aus. Der Beherbergungsunternehmer gibt dem Gast neben dem amtlichen Vordruck für die Kurtaxenerhebung, den auszufüllen der Gast rechtlich verpflichtet ist, kurzerhand einen zweiten, separaten Erhebungsbogen des Fremdenverkehrsvereins aus. Den füllt der Gast freiwillig und anonym aus. Er weiß, daß dieser Fragebogen der Gemeinde nicht mit seinem Namen zur Kenntnis gelangt, sondern vom Beherbergungsunternehmer unmittelbar an den Fremdenverkehrsverein geschickt wird. Die Antworten und Anregungen werden offener und ehrlicher sein; für die Fremdenverkehrsvereine sind sie eine wertvolle Arbeitshilfe.

Zu berücksichtigen ist auch, daß in Zukunft die Erhebung von Daten im Bereich des Tourismus mit Vorrang durch oder gemäß der Richtlinie 95/57/EG DES RATES vom 23. November 1995 über die Erhebung statistischer Daten im Bereich des Tourismus (ABl. EG Nr. L 291 S. 32) geregelt sein wird: Der deutsche Gesetzgeber hat bis zum Ende des Jahres 2000, in einigen Fällen auch schon bis zum Ende des Jahres 1998, ein statistisches Informationssystem im Bereich des Tourismus aufzubauen, welches fast alle der in der Mustersatzung vorgesehenen Erhebungsmerkmale enthält. Ich hoffe, daß die Regulierungs- und Datensammelwut der (EU-) Bürokraten sich in Grenzen halten läßt.

Über die Einzelheiten eines überarbeiteten Musterentwurfs bin ich derzeit mit dem SMWA noch im Gespräch.

5.7.10 Verhältnis von § 9 Abs. 6 SächsStatG zu § 14 GewO

Nach § 14 Abs. 6 und 7 GewO ist die Übermittlung von Daten Gewerbetreibender vom Gewerbeamt an andere öffentliche Stellen nur zulässig, soweit diese Daten zur Aufgabenerfüllung des Empfängers erforderlich sind und beim Betroffenen nur mit unverhältnismäßig hohem Aufwand erhoben werden könnten. Eine Stadt bat mich zu prüfen, in welchem Verhältnis diese Vorschrift zu § 9 Abs. 6 SächsStatG steht. Dieser regelt, daß Daten, die im Geschäftsgang von Verwaltungsstellen der Gemeinden, also auch des Gewerbeamtes, angefallen sind, ohne die sich aus § 14 Abs. 6 und 7 GewO ergebenden Übermittlungsbeschränkungen, also unter weniger strengen Voraussetzungen, übermittelt werden dürfen.

Ich habe der Stadt dargelegt, daß zwischen beiden Vorschriften kein Widerspruch besteht und insbesondere § 14 Abs. 6 und 7 GewO für die Übermittlung von Gewerbedaten an die kommunale Statistikstelle keine Einschränkung gegenüber der in § 9 Abs. 6 SächsStatG gegebenen Erlaubnis bewirkt: Die Übermittlungsbefugnisse gemäß § 14 Abs. 6 und 7 GewO gelten ausschließlich für den Bereich der Nutzung der Daten zu Zwecken des Verwaltungsvollzugs, also zu nicht-statistischen Zwecken. Sollen dagegen personenbezogene Daten innerhalb der Gemeindeverwaltung zu statistischen Zwecken übermittelt werden, so richtet sich die Zulässigkeit der Übermittlung allein nach § 9 Abs. 6 SächsStatG. Beide Bereiche sind voneinander zu unterscheiden. Das Gewerbeamt darf Daten von Gewerbetreibenden zu statistischen Zwecken sowohl selbst unter den Voraussetzungen von § 7 Abs. 1 SächsStatG zur Durchführung einer Statistik im Verwaltungsvollzug nutzen als auch - im Wege der innerkommunalen Funktionsübertragung - gemäß § 9 Abs. 6 SächsStatG an die kommunale Statistikstelle übermitteln. Nach einer Übermittlung an die kommunale Statistikstelle greift, was die Speicherung betrifft, jedoch dann das Gebot der frühestmöglichen Anonymisierung gemäß § 1 Abs. 2 SächsStatG ein, d. h. es müssen die individualisierenden Angaben alsbald in Tabellenform zusammengeführt werden.

5.7.11 Abgrenzung der Statistik gegenüber § 136 BauGB

In der kommunalen Statistikstelle einer sächsischen Großstadt zeigte man mir eine Datei, die sich aus Teilen des Meldedatensatzes zusammensetzte: Zwar unter Ausschluß des Namens der gemeldeten Person, aber unter Einschluß der genauen Anschrift. (Daß diese nicht mit der namentlichen Bezeichnung, sondern unter Verwendung eines verwaltungsinternen Straßen-Schlüssels gespeichert war, war datenschutzrechtlich unerheblich.)

Diese adressenscharfe Speicherung von *Einzelangaben* (in der Terminologie des Statistikrechts, vgl. § 18 f. SächsStatG, § 16 BStatG) begründete man mir gegenüber damit, daß man die Daten adressenscharf vorhalten müsse für städtebauliche Sanierungsmaßnahmen nach § 136 BauGB.

Diese Begründung stellte sich als falsch heraus: Die bei städtebaulichen Sanierungsmaßnahmen gemäß § 141 BauGB durchzuführenden *vorbereitenden Untersuchungen* sind kein Teil der amtlichen Statistik; ihre Durchführung stellt keinen statistischen Zweck dar, sie ist Datenerhebung eigener Art. In einer Statistik werden Daten auf Vorrat zur Auswertung zu schon bekannten oder sich noch ergebenden, aber grundsätzlich absehbaren Planungszwecken gespeichert. Demgegenüber hat sich die für das Verfahren gemäß § 141 BauGB zuständige Behörde im parzellenscharfen Umfang des Untersuchungsgebietes von der Meldebehörde, der Bauordnungsbehörde oder auch der Gewerbebehörde die dazu benötigten - personenbezogenen - Daten übermitteln zu lassen. Sie kann ferner unmittelbar bei den Betroffenen Daten auf der Grundlage der gemäß § 138 BauGB bestehenden Auskunftspflicht erheben.
Demgegenüber hat die kommunale Statistikstelle mit dem Verfahren nach §§ 136 ff. BauGB nur insofern zu tun, als sie bei ihr ohnehin vorhandene statistische Zahlen beitragen darf.

Die vorbereitende Untersuchung möglicher städtebaulicher Sanierungsgebiete gemäß § 141 BauGB scheidet also als ein Zweck, der die dauernde adressenscharfe Speicherung von Meldedaten im Rahmen der Statistik erforderlich macht, aus. Auch ein anderer Zweck, der diese rechtfertigende Wirkung haben könnte, besteht nicht. Daraus folgt: Die genannten oder ähnliche individualisierende Daten dürfen in der kommunalen Statistikstelle nicht adressenscharf gespeichert werden. Nach einer ggf. stattfindenden und in diesem Falle dann schnell zu absolvierenden Kontrolle der Plausibilität der (in diesem Fall gemäß § 9 Abs. 6 SächsStatG aus anderen Teilen der Stadtverwaltung übermittelten) Daten kommt *das Gebot der frühestmöglichen Anonymisierung* gemäß § 1 Abs. 2 a. E. SächsStatG zum Tragen: Als Hilfsmerkmal werden die betreffenden individualisierenden Daten nicht mehr benötigt; aggregationsfähig sind diese Daten nur insoweit, als sie eine Zuordnung des Einzelangaben-Datensatzes zu einem bestimmten räumlichen Aggregationsbereich (Stadtplanungsbezirke, Blockseiten) ermöglichen. Die genannten individualisierenden Daten sind in dem betreffenden Einzelabgaben-Datensatz demzufolge unverzüglich durch eine Kennung zu ersetzen, welche den Einzelangaben-Datensatz einem bestimmten räumlichen Aggregationsbereich

zuordnet.

Ich konnte in dieser Frage vollständige Übereinstimmung mit der Rechtsauffassung des SMI feststellen.

5.7.12 Statistik im Verwaltungsvollzug für das Ministerium - am Beispiel der Meldung von Aufhebungsverträgen durch Oberschulämter an das SMK

In dem oben unter 5.1.15 behandelten Vorgang hat das SMK im Hinblick auf § 31 Abs. 1 SächsDSG auf die Übermittlung der Namen der Lehrkräfte sowie der Bezeichnung der betreffenden Schule verzichtet. Die Oberschulämter sollen künftig also nur noch Angaben zum Schulamt, Geschlecht, Alter, zur Fächerkombination, Anzahl der abgeleisteten Dienstjahre, Höhe der Abfindung sowie zum Zeitpunkt des Ausscheidens an das SMK übermitteln. Diese Daten würden zu statistischen Zwecken benötigt.

Damit ist der Vorgang datenschutzrechtlich jedoch noch nicht zuende gedacht. Zunächst ist schon das Nutzen der Daten aus den einzelnen Verwaltungsvorgängen - hier der Dienstverhältnisse und ihrer Beendigung durch Aufhebungsvertrag - ein Datenverarbeitungsvorgang, der einer Rechtsgrundlage bedarf, zumal er mit einer *Zweckänderung* verbunden ist: Die Daten werden ja nicht zum ursprünglichen Zweck, nämlich der Durchführung konkreter Maßnahmen der Personalverwaltung, genutzt, sondern eben zu statistischen Zwecken, nämlich um dem Ministerium einen Überblick über die Gesamt-Verhältnisse in Sachen Aufhebungsverträge zu geben.

Rechtsgrundlage ist die allgemeine Erlaubnis für Statistiken im Verwaltungsvollzug gemäß § 7 Abs. 1 SächsStatG. Danach bedarf die Durchführung einer Statistik keiner Anordnung durch besondere Rechtsvorschrift, wenn sie ausschließlich der Erfüllung der Aufgaben der öffentlichen Stelle, in deren Geschäftsgang die Daten anfallen, oder der jeweils übergeordneten öffentlichen Stelle dient.
Handelt es sich um diesen Zweck, also um Statistik, tut der Name des Lehrers überhaupt nichts zur Sache, ist er also aus dem Datensatz alsbald zu löschen. Daß die Bezeichnung der betreffenden Schule ebenfalls aus dem Datensatz gelöscht worden ist, zeigt, daß das Ministerium einen weniger kleinteiligen Überblick benötigt, daß also die einzelnen Grundschulen nicht Aggregationseinheiten sein sollen.
Aber auch nach Weglassen der Identifikatoren "Name" und "Schule" handelt es sich noch um auf einzelne Personen bezogene Datensätze (vgl. § 3 Abs. 1 SächsDSG). Daß diese in dieser schwach anonymisierten Form noch nicht an das Ministerium weitergegeben werden dürfen, folgt ebenfalls aus dem Statistikrecht: Auch Statistiken im Verwaltungsvollzug sind gemäß § 2 Abs. 1 Nr. 5 SächsStatG Teil der amtlichen Statistik im Freistaat Sachsen. Auch für sie gelten daher uneingeschränkt die Grundsätze des § 1 Abs. 2, 2. Halbs. SächsStatG, insbesondere auch der Grundsatz der frühestmöglichen Anonymisierung. Danach sind Einzelangaben identifizierenden Charakters zu anonymisieren, sobald dies ohne Gefährdung des Zwecks der Statistik möglich ist. Mittel der Anonymisierung ist regelmäßig die Aggregierung, d. h. die

Zusammenführung von Einzelangaben zu Tabellen.

Eine Anonymisierung läßt sich durch Aggregierung der zu übermittelnden Daten bereits in den Oberschulämtern ohne Gefährdung des Zwecks der Statistik erreichen. Insbesondere kann bereits in den Oberschulämtern geprüft werden, ob die Daten schlüssig und vollständig sind. Die Aggregierung der Daten erst beim SMK vorzunehmen verstieße gegen das Gebot der frühestmöglichen Anonymisierung.

Demnach erhält das SMK von den drei Oberschulämtern jeweils eine oder mehrere Tabellen, je nach den Fragestellungen, die es hat. Dabei sind Gruppen von Merkmalsausprägungen, wie etwa Altersklassen ("Alter zwischen 40 und 45") oder Größenordnungen von Abfindungen ("Abfindungen zwischen 20 und 25 TDM") je nach Zweckmäßigkeit zu bilden.

Das Ministerium dürfte seinerseits Tabellenfeldwerte, die kleiner als 3 sind, an andere Stellen oder Personen nur nach Maßgabe von § 19 SächsStatG übermitteln.

5.7.13 Beteiligung der kommunalen Statistikstelle an der Durchführung der Bautätigkeitsstatistik

Über die Bautätigkeit im Hochbaubereich wird eine Statistik auf der Grundlage des 2.BauStatG durchgeführt. Erhoben werden u. a. Angaben zum Bauherrn, zur Lage des Baugrundstücks, zur Art der Baumaßnahme, zur Zahl der Wohneinheiten etc. Auskunftspflichtig sind gemeinschaftlich die Bauherren, die Bauaufsichtsbehörden und für bestimmte Angaben auch die Gemeinden, § 3 2.BauStatG. Das bei der Durchführung der Statistik einzuhaltende Verfahren ist in einer Verwaltungsvorschrift, der VwVBauStat, genau geregelt: Die Auskünfte sind vom Bauherrn auf den vom Statistischen Landesamt herausgegebenen und numerierten „Erhebungsbögen für Baugenehmigungen“ zu erteilen, anschließend mit dem Bauantrag bei der zuständigen Gemeinde einzureichen, dort zu ergänzen und an die Bauordnungsbehörde weiterzugeben. Diese hat den Erhebungsbogen selbst oder mit vom Auskunftspflichtigen eingeholten Angaben auf Vollständigkeit und Richtigkeit zu überprüfen, nötigenfalls zu ergänzen und schließlich an das Statistische Landesamt weiterzuleiten.

Abweichend davon übersendet die Bauordnungsbehörde einer größeren sächsischen Stadt, wie ich in Erfahrung gebracht habe, die Erhebungsbögen zunächst zum Zwecke einer Vor-Plausibilisierung an die kommunale Statistikstelle. Das ist eine Übermittlung der darin enthaltenen Daten, für die es an einer Rechtsgrundlage fehlt. Die Beteiligung der kommunalen Statistikstelle an der Durchführung der Bautätigkeitsstatistik, insbesondere die Überlassung der Erhebungsbögen, ist rechtswidrig.
Zumindest was dieses Ergebnis betrifft, befinde ich mich in Übereinstimmung mit dem SMI.
Im einzelnen ergibt sich dieses Ergebnis aus folgendem:

Die Bauordnungsbehörde ist im vorliegenden Falle in einer doppelten Eigenschaft tätig, nämlich als Mit-Auskunftspflichtiger sowie, nämlich insoweit sie von dem auskunftspflichtigen Bauherrn die Angaben für die Weiterleitung an das Statistische Landesamt einholt, als Erhebungsbeauftragter. Als Auskunftspflichtiger verwendet sie die bei ihr im Verwaltungsvollzug angefallenen Daten. Gleichwohl kommt § 9 Abs. 6 SächsStatG als Übermittlungserlaubnis nicht in Frage. Denn insoweit die Bauordnungsbehörde auf dem Erhebungsbogen vorhandene, vom auskunftspflichtigen Bauherrn eingetragene Daten weitergibt, übermittelt sie nicht im Sinne dieser Vorschrift in ihrem Geschäftsgang angefallene Daten. Denn damit ist, wie auch in § 7 Abs. 1 SächsStatG, der dem *Verwaltungsvollzug,* also der nicht-statistischen Tätigkeit dienende Geschäftsgang gemeint. Zudem ist durch den Rücklauf von der kommunalen Statistikstelle in die Bauordnungsbehörde (vor der Weitergabe an das Statistische Landesamt) nicht gewährleistet, daß die Daten ausschließlich statistischen Zwecken dienen. Schließlich ist es auch zweifelhaft, ob die bloße Tatsache, daß die spätere Auswertung durch das Statistische Landesamt auch der Gemeinde zugute kommt, den diesbezüglichen Anforderungen des § 9 Abs. 6 Satz 1 SächsStatG genügt.

Konkret führt die bisherige Praxis dazu, daß zusätzlich zu den Bediensteten der Baugenehmigungsbehörde Bedienstete einer ganz anderen Stelle den (personenbezogene Daten enthaltenden) Erhebungsbogen zur Kenntnis nehmen, die ohne diese ‘Aufgabenübertragung’ mit den Daten in dieser Form nichts zu tun hätten: Die kommunale Statistikstelle ist im Rahmen des Statistikwesens insoweit nicht zuständig. Trotz der besonderen Kautelen, unter denen die kommunalen Statistikstellen gemäß § 9 SächsStatG stehen, dürfen zu Zwecken der Durchführung der Baustatistik als einer Bundesstatistik erhobene Einzelangaben der kommunalen Statistikstelle nicht übermittelt werden. Dies ergibt sich aus § 16 Abs. 5 Satz 1 BStatG, der einer Anwendung des § 5 Abs. 2 2.BauStatG entgegensteht: Abgesehen davon, daß § 5 Abs. 2 2.BauStatG nie am vierjährigen Übergangsbonus des § 26 Abs. 3 BStatG teilgenommen hat, unterliegt die Vorschrift dem Vorrang des § 16 Abs. 5 BStatG als des späteren Gesetzes, und die Anforderungen, welche diese Vorschrift an die Übermittlung von Einzelangaben an kommunale Stellen stellt, erfüllt § 5 Abs. 2 2.BauStatG nicht. Denn die Einzelangaben-Übermittlung ist in dem die Bundesstatistik anordnenden Gesetz (2.BauStatG) nicht auf ausschließlich statistische Zwecke und nicht auf die zur Durchführung statistischer Aufgaben zuständigen Stellen beschränkt. Genausowenig sind Art und Umfang der zu übermittelnden Einzelangaben tatsächlich *bestimmt* (offengelassen bei Dorer/Mainusch/Tubies, Rdnr. 49 zu § 16 BStatG).

Zumindest für große Kommunen besteht ein einfacher Ausweg: Diejenigen, die bisher in der kommunalen Statistikstelle diese Arbeiten erledigten, werden in die Baugenehmigungsbehörde umgesetzt; damit die Statistik aber tatsächlich durchgeführt wird - denn nur eine halbwegs zutreffende Statistik ist eine rechtmäßige Statistik -, muß gewährleistet sein, daß die betreffende Arbeitskraft auch wirklich damit befaßt wird.

5.8 Archivwesen

Zugang zu und Veröffentlichung von personenbezogenen Daten im Zusammenhang mit der Erforschung der jüngeren Geschichte von Fakultäten sächsischer Hochschulen

Eine Fakultät der Universität Leipzig hat damit begonnen, ihre Geschichte seit 1945 - in Dissertationsschriften und zugleich zur Veröffentlichung in der Festschrift zur 600-Jahrfeier der Universität im Jahre 2009 bestimmt - zu erforschen. Wegen Fragen des Zugangs zu Sitzungsprotokollen des Fakultätsrates, zu Archivgut des Universitätsarchivs und staatlicher Archive und wegen der Veröffentlichung personenbezogener Angaben aus diesen Unterlagen sowie auch aus den Aussagen von Zeitzeugen hat sich der die Arbeiten betreuende Professor an mich gewandt.

(1) Hervorzuheben war zunächst die spezielle Regelung des Sächsischen Archivgesetzes, wonach die sogenannten *allgemeinen* Schutzfristen (30 bzw. 60 Jahre, § 10 Abs. 1 Satz 1 und 2 SächsArchG) *nicht* gelten für Unterlagen aus den Beständen der Rechtsvorgänger des Freistaates Sachsen selbst sowie der Funktionsvorgänger der Gerichte, Behörden und sonstigen öffentlichen Stellen des Freistaates und außerdem aus der Zeit vom 8. Mai 1945 bis zum 2. Oktober 1990 für das von den ehemaligen staatlichen oder wirtschaftsleitenden Organen, Kombinaten, Betrieben, Genossenschaften und Einrichtungen, aber auch Parteien, gesellschaftlichen Organisationen und juristischen Personen stammende Archivgut (§ 10 Abs. 2 Satz 2 i. V. m. § 4 Abs. 2 Satz 2 und 3 SächsArchG). Unter beide Regelungen fallen die (vom Staat eingerichteten) Universitäten der DDR und der Zeit davor.
Hinzu kommt: Soweit Amtsträger in Ausübung ihres Amtes betroffen sind, gelten ganz allgemein - aus verfassungsrechtlichen Gründen - die zusätzlichen dem *Persönlichkeitsschutz* dienenden Schutzfristen (§ 10 Abs. 1 Satz 3 und 4 SächsArchG) gerade nicht (§ 10 Abs. 2 Satz 3, 1. Halbs. SächsArchG). Diese Regelung wird durch § 10 Abs. 2 Satz 3, 2. Halbs. für Unterlagen aus der Zeit vom 8. Mai 1945 bis zur Wiedervereinigung über den eigentlich staatlichen Bereich im heutigen Sinne hinaus auf den halbstaatlichen Bereich erstreckt, also auf die erwähnten in § 4 Abs. 2 Satz 2, 2. Hälfte, und Satz 3 SächsArchG genannten Stellen, zu denen eben auch die Universitäten gehören; d. h. die Funktionsträger dieser Stellen werden wie heutige Amtsträger behandelt.

Soweit also Unterlagen aus Archiven als Quellen benutzt werden sollen, die dem Sächsischen Archivgesetz unterstehen, besteht demnach ein im wesentlichen freier Zugang zu personenbezogenen Daten. Anonymisiert werden müßten von seiten des Archives allerdings etwa die Daten von Opfern, z. B. disziplinierten Studenten, es sei denn, sie erteilten ihre Einwilligung gemäß § 10 Abs. 4 Satz 3 SächsArchG.

Jedoch kann es dem Forscher verboten sein, sein Forschungsergebnis in personenbezogener Weise mitzuteilen: Der Zugang des Forschers zu personenbezogenen Daten hat einen größeren Umfang als sein Recht, im

Forschungsergebnis personenbezogene Daten zu veröffentlichen. Denn in der Veröffentlichung liegt eine Vertiefung des Eingriffes in das Persönlichkeitsrecht. Meist ist es dem Forscher möglich, sein Forschungsergebnis so zu komprimiern, daß es auch ohne Personenbezug sinnvoll und verständlich ist.

Es bietet sich an, ergänzend zu § 10 Abs. 4 Satz 2, 2. Halbs. SächsArchG die allgemeine Regelung des § 30 SächsDSG heranzuziehen, wonach bei der Veröffentlichung von Forschungsergebnissen personenbezogene Daten nur offengelegt werden dürfen, soweit dies für die Darstellung von Ereignissen der Zeitgeschichte unerläßlich ist und überwiegende schutzwürdige Interessen des Betroffenen nicht entgegenstehen. Diese Regel ist wegen ihres Bezuges auf die "Zeitgeschichte" eine archivrechtsnahe Vorschrift, und sie ist Ausdruck des verfassungsrechtlichen Grundsatzes der Verhältnismäßigkeit.

Im Bereich der Sozialgeschichte, wo es um Massendaten und Strukturen geht, stellt diese Regel keine Einschränkung für die Forschung dar. Individualisierende Angaben hätten in der Darstellung des Forschungsergebnisses nichts zu suchen. Anders da, wo ein Geschehen dargestellt wird, das sich nicht verstehen läßt ohne die Berücksichtigung - und damit Darstellung - des Handelns einzelner Personen. Hier kann ein Veröffentlichungsverbot nur Randfiguren des Geschehenen betreffen. Denn das die Wissenschaftlichkeit allein ausmachende Gebot der bestmöglichen Wahrheitssuche verbietet es, durch Weglassungen hervorgerufene Halbwahrheiten darzustellen. Da man aus Handlungsgeflechten Personen, die eine einigermaßen wichtige Rolle gespielt haben, nicht bei der Darstellung ausblenden kann, ohne daß die ganze Darstellung ein unangemessenes und damit von vornherein unwahres Bild entstehen läßt, ist in der zeitgeschichtlichen Forschung der Anwendungsbereich der Veröffentlichungsklausel des § 30 Abs. 4 SächsDSG sehr gering, nämlich eben beschränkt auf ausgesprochene Randfiguren.
Jedoch: Nach der Wertung des Sächsischen Archivgesetzes als des gegenüber dem Sächsischen Datenschutzgesetz späteren und auch spezielleren Gesetzes soll die Erforschung des Handelns gerade auch der halbstaatlichen Stellen in der Zeit zwischen dem 8. Mai 1945 und der Wiedervereinigung nicht beschränkt werden, sondern soweit möglich noch in der 'Erlebnisgeneration' beginnen können. Wegen der Kleinräumigkeit des Forschungsgegenstandes wäre es nicht möglich, bis zum Ablauf der Schutzfristen des § 10 Abs. 1 Satz 3 und 4 SächsArchG das jüngere Zeitgeschehen der DDR zu erforschen, wenn alle wichtigen Personen nur anonym dargestellt werden dürften. Dies wäre ersichtlich nicht im Sinne des Sächsischen Archivgesetzes.

Die Kleinräumigkeit eines Forschungsgegenstandes wie der Geschichte einer Universitätsfakultät schließt es ohnehin für den größten Teil der Adressaten der Veröffentlichung aus, die das Geschehen 'tragenden' Personen anonym darzustellen. Dies galt im vorliegenden Fall um so mehr, als es sich um eine kleinere, nicht an jeder Universität vertretene Fachrichtung handelt. Im deutschen Sprachraum sind die Vertreter einzelner Teilfächer dann doch ein vergleichsweise kleiner, überschaubarer Personenkreis, für den sich letztlich nichts anonymisieren läßt.

(2) Zu klären war auch die Frage, inwieweit Zugang zu Unterlagen besteht, die bei den Dienstgeschäften der Fakultät entstanden sind und sich noch dort befinden, also noch nicht förmlich dem Universitätsarchiv angeboten und von diesem übernommen worden sind. Diese Unterlagen fallen, was die Verarbeitung der in ihnen enthaltenen personenbezogenen Daten betrifft, - noch - nicht unter das Sächsische Archivgesetz; die Nutzung dieser Daten zu Forschungszwecken wäre datenschutzrechtlich eine Zweckänderung. Hinsichtlich der amtsträger-bezogenen Daten gewährt das Sächsische Datenschutzgesetz für Forschungszwecke nur unter engeren Voraussetzungen Zugang zu personenbezogenen Daten als das Archivgesetz. Ich habe darauf, dort allerdings im Hinblick auf kommunale Archive, bereits in meinem 3. Tätigkeitsbericht auf S. 104 aufmerksam gemacht: In § 12 Abs. 2 Nr. 4 macht das SächsDSG die Nutzung personenbezogener Daten zu Forschungszwecken in jedem Fall davon abhängig, daß das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen am Unterbleiben der Kenntnisnahme von seinen Daten erheblich überwiegt. Dasselbe Erfordernis stellt das Archivgesetz, in § 10 Abs. 4 Satz 2, 1. Halbs., demgegenüber lediglich für den Fall der Verkürzung der Schutzfristen auf, die als persönlichkeitsschutzbezogene Schutzfristen (§ 10 Abs. 1 Satz 3 SächsArchG) gemäß § 10 Abs. 2 Satz 3 SächsArchG, wie vorstehend dargelegt, Amtsträgern in Ausübung ihrer Ämter von vornherein gerade nicht zukommen. Das Archivgesetz bietet also einen einfacheren Zugang gerade zu den 'Funktionsträger'-Daten!

Es liegt daher im Interesse der Erforschung der Geschichte der betreffenden Fakultät, wenn die Unterlagen, die als Quellen herangezogen werden sollen, dem zuständigen Archiv der Universität angeboten und von diesem übernommen werden. Da es sich um Daten aus der Zeit zwischen dem 8. Mai 1945 und der Wiedervereinigung Deutschlands handelt und die Universität und ihre Fakultäten unter die in § 4 Abs. 2 Satz 2 und 3 SächsArchG genannten Einrichtungen fallen, besteht, eigentlich vorrangig, die Pflicht, die Unterlagen gemäß § 5 Abs. 2 SächsArchG dem zuständigen staatlichen Archiv anzubieten. Mir ist nicht bekannt, inwieweit die staatlichen Archive bisher gegenüber den wissenschaftlichen Hochschulen diesen Anspruch, der gerade bei einem Vergleich zwischen § 14 und § 13 SächsArchG, also der Regelung für die kommunalen Archive unzweifelhaft ist, geltend gemacht haben. Diese Anbietungspflicht gegenüber den staatlichen Archiven wäre zumindest dann geltend zu machen, wenn es Widerstand gegen die alsbaldige Archivierung der betreffenden Unterlagen, also die Anbietung gegenüber dem Hochschularchiv oder die Übernahme durch das Hochschularchiv, geben sollte.

Ich habe das SMI, als die oberste Aufsichtsbehörde für das staatliche Archivwesen (§ 3 Abs. 2 Satz 1 SächsArchG), darauf hingewiesen, daß meiner Auffassung nach in solchen Fällen die staatlichen Archive aktiv werden müßten, damit der Wille des sächsischen Archivgesetzgebers verwirklicht wird.

Vgl. auch oben 1.2.

5.9 Polizei

5.9.1 Urteil des Sächsischen Verfassungsgerichtshofs zum Sächsischen Polizeigesetz

Bereits in meinem 2. Tätigkeitsbericht (5.10.1) habe ich die datenschutzrechtlichen Defizite des Sächsischen Polizeigesetzes aufgezeigt. Insbesondere in bezug auf den Einsatz der besonderen polizeilichen Mittel zur Datenerhebung hat der Sächsische Verfassungsgerichtshof in seinem Urteil zum SächsPolG vom 14. Mai 1996 meine Kritik an den Bestimmungen des SächsPolG zum Großteil bestätigt. Angerufen wurde der SächsVerfGH von 41 Abgeordneten des Sächsischen Landtages, die sich im Wege der abstrakten Normenkontrolle gegen die Vorschriften des SächsPolG über den vorbeugenden Polizeigewahrsam, die polizeilichen Datenerhebung unter dem Einsatz besonderer Mittel sowie über die Rasterfahndung wandten. Das Verfahren, in dem ich neben einer Reihe von Sachverständigen gehört wurde, wurde durch Urteil vom 14. Mai 1996 beendet. In der Entscheidung wurden einige datenschutzrechtliche Bestimmungen des SächsPolG für verfassungswidrig erklärt, andere Bestimmungen nur bei verfassungskonformer Auslegung und nach Maßgabe der vom Gericht ausgesprochenen Vorgaben für zulässig erachtet.

Wie andere Polizeigesetze enthält auch das SächsPolG Datenverarbeitungsbefugnisse zum Zweck der vorbeugenden Straftatenbekämpfung, d. h. die Polizei darf schon im Vorfeld konkreter Gefahren und nicht erst bei unmittelbar bevorstehenden Rechtsverstößen tätig werden. Hierzu hat der SächsVerfGH bemerkt, daß der Landesgesetzgeber - vor allem auf dem Gebiet der Bekämpfung der Organisierten Kriminalität - zwar grundsätzlich befugt sei, Regelungen zu erlassen, die den Einsatz besonderer Mittel zu diesem Zweck vorsehen. Allerdings dürfe der Einsatz dieser Mittel dann nur zum Schutz bedeutender Rechtsgüter, wie des Lebens, der Gesundheit und persönlichen Freiheit sowie zur Bekämpfung der organisierten Kriminalität erfolgen. Die vorbeugende Bekämpfung von Vergehen, die sich nur gegen bedeutende Sach- und Vermögenswerte richten, aber nicht gewerbs-, gewohnheits-, serien-, bandenmäßig oder sonst organisiert begangen werden, wie sie in § 36 Abs. 1 Nr. 2 Buchst. a SächsPolG vorgesehen ist, sei mit der Sächsischen Verfassung nicht vereinbar.

Ebenfalls nicht mit der Sächsischen Verfassung vereinbar sei die Datenerhebung mit besonderen Mitteln im Rahmen von Vorfeldermittlungen, wenn personenbezogene Daten aus Vertrauensverhältnissen, die durch Amts- und Berufsgeheimnisse geschützt sind, erhoben werden können, ohne daß sich dies aus einer ausdrücklichen, normenklaren und hinreichend bestimmten Regelung im SächsPolG ergebe. In dieser müsse normiert werden, zu Gunsten welcher Rechtsgüter, aus welchen Vertrauensverhältnissen sowie unter welchen Voraussetzungen und in welchen Grenzen aus solchen Vertrauensverhältnissen mit besonderen Mitteln im Vorfeld konkreter Gefahren Daten erhoben werden dürfen.

Wegen Verstoßes gegen den verfassungsrechtlichen Grundsatz der hinreichenden Bestimmtheit hat der SächsVerfGH auch die Vorschrift zur Überwachung sog. *"gefährlicher Intensivtäter"* beanstandet, also Personen, bei denen die Gesamtwürdigung der Person und der von ihr bisher begangenen Straftaten erwarten läßt, daß sie auch künftig Straftaten von erheblicher Bedeutung begehen werden (§ 39 Abs. 1 Nr. 2 Buchst. b). Wegen der Kumulation unbestimmter Rechtsbegriffe ("Gesamtwürdigung der Person" und "Straftaten von erheblicher Bedeutung") könne der Einsatz der besonderen Mittel nicht auf Erfahrungswissen und Alltagstheorien ohne objektive Fakten oder Beweisanzeichen, d.h. auf Tatsachen oder tatsächliche Anhaltspunkte, gestützt werden. In dieser Bestimmung sah der Verfassungsgerichtshof deshalb einen Verstoß "gegen die mit dem Recht auf informationelle Selbstbestimmung (Art. 33 SächsVerf) gewährleisteten Grundsätze der Normenklarheit und Normenbestimmtheit". Die Vorschrift wurde mit sofortiger Wirkung aufgehoben.

Auch die Erhebung personenbezogener Daten über Kontakt- und Begleitpersonen im Rahmen von Vorfeldermittlungen ist nach dem Urteil des Verfassungsgerichtshofs zu beschränken auf "Personen mit näheren persönlichen oder geschäftlichen Beziehungen zur Zielperson oder auf Verbindungen, die über einen längeren Zeitraum unterhalten oder unter konspirativen Umständen hergestellt oder gepflegt werden und auf Art, Gegenstand, Zweck und Ausmaß der Verbindung im Hinblick auf die angenommenen Straftaten". Das Gericht schließt damit eine Auslegung dieser Bestimmung aus, nach der zufällige Beziehungen für einen Kontakt ausreichen sollen. Des weiteren läßt es eine Auslegung nicht zu, nach der die Kontaktperson um ihrer selbst willen ausgeforscht wird und nicht mit dem Ziel, Hinweise über die angenommenen Straftaten zu gewinnen.

Schließlich wurde der vom sächsischen Gesetzgeber unternommene Versuch, die Grundrechtseingriffe bei der Anwendung der besonderen polizeilichen Mittel durch verfahrensrechtliche Maßnahmen zu kompensieren, vom SächsVerfGH als unzureichend erachtet. Das Gericht betont, daß es zwar dem Gesetzgeber kein Schutzkonzept vorgeben wolle, nennt aber beispielhaft zusätzliche verfahrensrechtliche Schutzmaßnahmen, die vom Gesetzgeber ergriffen werden könnten, um die Rechte der Betroffenen besser als bisher zu schützen. Beispielhaft erwähnt der Gerichtshof Evaluations- und Berichtspflichten, institutionelle Sicherungen wie Richter- und Ministervorbehalt oder das Erfordernis der Zustimmung anderer Behörden mit hinreichender Unabhängigkeit, wie beispielsweise des Datenschutzbeauftragten oder bestimmter Abteilungen der Staatsanwaltschaft. Als mangelhaft kritisiert der SächsVerfGH auch die Vorschriften zur Löschung und deren institutionelle Kontrolle bezüglich der durch besondere Mittel gewonnenen personenbezogenen Daten. Schließlich sieht er in dem generellen Verzicht auf Benachrichtigungspflichten den Anspruch auf Erlangung effektiven Rechtsschutzes verletzt. Das Auskunftsrecht des Betroffenen beim Einsatz heimlicher Mittel liefe nach Auffassung des Gerichts leer, wenn keine Benachrichtigungspflicht bestünde. Ein überwiegendes Allgemeininteresse könne einer Benachrichtigungspflicht nur im Einzelfall entgegenstehen.

Speziell in bezug auf den verdeckten Einsatz technischer Mittel zur Erhebung von Daten in oder aus Wohnungen nach § 40 Abs. 1 SächsPolG (sog. "Großer Lauschangriff") hat der SächsVerfGH festgestellt, daß durch diese Maßnahme nicht das allgemeine Persönlichkeitsrecht in seinem Wesensgehalt angegriffen werden dürfe, was der Fall wäre, wenn Räume von der polizeilichen Maßnahme betroffen würden, die zur absolut geschützten Privatsphäre gehörten. Weiterhin sei der Lauschangriff nur zulässig, wenn er sich gegen den für die Gefahr Verantwortlichen richte. § 40 Abs. 1 Nr. 1 SächsPolG ermächtige jedoch den Polizeivollzugsdienst ohne jede weitere Einschränkung in oder aus Wohnungen nichtverantwortlicher Dritter Daten zu erheben. Dies sei mit der Sächsischen Verfassung nicht vereinbar. Eingriffe in das Grundrecht Dritter auf Unverletztlichkeit der Wohnung müßten auf Extremfälle polizeilichen Notstands beschränkt werden (§ 7 SächsPolG). Davon abgesehen sei § 40 Abs. 1 Nr. 2 SächsPolG insoweit nicht mit der Sächsischen Verfassung vereinbar, als der Polizei erlaubt werde, bereits im Vorfeld einer Gefahr tätig zu werden. Diese Vorschrift halte sich nicht im Rahmen des Gesetzesvorbehalts des Art. 30 Abs. 3 Sächsische Verfassung, der für Eingriffe in das Grundrecht zur präventiven Gefahrenabwehr das Vorliegen einer "dringenden Gefahr" voraussetze.

Ich gehe davon aus, daß der Sächsische Gesetzgeber bei der Neufassung des SächsPolG eine umfassende Konkretisierung der beanstandeten Regelungen vornehmen wird. Dem SMI habe ich meine Unterstützung bei der Erarbeitung eines Gesetzentwurfs angeboten.

5.9.2 Entwurf eines Gesetzes über die Erprobung einer Sächsischen Sicherheitswacht (Sächsisches Sicherheitswachterprobungsgesetz - SächsSWEG)

Mit einer "Sächsischen Sicherheitswacht", in der "zuverlässige und engagierte Bürger aktiv bei der Gewährleistung der öffentlichen Sicherheit und Ordnung mitwirken und die Polizei unterstützen", will das SMI der steigenden Kriminalität und der zunehmenden Gewaltbereitschaft begegnen. Für die Erprobungsphase hat das SMI einen Referentenentwurf eines Sicherheitswachterprobungsgesetzes (SächsSWEG) erarbeitet und mir zur Stellungnahme zugeleitet.

An der ersten Fassung des Entwurfs mußte ich bemängeln, daß er nur unzureichend die Verarbeitung personenbezogener Daten durch die Bediensteten der Sächsischen Sicherheitswacht regelte. Maßnahmen der Sicherheitswacht mit Eingriffscharakter - wozu u.a. auch die Verarbeitung personenbezogener Daten zählt - sind nach dem Entwurf nur zulässig, wenn eine besondere gesetzliche Ermächtigung besteht. Diese besondere gesetzliche Ermächtigung kann nur aus dem SächsSWEG selbst abgeleitet werden. Deshalb habe ich beim Sächsischen Staatsministerium des Innern angeregt, Vorschriften zur Erhebung und Übermittlung von Daten in das SächsSWEG aufzunehmen oder insoweit auf das SächsPolG oder das SächsDSG zu verweisen. Ausdrücklich in das Gesetz aufgenommen werden sollte auch, daß die Bediensteten

der Sicherheitswacht nur kurzfristige Datenspeicherungen vornehmen dürfen. Für weitergehende Datenspeicherungen durch die Bediensteten der Sächsischen Sicherheitswacht sehe ich keine Veranlassung, zumal die Bediensteten der Sächsischen Sicherheitswacht Daten nicht für eigene, sondern für Zwecke der Polizeidienststelle erheben, bei der sie eingesetzt sind. In das Gesetz sollte deshalb die Regelung aufgenommen werden, daß die von den Angehörigen der Sächsischen Sicherheitswacht erhobenen Daten unverzüglich an ihre Polizeidienststelle weiterzuleiten sind. Nur bei einer solchen Verfahrensweise wäre es entbehrlich, daß die Sicherheitswacht ein Dateien- oder Geräteverzeichnis nach § 10 SächsDSG führt und Datensicherungsmaßnahmen nach § 9 SächsDSG trifft.

Schließlich habe ich beim Sächsischen Staatsministerium des Innern angeregt, in einer Verwaltungsvorschrift festzulegen, daß die durchgeführten Eingriffsmaßnahmen der Sicherheitswacht - zu Zwecken der internen und externen Kontrolle - schriftlich dokumentiert und diese Schriftstücke unverzüglich an die Polizeidienststelle weitergeleitet werden, ohne daß Kopien bei den Bediensteten der Sächsischen Sicherheitswacht verbleiben. Weiterhin sollte in der Verwaltungsvorschrift auf die Vorschriften des § 35 SächsPolG i. V. m. §§ 9, 10 SächsDSG bezüglich des Einsatzes und der Zusammenarbeit mit den Bediensteten der Sächsischen Sicherheitswacht konkretisierend hingewiesen werden. Schließlich sollte die Verwaltungsvorschrift regeln, in welchen (Ausnahme-)Fällen die Polizeidienststelle personenbezogene Daten an die Sicherheitswacht weiterleiten darf.

Ein Großteil meiner Anregungen wurde bereits in die Neufassung des Referentenentwurfs eingearbeitet. Ich bin zuversichtlich, daß bei den weiteren Beratungen eine datenschutzgerechte Gestaltung des Gesetzes erarbeitet wird.

5.9.3 Entwürfe von Verwaltungsvorschriften zum Einsatz Verdeckter Ermittler und zur Inspruchnahme von Informanten und Vertrauenspersonen

Die polizeiliche Datenerhebung durch Verdeckte Ermittler, Informanten und Vertrauenspersonen will das SMI in Verwaltungsvorschriften regeln. Zu den Entwürfen habe ich Stellung genommen.

Auf meine Kritik stieß der gewählte Zeitpunkt für den Erlaß dieser Vorschriften. Nach § 36 Abs. 2 Nr. 3 SächsPolG gehört der Verdeckte Ermittler zu den besonderen Mitteln zur Erhebung von Daten. Die Vorschriften, die den Einsatz dieser Mittel regeln, hat der SächsVerfGH teilweise für verfassungswidrig erklärt. Aus diesem Grund habe ich angeregt, vor Erlaß der Verwaltungsvorschrift zum Einsatz Verdeckter Ermittler die erforderliche Neufassung des SächsPolG abzuwarten.

Das gleiche gilt für Regelungen, die den Einsatz von Vertrauenspersonen und Informanten regeln. Zwar werden diese nicht wie die Verdeckten Ermittler unter Geheimhaltung ihrer richtigen Identität und ihrer Eigenschaft als Polizeibeamte

eingesetzt. Ihr Einsatz zählt nicht zu den besonderen Mitteln zur Erhebung von Daten und unterliegt nicht den strengen Voraussetzungen des § 36 Abs. 2 Nr. 3 SächsPolG, die der SächsVerfGH zum Teil für verfassungswidrig erklärt hat. Trotzdem arbeiten sie im Auftrag der Polizei mit dieser zusammen. Wegen ihrer Einbindung in die polizeilichen Weisungsstränge unterscheidet sich ihr Einsatz aber kaum von demjenigen Verdeckter Ermittler. Insbesondere weil die Aktivitäten einer Vertrauensperson aus der Sicht des Betroffenen heimlich erfolgen, halte ich es für erforderlich, einschlägige Datenerhebungsvoraussetzungen im SächsPolG zu normieren. Die allgemeine Datenerhebungsvorschrift des § 37 SächsPolG, die die Datenerhebung bei Dritten regelt, berücksichtigt m. E. nicht die Tiefe des Grundrechtseingriffs durch Vertrauenspersonen, wenn diese von der Polizei gezielt und organisiert eingesetzt werden, um bestimmte Informationen zu gewinnen.

5.9.4 Richtlinien für die Führung kriminalpolizeilicher personenbezogener Sammlungen (KpS-Richtlinien)

Bereits in meinem 3. Tätigkeitsbericht (5.9.2) habe ich empfohlen, die ausfüllungsbedürftigen Generalklauseln des Sächsischen Polizeigesetzes durch weitere konkretisierende Regelungen in den KpS-Richtlinien zu präzisieren. Das SMI kündigte daraufhin an, daß meine Anregungen in den Ergänzungsnachtrag zu den KpS-Richtlinien aufgenommen würden. Der mir im vergangenen Jahr vom Landeskriminalamt übersandte Ergänzungsnachtrag enthielt allerdings weniger Präzisierungen als vielmehr Wiederholungen des Textes des Sächsischen Polizeigesetzes. So ist nach wie vor nicht eindeutig geregelt,
- welche Kriminalakten bei welcher Dienststelle geführt werden,
- wann Kriminalakten zusammenzuführen sind,
- wie sich der Besitzübergang von Kriminalakten vollzieht,
- daß kriminalaktenrelevante Unterlagen der kriminalaktenführenden Stelle zuzuleiten sind,
- wie die Akten zu ordnen sind,
- wer für die Bestimmung der Aufbewahrungsdauer und für die Löschung (z. B. bei Löschungsanträgen Betroffener) verantwortlich ist,

Weiterhin fehlte der von mir schon vor längerer Zeit vorgeschlagene klarstellende Zusatz, daß es sich bei den Aussonderungsprüffristen grundsätzlich - also von Ausnahmen, z. B. bei gestörten Sexualstraftätern, abgesehen - um Höchstfristen handelt. In den KpS-Richtlinien sollte deshalb deutlich darauf hingewiesen werden, daß die Dauer der Speicherung auf das erforderliche Maß zu beschränken ist und die Frist für die Speicherung personenbezogener Daten geprüft, festgelegt und im Rahmen der Vorgangsbearbeitung überprüft werden muß. Bereits im Jahre 1995 wurde mir vom SMI zugesagt, diesen Zusammenhang in einem Erlaß an die Polizeidienststellen zu verdeutlichen.

Wegen Auslegungsschwierigkeiten in der Praxis habe ich weiterhin angeregt, den Begriff der automatisierten Datei in den KpS-Richtlinien wie folgt zu definieren:

"Unter automatisierten Dateien sind alle Dateien zu verstehen, die durch automatisierte Verfahren ausgewertet werden können. Auch Textverarbeitungsautomaten können unter diesen Begriff fallen, wenn damit personenbezogene Daten ausgewertet werden können. Bei Dateien, die bei vielen Polizeidienststellen zum gleichen Zweck und nach einem gleichen Schema geführt werden, besteht die Möglichkeit, Rahmenerrichtungsanordnungen zu erlassen."

In diesem Zusammenhang habe ich auch gebeten festzulegen, daß bei dem erstmaligen Einsatz automatisierter Verfahren die Zustimmung des Sächsischen Staatsministeriums des Innern zu einer Errichtungsanordnung erst erteilt wird, wenn meine Behörde Gelegenheit hatte, zu dem Entwurf Stellung zu nehmen.

Vom SMI wurde mir zugesagt, einige meiner Empfehlungen bereits jetzt in die KpS-Richtlinien einzuarbeiten. Weitere Anregungen sollen leider erst mit der geplanten Neufassung der KpS-Richtlinien für den Freistaat Sachsen nach Inkrafttreten des Gesetzes über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten (BKA-Gesetz) und der Änderung der KpS-Richtlinien des Bundes aufgegriffen werden.

5.9.5 EUROPOL

Nach dem - noch nicht ratifizierten - EUROPOL-Übereinkommen soll EUROPOL die Leistungsfähigkeit der zuständigen Behörden der Mitgliedstaaten und ihre Zusammenarbeit verbessern, wenn es darum geht, den Terrorismus, den illegalen Drogenhandel und die sonstigen schwerwiegenden Formen der internationalen Kriminalität (z. B. Nuklearkriminalität, Waffenhandel, illegaler Technologietransfer, Menschenhandel, Ausbeutung der Prostitution, Raub und Erpressung, Umweltkriminalität, Kraftfahrzeugkriminalität) zu bekämpfen. EUROPOL darf jedoch erst tätig werden, wenn tatsächliche Anhaltspunkte für eine kriminelle Organisationsstruktur vorliegen und von den genannten Kriminalitätsformen zwei oder mehr Mitgliedsstaaten in einer Weise betroffen sind, die aufgrund des Umfangs, der Bedeutung und der Folgen der strafbaren Handlungen ein gemeinsames Vorgehen der Mitgliedsstaaten erfordert. EUROPOL soll mittels eines Zentralcomputers Daten-Material sammeln, zusammenstellen, auswerten, analysieren und die nationalen Stellen so bei ihren Ermittlungen sachdienlich unterstützen.

Die effiziente Zusammenarbeit der Polizeibehörden der Mitgliedsstaaten bei der Bekämpfung der internationalen Kriminalität im Rahmen von EUROPOL halte ich für unerläßlich; sie muß jedoch von einem hohen Datenschutzstandard geprägt sein. Dieses Erfordernis wird - zumindest in bezug auf die Ausgestaltung der Rechte des Betroffenen - nur ansatzweise durch die Konvention beachtet. So haben die Betroffenen beispielsweise bei EUROPOL kein Akteneinsichtsrecht. Auch die Ablehnungsmöglichkeiten beim Auskunftsrecht sind sehr weitgehend. Besonders schwer wiegt, daß die Betroffenen die sie betreffende Datenverarbeitung durch

EUROPOL nicht gerichtlich überprüfen lassen können. Aber es gibt die Möglichkeit, die supranationale Gemeinsame Kontrollinstanz anzurufen, der für Deutschland der Bundesbeauftragte für den Datenschutz sowie ein Vertreter des Bundesrates angehören wird; sie sichert eine durchgreifende Kontrolle der Datenverarbeitung dieser europäischen Polizeibehörde.

5.9.6 Polizeiliche Beobachtung

Das Instrument der polizeilichen Beobachtung (PB) wurde durch das Gesetz zur Bekämpfung der Organisierten Kriminalität (OrgKG) im Jahre 1992 in die StPO eingeführt. Sein Ziel ist es, Zusammenhänge und Querverbindungen innerhalb eines Personenkreises zu erkennen, wobei kriminelle Strukturen aufgehellt werden sollen. Im Einzelfall wird der Betroffene in der Personenfahndungsdatei (oder sein Kfz in der Sachfahndungsdatei) im Informationssystem der Polizei (INPOL) ausgeschrieben. Anläßlich von Personenkontrollen z. B. an Grenzen und auf Straßen werden im "Trefferfall" der Name, die Begleiter, das benutzte Kfz, das Reiseziel und andere relevant erscheinende Informationen unbemerkt notiert und an die ausschreibende Behörde übermittelt (sogenannte Erkenntnismitteilungen). Durch die zufällig erfolgenden Personenkontrollen unterscheidet sich die polizeiliche Beobachtung von der gezielten Observation einer Person.

Die Gesamtzahl der zur PB ausgeschriebenen Personen bewegt sich bundesweit stetig bei ungefähr 4000 Personen im Jahr. Im Freistaat Sachsen wird nach meinen Feststellungen das Mittel der PB weit weniger als im Bundesdurchschnitt eingesetzt.

Meine Kontrollen beim Landeskriminalamt Sachsen haben gezeigt, daß das besondere Mittel der PB grundsätzlich nur dann effektiv ist, wenn zu erwarten ist, daß die ausgeschriebene Person im Rahmen von Personenkontrollen erkannt wird.

Dies wird regelmäßig dann der Fall sein, wenn ein Auslandsbezug vorhanden ist. Denn sachdienliche Erkenntnismitteilungen kamen, wie ich festgestellt habe, fast ausschließlich von den Behörden des Bundesgrenzschutzes. In Fällen, in denen der der Ausschreibung zugrunde liegende Sachverhalt keine Anhaltspunkte für einen Auslandsbezug bot, gab es keine - oder nicht sachdienliche - Erkenntnismitteilungen. In diesen Fällen ist das besondere Mittel der Datenerhebung wohl wenig geeignet.

5.9.7 Lichtbildernachweis in PASS

Vom LKA wurde ich über Planungen informiert, einen Lichtbildernachweis in das Polizeiliche Auskunftssystem Sachsen (PASS) zu integrieren. Danach sollen die Lichtbilder nicht nur wie bisher über die Lichtbilderkarteien, sondern auch über den Bildschirm abrufbar sein. Ziel dieser Maßnahme soll es sein, den sachbearbeitenden Polizeibediensteten einen schnelleren Zugriff auf die Lichtbilder zu ermöglichen. Nicht vorgesehen ist ein automatisierter Bildvergleich, d. h. eine Bilderkennung; das Bild soll vielmehr nur über die Personendaten abrufbar sein.

Problematisch an dem geplanten Vorhaben ist, daß bisher dezentral und manuell geführte Lichtbilderkarteien durch ein zentrales, automatisiertes Verfahren ersetzt werden sollen und dadurch die Eingriffsintensität gegenüber der konventionellen Verfahrensweise verstärkt wird. Auch das Bundesverfassungsgericht betont die Gefahren, die dadurch entstehen, daß - vor allem beim Aufbau integrierter Informationssysteme - personenbezogene Daten mit anderen Datensammlungen zu einem teilweise oder weitgehend vollständigen Persönlichkeitsbild zusammengefaßt werden (BVerfGE 65, 1,42). Diese Gefahren bestünden auch hier, wenn bisher gesondert geführte Dateien (Lichtbilderkarteien) in das jetzt schon umfangreiche Informationssystem PASS integriert würden.

Das vom LKA geplante Vorhaben wäre nur unter strenger Beachtung des Verhältnismäßigkeitsgrundsatzes zulässig. Warum der beabsichtigte automatisierte und zentrale Zugriff auf Lichtbilder für die Polizeiarbeit in Sachsen unerläßlich ist, hat mir das LKA jedoch noch nicht ausreichend dargelegt. Gerade weil in Sachsen weniger ed-Maßnahmen als im Bundesdurchschnitt vorgenommen werden, müßte besonders begründet werden, warum die manuell geführten Lichtbilderkarteien nicht mehr ausreichen. Ein als - nicht näher präzisiertes - Argument angeführter Zeitverlust, der durch die Versendung der Lichtbilder entstünde, kann eine landesweite Abrufmöglichkeit (noch) nicht rechtfertigen. Im Rahmen der Prüfung der Verhältnismäßigkeit müßte außerdem geklärt werden, ob es nicht genügt, nur Lichtbilder derjenigen Personen in PASS zu speichern, bei denen Anhaltspunkte bestehen, daß der Zugriff auf ihre Lichtbilder mit einer großen Wahrscheinlichkeit erforderlich sein wird, also beispielsweise in Fällen schwerer Kriminalität. Ich habe das LKA gebeten, mir die Erforderlichkeit der Maßnahme unter den genannten Gesichtspunkten noch klarer zu belegen.

Für den Fall, daß die Lichtbildeinstellung in PASS erforderlich sein sollte - was letzendlich nur die Polizei selbst entscheiden kann -, habe ich weiterhin angeregt, durch eine Dienstanweisung klarzustellen, unter welchen konkreten Voraussetzungen Lichtbilder angefertigt und gespeichert werden dürfen. Darüber hinaus könnte dort auch geregelt werden, in welcher Art und Weise der Lichtbildernachweis in PASS zur Täteridentifizierung genutzt werden darf; beispielsweise dürften Zeugen nur das Lichtbild und nicht auch die anderen in PASS enthaltenen Daten zu sehen bekommen. Weiterhin habe ich das LKA gebeten zu prüfen, den Kreis der Polizeibediensteten, die

auf die Lichtbilderdatei zugreifen können, auf wenige Personen zu beschränken. Ferner müßte geklärt werden, ob nach Einführung des automatisierten Lichtbildernachweises die dezentral bei den örtlichen Polizeidienststellen und dem LKA geführten Lichtbilderkarteien überflüssig würden und vernichtet werden müßten.

5.9.8 Videoüberwachung am Leipziger Hauptbahnhof

Die Polizeidirektion Leipzig führt zur Zeit in der Leipziger Bahnhofsgegend ein befristetes Pilotprojekt durch, in dem eine Videokamera zur Überwachung von Kriminalitätsschwerpunkten eingesetzt wird. Die Überwachung erfolgt mittels einer auf einem Hausdach installierten, um 300 Grad schwenkbaren Kamera, die von der Beobachtungszentrale im Polizeirevier Leipzig Mitte aus bedient wird. Bei den kontinuierlich erfolgenden Übersichtsaufnahmen ist die Brennweite so eingestellt, daß die einzelnen Personen nicht identifizierbar sind. Der Bildausschnitt kann durch Zoom-Steuerung vergrößert und danach aufgezeichnet werden, wenn Anhaltspunkte z. B. für den Verdacht einer Straftat bestehen. Bestätigt sich dieser Verdacht nicht, wird die Aufzeichnung unverzüglich gelöscht. An mehreren Stellen innerhalb des überwachten Gebiets weisen Schilder in deutscher und englischer Sprache auf die Videoüberwachung hin.

Der Videoüberwachung habe ich - vorerst für eine begrenzte Zeit - zugestimmt, weil zunächst geprüft werden mußte, ob diese Maßnahme ein geeignetes polizeiliches Mittel ist, die überdurchschnittlich hohe Kriminalitätsbelastung (Kfz-Diebstähle, Taschendiebstähle, Rauschgiftdelikte) zu bekämpfen. Ungefähr ein Drittel der Gesamtkriminalität in Leipzig entfällt auf den Innenstadtbereich. Die bislang eingesetzte "Einsatzgruppe Innenstadt" war zwar mit offener und verdeckter Präsenz sowie Großaktionen (Razzien) erfolgreich, erforderte jedoch einen kaum vertretbaren Personaleinsatz. Zudem war problematisch, daß die Polizeibediensteten vor Ort keinen genügenden Überblick über das Geschehen hatten. Von Beginn an war ich in die Gestaltung des Videoprojekts - auch an Ort und Stelle - eingebunden.

Aus datenschutzrechtlicher Sicht ist beim Einsatz von Videotechnik zu bedenken, daß die betroffenen Passanten einem gewissen Überwachungsdruck ausgesetzt werden, der bei manchem Auswirkungen auf das subjektive Gefühl einer freien Entfaltung seiner Persönlichkeit im überwachten Bereich auslöst. Auch wenn bloß Übersichtsaufnahmen angefertigt werden, die eine Identifizierung von Personen nicht zulassen, reicht bereits das bei einigen entstehende Gefühl aus, einen Eingriff in das Recht auf informationelle Selbstbestimmung zu bejahen.

Der Betroffene sieht nur die Videokamera. Ob sie eingeschaltet ist und ob sie Übersichtsaufnahmen erstellt oder ob er gezielt beobachtet wird und von ihm Aufzeichnungen angefertigt werden, kann er dagegen nicht beurteilen. Selbst wenn er über den Umfang der Maßnahme ausführlich informiert wird und weiß, daß Aufzeichnungen nur zu Strafverfolgungszwecken (wenn ein hinreichender Tatverdacht besteht) angefertigt werden, kann ein Passant kaum ausschließen, daß sein Bild

versehentlich - oder weil er sich in diesem Moment gerade zufällig im Aufnahmebereich befindet - von der Polizei aufgezeichnet wird. Allein diese Ungewißheit kann dazu führen, daß die Betroffenen sich nicht mehr ungezwungen, sondern "kameraorientiert" verhalten.

Dieser Eingriff in das Recht auf informationelle Selbstbestimmung wird von den meisten zwar als normal, also sozialadäquat angesehen, er ist aber nicht durch eine Einwilligung aller Betroffenen gedeckt. Es kann keine stillschweigende Einwilligung darin gesehen werden, daß den betroffenen Passanten die Videoüberwachung bekannt ist. Zwar kann es vertrauensbildend wirken, wenn die Polizei nicht heimlich agiert, sondern ausführlich über Sinn und Zweck der Maßnahme informiert. Von einer (freiwilligen) Einwilligung kann jedoch keine Rede sein, weil es keine oder nur unzureichende Alternativen zum Betreten des überwachten Innenstadt- und Bahnhofsgebietes gibt.

Bei der Suche nach einer Rechtsgrundlage kommen die § 38 Abs. 2 SächsPolG und § 100 c Abs. 1 StPO in Betracht, je nachdem, ob es sich um eine Maßnahme zur Gefahrenabwehr oder Strafverfolgung handelt. Bei der Rechtmäßigkeitsprüfung besonders zu beachten ist dabei der verfassungsrechtliche Grundsatz der Verhältnismäßigkeit. Ich habe unter anderem zu bedenken gegeben, daß verstärkte Überwachungsmaßnahmen der Polizei zwar dazu führen können, daß die Kriminalität an den überwachten Stellen zurückgeht, sich dann aber möglicherweise auf Orte verlagert, die nicht kontrolliert werden. Ob die auf dem Hausdach installierte Kamera es dem beobachtenden Polizeibediensteten überhaupt ermöglicht, aufgrund des Übersichtsbildes einen hinreichenden Straftatverdacht zu gewinnen, der ihm erst das Heranzoomen und Aufzeichnen erlaubt, muß die Erfahrung zeigen. Es dürfte auch schwer zu unterscheiden sein, ob ein berechtigter Fahrzeughalter sein Kfz aufschließt und etwas herausholt oder ob ein Dieb am Werke ist.

Meine Bedenken konnten jedoch weitgehend durch technische Verfeinerungen ausgeräumt werden. Eine Dienstanweisung für die beobachtenden Polizeibediensteten garantiert eine zulässige und zuverlässige Datenverarbeitung.

5.9.9 Videoüberwachung des Autobahnverkehrs durch die Polizei

Das Autobahnpolizeirevier Dresden setzt zur Ermittlung von Verkehrsverstößen im Zusammenhang mit Geschwindigkeitsübertretungen mit Videotechnik ausgestattete Fahrzeuge ein, die mögliche Raser verfolgen. Das Verfahren habe ich kontrolliert und dabei folgendes festgestellt: Eine Aufzeichnung erfolgt dann, wenn ein Verkehrsteilnehmer mit mehr als 21 km/h über der erlaubten Geschwindigkeit fährt. In diesem Fall erfolgen anschließend insgesamt drei Messungen, die zusammen in der Regel etwa drei Minuten (ein Aufzeichnungsvorgang erfordert eine Fahrstrecke von 500 m) dauern. Anschließend wird das Fahrzeug angehalten und dem Fahrer der Videofilm vorgeführt. Zwecks Dokumentation des Verwaltungshandelns und zum schnelleren Auffinden eines bestimmten Vorgangs auf der Videocassette führen die

Polizeibediensteten sogenannte Aufzeichnungsbücher, die in Anbetracht des parallel zu erstellenden, automatisierten Vorkommnisberichts die Gefahr der Doppelspeicherung bergen.

Ich halte die Überwachung des Autobahnverkehrs für dringend notwendig, bemängele aber, daß es für das automatisierte Videoaufzeichnungsverfahren keine Errichtungsanordnung gibt, die nach § 50 SächsPolG zu erstellen ist. Meiner Empfehlung, die Videoüberwachung des Autobahnverkehrs in einer solchen Dienstanweisung zu regeln, soll nach Mitteilung des SMI durch einen "Verkehrsüberwachungserlaß" entsprochen werden.

5.9.10 "Initiativermittlungen" im Rahmen der Bekämpfung der Organisierten Kriminalität

Beim Versuch der Strafverfolgungsbehörden, der - schwammig definierten - "Organisierten Kriminalität" (OK) Herr zu werden, versagt in vielen Fällen das klassische Bekämpfungsinstrumentarium. Aus Sicht der Sicherheitsbehörden sind Aufklärungserfolge, die auch die Hintermänner als Täter überführen, nur durch neue, tief in das Persönlichkeitsrecht eingreifende Ermittlungsmethoden zu erzielen.

Dazu gehören die sog. "Initiativermittlungen". Sie sollen bereits im Vorfeld eines Verdachtes zulässig sein, können also ausnahmsweise ohne einen konkreten Anfangsverdacht i. S. v. § 152 Abs. 2 StPO vorgenommen werden. Sie dienen dazu, einen wirklichen personenbeziehbaren Verdacht erst einmal zu gewinnen. Angesichts der Gefährlichkeit der Organisierten Kriminalität können solche Eingriffe - allerdings nur unter bestimmten Voraussetzungen - durchaus erforderlich sein. Zu beachten ist insbesondere der Grundsatz der Verhältnismäßigkeit: Es darf nicht sein, daß Staatsanwaltschaft und Polizei unter bloßer Nennung des Zauberwortes "OK" ermitteln und den Rechtsschutz der Betroffenen dadurch stark eingeschränken, daß die Informationsbeschaffung heimlich geschieht. Je weiter im Vorfeld von Straftaten ermittelt wird, um so größer ist auch die Gefahr, daß Daten Unbeteiligter verarbeitet werden. Dem muß durch klare Rechtsvorschriften begegnet werden. Darüber bin ich mit der Führung der sächsischen Polizei einig.

Initiativermittlungen (Ermittlungen ohne Anfangsverdacht) im Bereich der Organsisierten Kriminalität sollten deshalb nur unter folgenden Voraussetzungen zulässig sein:

- Die Straftaten, die das intensivere Instrumentarium rechtfertigen, müssen so konkret wie möglich bezeichnet werden.

- Es müssen konkrete Regelungen geschaffen werden, die eine Verwendung solcher Daten regeln, deren Verarbeitung sich im nachhinein als nicht notwendig herausstellt (Zweckbindungsgrundsatz). Hierunter fallen insbesondere Daten unbeteiligter Dritter. Aber auch Daten Betroffener, bei denen zwar der Bezug zur OK ausgeschlossen

werden kann, nicht aber der Verdacht in bezug auf die Begehung einer leichteren Straftat, dürfen nur unter bestimmten Voraussetzungen verarbeitet werden.

- Der Umfang der Initiativermittlungen muß ausführlich dokumentiert werden, um die notwendige interne und externe Kontrolle der Polizeibeamten und ihrer Informanten ausreichend sicherzustellen. In diesem Zusammenhang könnte auch daran gedacht werden, im OK-Bereich bei Initiativerermittlungen eine externe Kontrollinstanz einzuschalten, die die Zulässigkeit der Datenverarbeitung überprüft.

Das SMI habe ich gebeten, ein entsprechende Verfahrensweise sicherzustellen und in Entwürfen zu Rechtsvorschriften zu fassen.

5.9.11 Aufbewahrung von Unterlagen aus der strafprozessualen Fernmeldeüberwachung bei der Polizei

Zu Zwecken der Strafverfolgung ist unter den Voraussetzungen des § 100 a StPO die Überwachung des Fernmeldeverkehrs des Beschuldigten zulässig. Sind die hierdurch erlangten Unterlagen zur Strafverfolgung nicht mehr erforderlich, müssen sie gemäß § 100 b Abs. 6 StPO unverzüglich vernichtet werden. Die Entscheidung über die Vernichtung trifft im Ermittlungsverfahren die Staatsanwaltschaft, danach das mit der Sache befaßte Gericht.
Hierbei ist zu prüfen, ob die Unterlagen für die Strafverfolgung noch erforderlich sind oder nicht. Nicht mehr erforderlich sind sie spätestens mit Rechtskraft des Urteils in dem Verfahren, für welches sie erhoben worden sind bzw. gemäß § 100 b Abs. 5 StPO (Zufallsfunde) erhoben werden durften. Der Gedanke, die Unterlagen müßten für den Fall eines Wiederaufnahmeverfahrens aufbewahrt werden, kann nur in Ausnahmefällen zum Tragen kommen: Wiederaufnahmeverfahren sind grundsätzlich zeitlich unbefristet möglich - sogar über den Tod des Verurteilten hinaus. Da sich die Beweiserheblichkeit der Unterlagen für ein solches Verfahren nicht von vornherein ausschließen läßt, liefe die Pflicht zur Vernichtung leer.
Eine Aufbewahrung der Unterlagen über den Zeitpunkt der Rechtskraft des Urteils hinaus kommt also nur in Ausnahmefällen in Betracht, z. B. dann, wenn naheliegende Anhaltspunkte dafür erkennbar sind, daß es zu einem Wiederaufnahmeverfahren kommen und das Material hierfür von beweiserheblicher Bedeutung sein wird. Eine entsprechend restriktive Aufbewahrungsregelung hat das SMJus gegenüber dem Generalstaatsanwalt des Freistaates Sachsen getroffen.

5.9.12 Namensgleichheit in INPOL

Ein Petent wandte sich wegen der - wie sich später herausstellte: berechtigten - Befürchtung an mich, versehentlich im Informationssystem der Polizei (INPOL) gespeichert zu sein. Grund zu dieser Vermutung hatte er, weil er auffallend oft in Polizeikontrollen geriet. Ursache der versehentlichen Speicherung in INPOL war, daß eine andere Person bei ihrer erkennungsdienstlichen Behandlung den Namen des Petenten als sog. Aliasnamen angegeben hatte.

Um Verwechslungen des Petenten mit der anderen, rechtmäßig in INPOL gespeicherten Person zu verhindern, veranlaßte das Landeskriminalamt auf meine Initiative hin einen Vermerk in INPOL, aus dem sich ergibt, daß der Name des Petenten als Aliasname von einer anderen Person benutzt wird. Auch wurde in INPOL die Bundespersonalausweisnummer des Petenten vermerkt, um den kontrollierenden Polizeibediensteten deutlich zu machen, daß es sich bei der angetroffenen Person um den rechtmäßigen Namensträger handelt, der nicht in INPOL gespeichert ist.

5.9.13 Ermittlungen in einem "Taximörderfall"

Bei den Ermittlungen zu einem Dresdner "Taximörderfall" konnte aufgrund von Zeugenaussagen ein Phantombild des letzten bekannten Taxifahrgastes erstellt werden. Am Tatort waren Fingerspuren gesichert worden, die wahrscheinlich vom Täter stammten. Das daraufhin im Rahmen der Öffentlichkeitsfahndung in einer Zeitung veröffentlichte Phantombild führte mehrfach zu Personenhinweisen. Die Hinweisgeber wurden sämtlich von der Polizei vorgeladen, über den Sachverhalt informiert und ausdrücklich darauf hingewiesen, daß sie nicht als Beschuldigte vorgeladen wurden. Vielmehr seien sie gebeten, der Polizei bei der Aufklärung des Verbrechens zu helfen, indem sie ed-Maßnahmen bei sich durchführen ließen. Sie wurden darüber aufgeklärt, daß die von ihnen gefertigten Lichtbilder Zeugen vorgelegt und ihre Fingerabdrücke mit den Tatspuren verglichen würden. Schließlich wurde ihnen versichert, alle Unterlagen bei Nichtübereinstimmung unverzüglich zu löschen. Sämtliche Personen erklärten sich daraufhin bereit, Lichtbilder und Fingerabdrücke von sich fertigen zu lassen. Ende Juli 1996 wurde dann der Beschuldigte - auf andere Weise - ermittelt, woraufhin sämtliche ed-Unterlagen - außer denen des Beschuldigten - vernichtet wurden. Hiervon habe ich mich durch einen Kontrollbesuch beim Polizeipräsdium Dresden überzeugt und festgestellt, daß die Verfahrensweise im konkreten Fall datenschutzrechtlich nicht zu beanstanden war.

5.9.14 Ermittlungen im Rahmen von "Scheineheverfahren" nach § 92 Abs. 2 Nr. 2 AuslG

Das SMI habe ich darauf hingewiesen, daß Fragen zum ehelichen Sexualverhalten von der Polizei grundsätzlich nicht gestellt werden dürften, weil diese Frage den Bereich der besonders geschützten Intimsphäre berührt. Selbst so gewichtige Allgemeininteressen wie beispielsweise die Strafverfolgung erlauben keinen Eingriff

in den Bereich intimer, höchst privater Lebensgestaltung. Ein Eingriff in das Grundrecht wäre nur dann erlaubt, wenn die Befragung das einzige Mittel zur Aufklärung einer schweren Straftat wäre (vgl. BVerfGE 34, 238, 249 f.). Das Führen einer sog. "Scheinehe", um jemandem eine Aufenthaltsgenehmigung oder -duldung zu beschaffen, fällt ersichtlich nicht unter den Begriff der schweren Straftat. Fragen zum ehelichen Sexualverhalten im oben genannten Zusammenhang sind demnach unzulässig und haben zu unterbleiben. Das SMI teilt meine Rechtsauffassung; das ist erfreulich.

5.9.15 Speicherung von Wiederholungsfällen bei Verstößen im ruhenden Verkehr

Auf meine Initiative hin hatte das SMI bereits im Jahr 1994 per Erlaß den sächsischen Bußgeldstellen untersagt, Dateien oder Karteien zur Erfassung von Wiederholungstätern bei Verstößen im ruhenden Verkehr zu führen (vgl. 3. Tätigkeitsbericht unter 5.9.7).

Mir liegen jedoch Unterlagen vor, die darauf schließen lassen, daß diese Weisungslage nicht im erforderlichen Maße beachtet wird. Beispielsweise wurde vom Ordnungsamt der Stadt Leipzig im Zusammenhang mit einer hier einschlägigen Ordnungswidrigkeit festgestellt, daß wiederholt der verantwortliche Fahrzeugführer nicht zweifelsfrei durch den Halter bekanntgegeben wurde; man behalte sich deshalb vor, bei weiteren Verfahren einen Antrag auf Fahrtenbuchauflage zu stellen. Hieraus habe ich geschlossen, daß in diesen Fällen offenbar doch Daten über Ordnungswidrigkeiten gespeichert werden. Zwar ist richtig, daß vor der Anordnung einer Fahrtenbuchauflage unter anderem geprüft werden muß, ob die Maßnahme verhältnismäßig ist. Im Rahmen dieser Prüfung kann auch eine Rolle spielen, ob eine Verkehrsordnungswidrigkeit wiederholt begangen wurde. Dazu können die Daten aus Flensburg herangezogen werden. Entscheidend muß es nämlich auf die Gewichtigkeit der Verstöße ankommen, so daß es mir (und der Rechtsprechung) bedenklich erscheint, allein wegen der Begehung einiger geringfügiger Ordnungswidrigkeiten im ruhenden Verkehr (Halt- und Parkverstöße) ein Fahrtenbuch aufzuerlegen. Schließlich kann in diesen Fällen die disziplinierende Wirkung des Fahrtenbuchs schon durch die sog. Halterhaftung erzielt werden, wonach die Verfahrenskosten dem Halter auferlegt werden können.

Vor allem aber fehlt es für eine solche Speicherung - wie dem Erlaß des Sächsischen Staatsministeriums des Innern zu entnehmen ist - an der erforderlichen Rechtsgrundlage. Die Zulässigkeitsvoraussetzungen für die Speicherung von Daten sind in den § 28 bis 30 a StVG abschließend geregelt. Folge ist, daß außerhalb des beim Kraftfahrt-Bundesamt geführten Verkehrszentralregisters keine Datenspeicherungen im Bereich von geringfügigen Ordnungswidrigkeiten zulässig sind.

5.9.16 Praktikanten bei der Polizei

Der Sächsische Verfassungsgerichtshof hat in seinem Urteil zum Sächsischen Polizeigesetz auch festgestellt, daß eine Nutzung personenbezogener Daten durch den Polizeivollzugsdienst zu Zwecken der (polizeiinternen) Aus- und Fortbildung nur ausnahmsweise zulässig ist. Die Anonymisierung personenbezogener Daten darf nur dann unterbleiben, wenn sie nicht mit vertretbarem Aufwand möglich ist oder dem Aus- oder Fortbildungszweck entgegensteht und die berechtigten Interessen des Betroffenen an der Geheimhaltung der Daten nicht offensichtlich überwiegen. Die verfassungskonforme Auslegung der einschlägigen Vorschrift (§ 43 Abs. 6 SächsPolG) ergebe, daß die berechtigten Interessen des Betroffenen an der Geheimhaltung seiner Daten regelmäßig überwiegen. Dies insbesondere deshalb, weil "eine effektive Schulung des Personals regelmäßig auch unter Verwendung anonymisierten Datenmaterials möglich sein wird."

Diese vom Sächsischen Verfassungsgerichtshof für die polizeiinterne Ausbildung aufgestellten Grundsätze müssen erst recht für den Einsatz polizeifremder Praktikanten gelten. Auf den Einsatz von Schülern im Rahmen von Betriebspraktika sollte deshalb ganz verzichtet werden. An Studenten, die ein Praktikum beim Polizeivollzugsdienst absolvieren, sollten grundsätzlich keine personenbezogenen Daten übermittelt werden. Schließlich müßten Schutzvorkehrungen getroffen werden, die verhindern, daß Praktikanten unnötig personenbezogene Daten zur Kenntnis erhalten. Hingegen sind Rechtsreferendare Beamte auf Widerruf; bei ihnen sehe ich daher keine Probleme.

Vom Sächsischen Staatsministerium des Innern wurde mir mitgeteilt, daß Betriebspraktika für Schüler der allgemeinbildenden Schulen beim Polizeivollzugsdienst des Freistaates Sachsen nicht durchgeführt würden. Weiterhin wurde vom Sächsischen Staatsministerium des Innern durch Erlaß sichergestellt, daß die Studenten "zu Beginn ihres Praktikums nach Maßgabe des Verpflichtungsgesetzes auf die gewissenhafte Erfüllung ihrer Obliegenheiten, insbesondere der Pflicht zur Verschwiegenheit und der Einhaltung des Datengeheimnisses, förmlich zu verpflichten" sind. Die Praktikanten hätten während des Praktikums "nur die für die Erfüllung des Praktikumzieles unbedingt erforderlichen personenbezogenen Daten" zur Kenntnis zu erhalten. Dieser Erlaß ist zwar durchaus geeignet, die Beschäftigten der Polizei, die die Praktikanten betreuen, für Datenschutzbelange in diesem Bereich zu sensibilisieren. Wünschenswert wäre allerdings gewesen, wenn der Erlaß konkreter umrissen hätte, in welchen (Ausnahme-)Fällen personenbezogene Daten an Studenten übermittelt werden dürfen und welche Schutzvorkehrungen zu treffen sind, um eine unnötige Kenntnisnahme personenbezogener Daten zu verhindern.

5.9.17 Auskunftsersuchen an meine Dienststelle

Immer wieder fragen mich Petenten, welche Daten über sie bei der Polizei gespeichert sind. Selbstverständlich könnte ich dies im Rahmen meiner Kontrollbefugnisse in Erfahrung bringen. Denn nach §§ 24, 25 SächsDSG habe ich den Umfang und die

Rechtmäßigkeit sämtlicher bei den öffentlichen Stellen des Freistaates Sachsen gespeicherten personenbezogenen Daten zu kontrollieren. Allerdings bin ich ohne Genehmigung der Polizei nicht dazu befugt, dem Petenten die zu ihm gespeicherten Daten mitzuteilen.

Nach § 51 SächsPolG i. V. m. § 17 SächsDSG hat jedermann gegenüber der speichernden Polizeidienststelle einen Anspruch auf kostenlose Auskunft über die zur Person gespeicherten Daten. Auch kann Auskunft über den jeweiligen Zweck der Speicherung sowie über die Herkunft der Daten, die Empfänger von Datenübermittlungen und die jeweils übermittelten Daten verlangt werden. Lehnt die Polizeidienststelle den Antrag ab, muß sie den Betroffenen nach § 17 Abs. 6 Satz 2 SächsDSG darauf hinweisen, daß er sich an mich wenden kann, damit ich den Sachverhalt datenschutzrechtlich überprüfen kann. Allerdings darf dann meine Mitteilung an den Betroffenen keine Rückschlüsse auf den Erkenntnisstand der Polizeidienststelle zulassen, es sei denn, diese stimmt einer weitergehenden Auskunft zu.

5.9.18 Pressearbeit der Polizei

Weil das Informationsbedürfnis der Öffentlichkeit im Bereich polizeilicher Aufgabenerfüllung besonders ausgeprägt ist, habe ich beim SMI angeregt, den Polizeidienststellen eine verbindliche Handlungsanweisung zu geben, die ihnen hilft, die widerstreitenden Grundrechtspositionen verfassungskonform gegeneinander abzuwägen. Wie ich bereits im Zusammenhang mit der von mir beanstandeten Verwaltungsvorschrift über das Justizpressewesen (4. Tätigkeitsbericht 8.1) ausführlich dargelegt habe, besteht häufig ein Spannungsverhältnis zwischen dem Informationsrecht der Öffentlichkeit und dem Persönlichkeitsrecht des Einzelnen. Wie Gespräche mit Pressesprechern der Polizei mir zeigen, könnte ein entsprechender Erlaß, den es in einigen anderen Bundesländern bereits gibt, die Arbeit mit der Presse wesentlich erleichtern.

Eine solche Regelung muß auf jeden Fall die Unschuldsvermutung beachten, die es grundsätzlich verbietet, den Namen eines Beschuldigten, eine Abbildung oder sonstige Hinweise auf seine Person im Rahmen eines Ermittlungsverfahrens zu veröffentlichen. Aber auch die Ausnahmen von diesem Grundsatz (z. B. Nennung von Daten sog. "absoluter Personen der Zeitgeschichte" oder - bereits verurteilter - "relativer Personen der Zeitgeschichte" oder im Rahmen der Öffentlichkeitsfahndung) sollten möglichst detailliert beschrieben werden. Darüber hinaus sollte klargestellt werden, daß die Pressestellen der Polizeidienststellen mit personenbezogenen Daten so restriktiv wie möglich umzugehen haben, damit auch Personen aus dem Umfeld des Betroffenen diesen durch die veröffentlichten Angaben nicht identifizieren können. Bereits jetzt werden grundsätzlich in den Polizeiberichten der polizeilichen Pressestellen weder die Vornamen noch die Anfangsbuchstaben der Nachnamen der Betroffenen genannt. Ich habe angeregt, diese gute Praxis in der generellen Anweisung festzuschreiben.

Das SMI hat mir in Aussicht gestellt, einen solchen Erlaß zu erarbeiten.

5.10 Verfassungsschutz

Beratung und Kontrolle des Landesamtes für Verfassungsschutz

Wie in den Vorjahren konnte ich auch im Berichtszeitraum beim Landesamt für Verfassungsschutz ein hohes Maß an Aufgeschlossenheit gegenüber datenschutzrechtlichen Positionen registrieren. Aus Anlaß von Eingaben führte ich mehrere Kontrollen im Landesamt durch. In keinem Fall mußte ich eine Beanstandung aussprechen. Ein datenschutzrechtlicher Mangel sei allerdings an dieser Stelle aufgezeigt:

Bei einer Kontrolle stellte ich fest, daß im LfV nach Eingang meiner Mitteilung, die zu einem Petenten geführte Akte prüfen zu wollen, Aktenstücke vernichtet wurden, bevor ich kontrolliert hatte. Ein „datenschutzrechtlicher Schaden" trat glücklicherweise aber nicht ein, weil anhand der noch vorhandenen Vernichtungsprotokolle rekonstruiert werden konnte, welche Informationen vernichtet worden waren. Die Informationen waren nämlich noch in den parallel geführten Sachakten enthalten und konnten auf diese Weise gefunden werden. Aufgrund meiner Kritik erließ das LfV umgehend eine schriftliche Dienstanweisung, mit der nach Eingang meiner Ankündigung, eine Datenschutzkontrolle durchzuführen, eine Veränderungssperre für Akten verfügt wird. Ebenfalls per Hausverfügung wurde geregelt, daß Ermittlungen von Wohnsitzen auf das „Notwendige und rechtlich Zulässige" zu beschränken sind. Somit ist sichergestellt, daß Anschriften beispielsweise aus der Kinderzeit der Betroffenen nicht ermittelt und Akteninhalt werden. Dies ist bedeutsam, weil nach dem Sächsischen Verfassungsschutzgesetz die Verarbeitung von Daten Minderjähriger unter 16 Jahren verboten ist. Ebenfalls per Hausverfügung wurde festgelegt, daß Akten zeitlich eindeutig datiert sind. Hintergrund war meine Feststellung, daß ein Eingangsvermerk einer Akte nicht datiert war, so daß nicht exakt festgestellt werden konnte, wann die Akte angelegt wurde.

Positiv hervorzuheben ist, daß die interne Datenschutzkontrolle beim LfV sachgerecht institutionalisiert ist. Die strikte Umsetzung von datenschutzrechtlichen Hinweisen ist nach meinen Kontrollerfahrungen jederzeit gewährleistet. So kündigte der behördliche Datenschutzbeauftragte aus Anlaß einer meiner Kontrollen per Hausverfügung eine interne Querschnittsprüfung bestimmter Aktenbestände im gesamten Amt an.

Im Zusammenhang mit der Einführung des amtsinternen Informationssystems ISIS (4. Tätigkeitsbericht, 5.10.1) traten vereinzelt Schwierigkeiten bei der Zusammenführung bislang manuell geführter, in Akten gespeicherter Informationsbestände auf. Ich habe mich jedoch davon überzeugen können, daß die Amtsleitung die Probleme erkannt hat und lösen wird.

Als erfreulich möchte ich hervorheben, daß das LfV Auskunftsersuchen nicht pauschal mit dem Hinweis auf § 9 Abs. 2 SächsVerfG „abwehrt", eine materielle Auskunft gefährde die Aufgabenerfüllung des Amtes. So setzte sich das LfV mehrfach mit mir in Verbindung, um Petenten, die mit einer gewissen Berechtigung davon ausgehen

durften, daß ihre Daten vom LfV erfaßt sind, eine inhaltliche Auskunft zu geben. Diese Art, transparent mit vorhandenen Informationen umzugehen, wird in bestimmten Fällen durchaus auch präventive Wirkung haben.

5.11 Landessystemkonzept / Landesnetz

InfoHighway Landesverwaltung

Die im Juni 1995 bei der Staatskanzlei gegründete "Koordinierungs- und Beratungsstelle für Informations- und Kommunikationstechnik (KoBIT)" wurde nach dem Kabinettbeschluß vom 13. Februar 1996 mit der Erarbeitung eines Konzeptes "InfoHighway Landesverwaltung" beauftragt. Der von ihr geleitete gleichnamige Arbeitskreis (AK), zu dessen Beratungen ich hinzugezogen werde, hat sich mittlerweile in mehreren Schritten, die jeweils mit der Verabschiedung eines Arbeitspaketes beendet wurden, mit dem Thema befaßt.

Nach einer Beschreibung des Kommunikationsbedarfes und der Ziele der Landesbehörden sowie einer Bestandsaufnahme und Analyse der Kommunikationsstruktur wurden technische, organisatorische und betriebliche Anforderungen ermittelt. Auf dieser Grundlage hat der AK verschiedene Lösungskonzepte für den "InfoHighway" formuliert:

- ein "Virtual Private Network" (die Landesverwaltung bekommt von einem Auftragnehmer bestimmte Dienste geliefert, hat aber keinen Einfluß auf die Art und Weise, wie dies geschieht),
- ein "Corporate Network" (der Freistaat macht und bestimmt alles selbst)
- "Betrieb durch einen Generalunternehmer" (eine Mischform: Der Generalunternehmer liefert bestimmte vorgegebene Dienste, der Freistaat kann aber bei der Umsetzung mitbestimmen).

Im März 1997 entschied sich der Arbeitskreis in einer Grundsatzentscheidung für die letzte Variante. Sie wird zur Zeit genauer untersucht.

Datenschutzrechtliche Fragen tauchten in mehreren Arbeitsschritten auf. Sie wurden von dem Arbeitskreis angemessen berücksichtigt. Ich unterstütze diesen Prozeß und werde ihn intensiv begleiten.

5.12 Ausländerwesen

Abgabe des Personalausweises bei Besuch eines Asylbewerberheims

Das von einem Asylbewerberheim praktizierte Verfahren, sich von Heimbesuchern den Personalausweis aushändigen zu lassen und den Betroffenen erst beim Verlassen

des Heimgeländes wiederzugeben, war datenschutzrechtlich nicht zu beanstanden. Diese Verfahrensweise ist vom „Hausrecht“ gedeckt. Hierunter versteht man das durch § 123 StGB (Hausfriedensbruch) geschützte und auf Eigentum bzw. Besitz begründete Recht, darüber zu bestimmen, welche Personen sich aus welchem Grund und wie lange in einem Raum oder auf einem Gelände aufhalten dürfen. Von diesem Recht mitumfaßt ist auch die Befugnis, Vorkehrungen zum Schutz des Hausrechts zu treffen.

Das Einbehalten von Personalausweisen der Heimbesucher während der Besuchszeit halte ich für geeignet, sicherzustellen, daß die Besucher des Heims nach Beendigung des Besuchs das Heimgelände wieder ordnungsgemäß verlassen. Nicht zulässig wäre jedoch das Kopieren der Ausweispapiere und deren Aufbewahrung.

5.13 Sonstiges

5.13.1 Sächsisches Sammlungsgesetz

Relativ spät wurde ich am Entwurf eines Sächsischen Sammlungsgesetzes beteiligt. Erst zu den Ausschußberatungen im Sächsischen Landtag wurde ich hinzugezogen.

Meine Bitten, verschiedene Bestimmungen an den Grundsätzen des "Volkszählungsurteils" vom 15.12.1983 (BVerfGE 65, 1, 42, 44) zu messen, wurden ausführlich mit dem zutreffenden Ergebnis erörtert, daß § 9 (Verpflichtung des Veranstalters, der zuständigen Behörde auf Verlangen Auskünfte zu geben und Unterlagen vorzulegen) dem Erforderlichkeitsgrundsatz entspricht.

5.13.2 Datenschutz im Einbürgerungsverfahren

Die Einbürgerungsbehörde prüft, ob der Bewerber die gesetzlichen Voraussetzungen für eine Einbürgerung erfüllt. Hierzu kann es erforderlich sein, daß sie auch Informationen vom Arbeitsamt, Sozialamt bzw. der Finanzbehörde einholt.
Das SMI beteiligte mich an einem Erlaß, in dem die Einbürgerungsbehörden u.a. zur datenschutzgerechten Abwicklung solcher Datenerhebungen angehalten werden sollten.
Eine vorgesehene Einwilligungserklärung und ein dazugehöriges Hinweisblatt für die Antragsteller entsprachen meinen Vorstellungen nicht. U. a. ließen die Entwürfe die Entbindung der beteiligten Behörden vom Sozialgeheimnis bzw. Steuergeheimnis vermissen.
Ich stellte deshalb klar, daß die beabsichtigte Verfahrensweise mit dem Grundsatz, die Daten (die nicht allgemein zugänglich sind) zunächst beim Einbürgerungsbewerber selbst zu erheben (§ 11 Abs. 2 Satz 1 SächsDSG), nicht zu vereinbaren sei. Auch wies ich darauf hin, daß dem Betroffenen durch die Verweigerung der Einwilligung keine Rechtsnachteile entstehen dürfen (§ 4 Abs. 2 Satz 2 SächsDSG).
Weil es sich bei der beabsichtigten Datenerhebung beim Sozialamt, Arbeitsamt bzw. Finanzamt um eine “Datenerhebung bei Dritten” handelt, für die es keine spezielle

Rechtsgrundlage gibt, ist § 11 Abs. 4 Nr. 2 SächsDSG einschlägig. Danach ist die mit einer Durchbrechung des Sozial- und Steuergeheimnisses einhergehende Datenerhebung bei den in Rede stehenden Behörden von der Einwilligung der Betroffenen abhängig.

Ich schlug daher für das Informationsblatt folgende Formulierungen vor:

"...Zur Bearbeitung Ihres Einbürgerungsantrags kann es unter Umständen erforderlich sein, daß Sie uns Unterlagen vom zuständigen Sozialamt, vom Arbeitsamt bzw. vom Finanzamt vorlegen müssen (z.B. Bescheinigung über den Bezug von Sozialhilfe, Bescheinigung über den Bezug von Arbeitslosengeld, Steuerbescheid).
Um sich den Weg zu diesen Behörden zu ersparen, können Sie uns ermächtigen, die erforderlichen Informationen dort unmittelbar anzufordern. Diese Behörden dürfen uns nämlich ohne Ihre ausdrückliche Einwilligung keine Informationen übermitteln, da sie dem Sozialgeheimnis bzw. dem Steuergeheimnis unterliegen. Zur Beschleunigung des Verfahrens empfehlen wir daher, beiliegende Einwilligungserklärung zu unterschreiben. ..."

Die Einwilligungserklärung bat ich wie folgt zu fassen:

"Ich bin damit einverstanden, daß sich die Einbürgerungsbehörde zur Prüfung der Voraussetzungen der von mir beantragten Einbürgerung vom Arbeitsamt, Sozialamt bzw. dem Finanzamt die erforderlichen Daten übermitteln läßt. Die beteiligten Stellen entbinde ich insoweit vom Sozialgeheimnis bzw. vom Steuergeheimnis. Die Einwilligung erstreckt sich auf die nachfolgenden von der Einbürgerungsbehörde durch Ankreuzen gekennzeichneten Bereiche:

die beim Finanzamt vorhandenen dem Steuergeheimnis unterliegenden Daten,
die beim Sozialamt vorhandenen Daten über meinen Sozialhilfebezug sowie die dem zugrundliegenden tatsächlichen Umstände,
die beim Arbeitsamt vorhandenen Daten über meinen Bezug von Arbeitslosenhilfe oder Arbeitslosengeld sowie die dem zugrundliegenden tatsächlichen Umstände.

Mir ist bekannt, daß eine abschließende Prüfung meines Einbürgerungsantrages ohne die Information dieser Stellen nicht möglich ist und ich die erforderlichen Unterlagen bei Verweigerung der Einwilligung selbst beizubringen habe."

Das SMI hat diese Anregungen vollständig übernommen und die Einbürgerungsbehörden entsprechend unterrichtet.

6 Finanzen

6.1 Bereichsspezifischer Datenschutz in der Abgabenordnung: Kontrollkompetenz des Datenschutzbeauftragten bei Finanzbehörden

Die Datenschutzbeauftragten des Bundes und der Länder stimmen überein, daß in der Abgabenordnung bereichsspezifische Regelungen zum Umgang mit personenbezogenen Daten erforderlich sind. Den Katalog der datenschutzrechtlichen Forderungen habe ich dem SMF mit der Bitte um Unterstützung auf Bundesebene übersandt.

Bei einer Sitzung der Referatsleiter 'Abgabenordnung' des Bundes und der Länder im Dezember 1996 kristallisierte sich bedauerlicherweise heraus, daß seitens der Finanzministerien die Bereitschaft, die Abgabenordnung gemäß den Vorgaben des Bundesverfassungsgerichts (BVerfGE 65, 1 ff.) um bereichsspezifische Datenschutzbestimmungen zu ergänzen, auf Null gesunken ist.

Meine bisher gezeigte Zurückhaltung, in der immer noch nicht abgeschlossenen Aufbauphase das SMF mit notwendigen, aber möglicherweise die Steuerverwaltung zur Zeit noch hemmenden Forderungen zu überziehen, gerät ins Wanken, wenn die AO-Referenten wie folgt argumentieren:

- Hinter der Forderung nach einheitlicher Terminologie stecke doch nicht nur der Wunsch der Datenschutzbeauftragten, Datenschutzbegriffe wie Erheben, Speichern, Übermitteln und Löschen in die Abgabenordnung einzuführen, vielmehr wollten die Datenschützer ein Einfallstor für eine stärkere Einengung und damit Behinderung der Datenverarbeitung im Besteuerungsverfahren erreichen;
- wenn etwas in der Abgabenordnung nicht geregelt sei, hieße das doch nicht, daß es verboten wäre (Vorbehalt des Gesetzes?);
- wenn sich ein Sachverhalt änderte - etwa die Automation der Besteuerungsverfahren - so brauche nicht gleich das Gesetz geändert zu werden;
- die Forderung, durch gesetzliche Regelungen mehr Transparenz für den Steuerpflichtigen zu schaffen, gehe ins Leere, da die Bürger das Gesetz sowieso nicht läsen;
- das Bundesverfassungsgericht habe den ausreichenden Datenschutz in der Abgabenordnung bis jetzt bestätigt, erst wenn von ihm eine Verletzung des Datenschutzes festgestellt sei, müsse die Abgabenordnung geändert werden;
- alle Vorschläge, die zu datenschutzrechtlichen Verbesserungen der Abgabenordnung gemacht würden, seien bereits in der Abgabenordnung enthalten bzw. alle damit verbundenen Fragen könnten schon jetzt gelöst werden.

Äußerungen dieser Art sind im Hinblick auf die verbindlichen (!), vom Bundesverfassungsgericht im Volkszählungsurteil aufgestellten Grundsätze (BVerfGE 65, 1 ff.) nicht sonderlich geeignet, dem Grundrecht auf informationelle Selbstbestimmung, das auch einem Steuerpflichtigen zusteht, zu dienen.

Auch die vereinzelten Äußerungen, mit denen dem Datenschutzbeauftragten die Kontrollkompetenz bei den Finanzbehörden streitig gemacht wird, sind diesem Grundrecht nicht förderlich und ignorieren nicht nur Art. 57 der Sächsischen Verfassung, sondern auch § 24 SächsDSG. Dort heißt es nämlich, daß der Datenschutzbeauftragte das Grundrecht auf informationelle Selbstbestimmung (insgesamt und auf allen Gebieten der öffentlichen Verwaltung) schützt und nicht nur die Einhaltung des SächsDSG kontrolliert, vielmehr auch die Einhaltung *anderer Vorschriften über den Datenschutz* (z. B. der AO - Steuergeheimnis). Außerdem erstreckt sich seine Kontrolle auch auf personenbezogene Daten, die einem Berufs- oder besonderen Amtsgeheimnis (z. B. § 30 AO - Steuergeheimnis) unterliegen. Eine Einschränkung der Kontrollkompetenz hat der Gesetzgeber, aus Gründen der Gewaltenteilung und der Unabhängigkeit, ausschließlich für die Gerichte vorgesehen (§ 24 Abs. 2 SächsDSG).

Wegen dieser eindeutigen Rechtslage wäre es schade, wenn das bisher doch kooperative Verhältnis zum SMF durch unnötiges Kompetenzgerangel in Mitleidenschaft gezogen würde.

6.2 Werbungskosten für Auslandsstudienreisen - Aufforderung des Finanzamtes an den Steuerpflichtigen, Namen und Anschriften der Mitreisenden mitzuteilen

Eine Steuerpflichtige, die eine Auslandsstudienreise bei den Werbungskosten absetzen wollte, erhielt vom Finanzamt die Aufforderung, die Namen und Anschriften der übrigen Reiseteilnehmer nachzureichen. Ganz abgesehen davon, daß die Betroffene keine Aufzeichnungen über die Mitreisenden geführt hatte, hatte sie auch Zweifel an der Rechtmäßigkeit eines solchen Verlangens.

Meinen Ermittlungen zufolge beruhte die Aufforderung auf einer entsprechenden Weisung der OFD, in der den Finanzämtern u. a. unter Hinweis auf Abschnitt 35 LStR 1996 als unerläßlich aufgegeben wurde, vor der Entscheidung über die steuerliche Abzugsfähigkeit insbesondere das Reiseprogramm anzufordern und auch die Namen und Anschriften der übrigen Reiseteilnehmer zu ermitteln. Tatsächlich sollen die Namen und Anschriften dazu dienen, zur Wahrung der steuerlichen Gerechtigkeit den für die Mitreisenden zuständigen Finanzämtern die getroffene Entscheidung (Werbungskosten anerkannt oder nicht) vorsorglich für den Fall mitzuteilen, daß dort ein entsprechender Antrag gestellt wird.

Abschnitt 35 LStR 1996 enthält einen Kriterienkatalog, wonach u. a. ein "homogener Teilnehmerkreis" für die Anerkennung solcher Aufwendungen als Werbungskosten spricht. Dem SMF, das ich um Stellungnahme zur Rechtmäßigkeit solcher Datenerhebungen bei Dritten bzw. über Dritte bat, teilte ich mit, daß die Nennung von Namen und Anschriften der Mitreisenden keineswegs als Indiz für einen "homogenen Teilnehmerkreis" gewertet werden könne. Um einen Teilnehmerkreis als "homogen" einschätzen zu können, genügen vielmehr berufsbezogene Angaben wie z. B. "Lehrer",

"Zahnärzte", "Chemiker", "Steuerberater", "Biologen".

Nicht überzeugt hat mich daher der Versuch des SMF, die Datenerhebung (über Dritte bzw. bei Dritten) mit §§ 90, 93 AO zu rechtfertigen. Zwar haben die (am konkreten Besteuerungsverfahren) Beteiligten und unter den engen Voraussetzungen des § 93 Abs. 1 Satz 3 AO auch andere Personen (dies sind gemäß § 78 AO keinesfalls die bislang unbekannten Mitreisenden) die zur Feststellung eines für die Besteuerung erheblichen Sachverhalts erforderlichen Auskünfte nach § 93 Abs. 1 AO zu erteilen; jedoch darf dies nicht zur Ermittlung unbekannter potentieller Steuerpflichtiger führen, von denen bislang ungewiß ist, ob sie überhaupt Werbungskosten für die Studienreise geltend zu machen beabsichtigen.

Immerhin hat der Dialog mit dem SMF inzwischen - wenn auch aus meiner Sicht unbefriedigend - zur Unterrichtung der Finanzämter geführt, daß die Namen und Anschriften der übrigen Reiseteilnehmer nunmehr unmittelbar vom Reiseveranstalter (also nicht mehr beim Steuerpflichtigen selbst) unter Hinweis auf dessen Auskunftspflicht gemäß § 93 AO angefordert werden können (Reiseveranstalter können z. B. sein: Bildungseinrichtungen, Berufskammern und -verbände, Gewerkschaften). Das SMF stützt sich dabei auf das BFH-Urteil vom 22.4.1986, Az.: VII R 127/82, das sich allerdings nicht mit der Frage der Zulässigkeit einer Datenerhebung nach § 93 Abs. 1 Satz 3 AO befaßt, sondern ausschließlich mit der *Höhe des Streitwertes,* falls der Reiseveranstalter die Bekanntgabe von Namen und Anschriften der Reiseteilnehmer verweigert. Aus diesem Urteil schließen zu wollen, daß die von mir problematisierte Datenerhebung nach § 93 Abs. 1 AO zulässig sei, bedarf schon einiger Phantasie.

Meine im Gegensatz zum SMF vertretene Auffassung, nämlich daß § 93 Abs. 1 AO die Datenerhebung über Namen und Anschriften der (übrigen) Reiseteilnehmer (die mit dem konkreten Besteuerungsverfahren nicht das geringste zu tun haben) weder beim Steuerpflichtigen selbst noch beim Reiseveranstalter rechtfertigt, erfordert einen weiteren Dialog. Läßt sich nämlich bereits die Erhebung von Namen und Anschriften der Mitreisenden mit § 93 Abs. 1 AO nicht vereinbaren, wären Kontrollmitteilungen an deren Finanzämter erst recht unzulässig.

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

Im 4. Tätigkeitsbericht (6.2) habe ich auf eine denkbare Kollision einer Auftragsvergabe durch die Finanzbehörden an den e-Postdienst mit dem Steuergeheimnis (§ 30 AO) sowie auf Sicherheitsdefizite im e-Mailverfahren hingewiesen. Vom SMF habe ich mittlerweile erfahren, daß die Referatsleiter 'Abgabenordnung' der obersten Finanzbehörden des Bundes und der Länder einer Auftragsvergabe an den e-Postdienst im Hinblick auf das Steuergeheimnis ablehnend gegenüberstehen.

Diese Haltung begrüße ich, weil bei der Verwendung von e-Mail die Vertraulichkeit, Integrität und die Verfügbarkeit der Daten nicht gewährleistet sind, da sie auf ihrem Weg durch das Netz mitgeschnitten, verfälscht und abgefangen werden können. Für mich ist es immer wieder unverständlich, wie wenig Sensibilität die Deutsche Post AG im Umgang mit personenbezogenen Daten (z. B. mit solchen Angeboten) entwickelt.

6.4 Datenschutzrechtliche Einordnung der Arbeitsgemeinschaft "Kammerleitstelle für Bemessungsgrundlagen" e. V. (AKG)

Zwischen der Finanzverwaltung des Freistaates Sachsen und den sächsischen Industrie- und Handelskammern und den Handwerkskammern besteht - wie in den anderen Bundesländern - eine Vereinbarung, daß mit der Berechnung der Kammerbeiträge die AKG beauftragt wird. Hierzu ist es erforderlich, Besteuerungsgrundlagen, die dem Steuergeheimnis (§ 30 AO) unterliegen, zur Beitragsbemessung der AKG zur Verfügung zu stellen. Nach § 31 Abs. 1 AO sind die Finanzbehörden berechtigt, Besteuerungsgrundlagen, Steuermeßbeträge und Steuerbeträge an die *Kammern* zur Festsetzung von Abgaben mitzuteilen, die an diese Besteuerungsgrundlagen, Steuermeßbeträge oder Steuerbeträge anknüpfen. Datenschutzrechtlich war zu prüfen, ob die Mitteilung über steuerrelevante Angaben an die privat organisierte AKG zulässig ist.

Dem SMF und dem SMWA habe ich nach eingehender Würdigung der mir zur Verfügung gestellten Vereinbarungen mitgeteilt, daß die AKG datenschutzrechtlich als Auftragnehmer i. S. v. § 7 SächsDSG einzuordnen ist.

Die vorgesehenen personellen, technischen und organisatorischen Maßnahmen (z. B. Verpflichtung des AKG-Personals nach dem Verpflichtungsgesetz und auf das Datengeheimnis, Musteranweisung mit ausführlichen Regelungen zu Datenschutz und Datensicherungsfragen für Leitstellen) entsprechen im Hinblick auf bereits durchgeführte Datenschutzkontrollen durch die Bezirksregierung Arnsberg und die Landesbeauftragte für den Datenschutz Nordrhein-Westfalen den datenschutzrechtlichen Anforderungen.

Klärungsbedürftig bleibt jedoch nach wie vor, wem die datenschutzrechtliche Kontrollkompetenz für die von den sächsischen Kammern und Finanzbehörden an die AKG gelieferten Daten obliegen soll. Nach meinem Dafürhalten müßte sich die AKG bezüglich der sächsischen Daten vertraglich meiner Kontrollkompetenz unterwerfen (desgleichen bezüglich der anderen Länderdaten den dortigen Datenschutzbeauftragten). Eine entsprechende Ergänzung der Vereinbarungen habe ich angeregt.

6.5 Fördermitteldatenbank und Fördermittelverwaltung

Seit Jahren ist die Staatsregierung bemüht, ein einheitliches Konzept für die Fördermittelverwaltung zu erarbeiten. Ziel soll es dabei u. a. sein, unzulässige Doppelförderungen aufzudecken, aber auch die Staatsregierung durch Recherchemöglichkeiten mit aktuellen Informationen für die Fördermittelpolitik zu versorgen.

Wie schwierig das Unterfangen offenbar ist, zeigt sich an den wiederholten Wechseln der Federführung der Projekte. Das ursprünglich verantwortliche SMI hat die Verantwortung ans SMF abgeben. Im Jahre 1996 wechselte die Verantwortung schließlich zur Staatskanzlei, wo nunmehr an zwei Projekten, nämlich an der Schaffung der Voraussetzungen für eine "landeseinheitliche Fördermitteldatenbank" als Informationsinstrument für die Staatsregierung sowie an der Entwicklung einer "einheitlichen Fördermittelverwaltung" für die mit der Fördermittelvergabe zuständigen Behörden gearbeitet wird.

Zuletzt habe ich zu beiden Projekten mit der Bitte um weitere Beteiligung wie folgt Stellung genommen:

1. Landeseinheitliche Fördermitteldatenbank

Der Arbeitsgruppe Landeseinheitliche Fördermitteldatenbank wurde am 15. Dezember 1996 das Modell für eine Datenbank übergeben, das die Randbedingungen und den Abdeckungsgrad bezüglich der Rechercheanforderungen sowie einen Vorschlag für eine erste Realisierungsetappe enthalten soll. Sollte daran gedacht sein, den recherchierenden Stellen (Ressorts) personenbezogene (also nicht aggregierte) Fördermitteldaten zur Verfügung zu stellen, so erinnere ich an den bereits früher gegebenen Hinweis, hierfür eine gesetzliche Grundlage zu schaffen (Art. 33 SächsVerf), die den Grundsätzen des Volkszählungsurteils vom 15. Dezember 1983 (BVerfGE 65, 1, 42-44) entsprechen muß. § 44 SHO dürfte jedenfalls nicht ausreichen.

Einer kürzlich eingegangenen Mitteilung der SK zufolge ist die Schaffung einer gesetzlichen Grundlage, an deren Vorbereitung man mich zu beteiligen beabsichtigt, vorgesehen.

2. Einheitliche Fördermittelverwaltung

Im Protokoll des Arbeitskreises Informationstechnik vom 5. Dezember 1996 ist u. a. nachzulesen, daß für die "Einheitliche Fördermittelverwaltung" ein erster optimistischer, noch nicht abgestimmter Projektplan vorgestellt worden sei. Jedoch seien die Arbeiten zur Detaillierung des funktionalen Grobablaufplans zugunsten der Strukturierungsarbeiten für die Landeseinheitliche Fördermitteldatenbank (siehe oben) zurückgestellt worden.

Gleichwohl gebe ich im Hinblick auf die weitere Entwicklung zu bedenken, daß die Fördermittelvergabe stets auch eine Verarbeitung personenbezogener Daten der Antragsteller und damit einen Eingriff in deren Recht auf informationelle Selbstbestimmung mit sich bringt. Beschränkungen dieses Grundrechts bedürfen, dem Volkszählungsurteil (a.a.O. S. 42-46) entsprechend, einer (verfassungsmäßigen) gesetzlichen Grundlage, aus der sich die Voraussetzungen und der Umfang der Beschränkungen klar und für den Antragsteller erkennbar ergeben und die damit dem rechtsstaatlichen Gebot der Normenklarheit entspricht (BVerfGE 45, 400, 420 m.w.N.), wobei der Grundsatz der Verhältnismäßigkeit zu beachten ist. § 44 SHO dürfte (für sich gesehen) als solche Rechtsgrundlage nicht ausreichend sein. Ob auf die Auffangvorschriften des Sächsischen Datenschutzgesetzes (hier: §§ 11 f.) zurückgegriffen werden kann, hängt von der durch die automatisierte Fördermittelverwaltung bedingten Tiefe des Eingriffs in das Grundrecht auf informationelle Selbstbestimmung ab.

An der Entwicklung werde ich mich weiterhin beteiligen.

6.6 Veröffentlichung personenbezogener Daten bei Verurteilungen und strafbewehrten Unterlassungserklärungen in der Mitteilungsschrift der Steuerberaterkammer des Freistaates Sachsen

Vom Berliner Datenschutzbeauftragten wurde ich informiert, daß die Steuerberaterkammer Berlin in ihrer Mitteilungsschrift regelmäßig personenbezogene Daten von Personen veröffentlicht, gegen die die Steuerberaterkammer wegen unerlaubter Hilfe in Steuersachen einschließlich sog. Überschußwerbung rechtlich vorgegangen ist. Bei seiner Überprüfung der Rechtmäßigkeit dieser Vorgehensweise wurde meinem Berliner Kollegen mitgeteilt, daß sich die Vertreter der obersten Finanzbehörden des Bundes und der Länder bereits mit diesem Thema befaßt und die Veröffentlichungen „in Anlehnung an § 23 Abs. 2 UWG“ für zulässig erachtet hätten. Dabei wurde offensichtlich verkannt, daß die in § 23 Abs. 2 UWG vorgesehene Veröffentlichung bei Wettbewerbsverstößen ausschließlich von einem Gericht - also nicht von der Steuerberaterkammer - angeordnet werden kann.

Meinen Feststellungen zufolge wird in Sachsen ebenso verfahren wie in Berlin. Deshalb habe ich die für die Steuerberaterkammer des Freistaates Sachsen zuständige Aufsichtsbehörde - das SMF - über die vom Arbeitskreis Steuerverwaltung der Datenschutzbeauftragten des Bundes und der Länder vertretene Rechtsauffassung informiert, daß sich Veröffentlichungen der o. a. Art jedenfalls nicht auf § 23 Abs. 2 UWG stützen lassen. Eine legitimierende Rechtsgrundlage existiert nicht. Eine Veröffentlichung mit Einwilligung gemäß § 4 Abs. 1 Nr. 2 und Abs. 2 und 3 SächsDSG erscheint mir im Hinblick auf die mit der Veröffentlichung einhergehende Prangerwirkung nicht realistisch möglich zu sein. Die unzulässigen Veröffentlichungen verstoßen also gegen § 83 Abs. 1 StBerG, § 203 Abs. 2 StGB, § 32 SächsDSG.

Bei allem Verständnis für Bestrebungen, einen Berufsstand von „schwarzen Schafen“ freizuhalten: Ohne legitimierende bundeseinheitliche Rechtsnorm muß künftig auf diese Veröffentlichungen verzichtet werden.

Merke: Nicht alles, was vernünftig erscheint oder von vielen gewünscht wird, ist gestattet. Wir müssen uns daran gewöhnen, daß eine Rechtsgrundlage für jeden amtlichen Umgang mit Daten nötig ist.

Die Steuerberaterkammer für den Freistaat Sachsen habe ich gebeten, bis zu einer erforderlichen bundesweiten Klärung auf entsprechende Veröffentlichungen zu verzichten.

Das SMF hat seine Bereitschaft zu erkennen gegeben, die Problematik auf der nächsten Berufsreferentensitzung im Mai 1997 mit den Vertretern der obersten Finanzbehörden des Bundes und der Länder erneut zu erörtern.

7 Kultus

7.1 Aufnahmeverfahren zum Besuch von Förderschulen

Die Förderschulordnung regelt detailliert das Verfahren zur Aufnahme von Schülern an Förderschulen (§ 12 SOFS). Sie ist im Mai 1996 in Kraft getreten und enthält gegenüber dem bis dahin praktizierten, durch Rechtsvorschriften nicht näher geregelten Verfahren wesentliche Neuerungen für das Zusammenwirken der Beteiligten (Schulaufsichtsbehörde, Regelschule, Förderschule, Amts- und Fachärzte, psychologische Gutachter, Sorgeberechtigte). Jetzt ist die Schulaufsichtsbehörde "Herr des Aufnahmeverfahrens", sie hat die vorgeschriebenen Gutachten einzuholen, Klassenlehrer und Schulleiter zu beteiligen, die Sorgeberechtigten anzuhören usw.

Bisher verwendete Vordrucke müssen nun an das neue Verfahren angepaßt werden, insbesondere die im Mittelpunkt des Aufnahmeverfahrens stehende 18seitige "Pädagogisch-psychologische-medizinische Dokumentation" (Aufnahmedokumentation). Mit ihr hatten die Schulen im alten Aufnahmeverfahren die Daten über Schüler mit einem vermuteten Förderbedarf zuammenzutragen und der Schulaufsichtsbehörde zur Entscheidung vorzulegen. Das SMK hat mich in die Überarbeitung der Aufnahmedokumentation einbezogen. Ich habe an den Arbeitsgruppensitzungen des SMK mit den Vertretern der nachgeordneten Schulaufsichtsbehörden und den Förderschulen beratend teilgenommen. Da sich eine kompetente datenschutzrechtliche Beratung nicht in der Frage erschöpft, ob die in einem Vordruck vorgesehenen Angaben erforderlich sind oder nicht, sondern auch das Verfahren betrachtet, in das ein Vordruck eingebunden ist, habe ich auch eine strukturelle Überarbeitung angeregt, nämlich die Entfernung ganzer Teile und die Aufteilung des Gesamtvordrucks in Einzelvordrucke. Dadurch wird sichergestellt, daß Datenerhebungen und -übermittlungen den in der Förderschulordnung vorgegebenen Phasen des Aufnahmeverfahrens entsprechen und keine unzulässigen Datenerhebungen und -übermittlungen erfolgen.

Die Aufgabe ist noch nicht abgeschlossen. Derzeit liegt der Entwurf eines Vordrucksatzes vor, der noch neun Blätter umfaßt und noch einmal mit den Praktikern diskutiert werden muß. Ich habe dringend geraten, zu diesen Vordrucken eine erläuternde Verwaltungsvorschrift zu erlassen.

7.2 Datenschutz bei Ordnungsmaßnahmen gegen Schüler

Gemäß § 39 SchulG können nach dem Grundsatz der Verhältnismäßigkeit Erziehungs- und Ordnungsmaßnahmen gegenüber einem Schüler getroffen werden - vom schriftlichen Verweis durch den Klassenlehrer bis zum Ausschluß aus der Schule. Vor der Entscheidung ist der Schüler anzuhören. Ist er minderjährig, ist auch die Anhörung der Erziehungsberechtigten vorgeschrieben. Das Schulgesetz ermächtigt das SMK, Einzelheiten in einer Rechtsverordnung zu regeln. Warum eine solche Rechtsverordnung bisher nicht erlassen worden ist, ist mir unbekannt.

Eine Schule hat mich um Auskunft gebeten, ob Ordnungsmaßnahmen gegen Schüler in Konferenzen und auf Elternabenden behandelt werden dürfen und ob sie der Schulaufsichtsbehörde mitzuteilen sind. Ich habe mich dazu folgendermaßen geäußert:

Nur die Schule, der Schüler und ggf. seine Erziehungsberechtigten sind nach § 39 SchulG an dem Verfahren beteiligt; Dritte geht eine beabsichtigte oder getroffene Ordnungsmaßnahme folglich nichts an. Der Begriff "Schule" wird in der noch zu erlassenden Rechtsverordnung zu konkretisieren sein. Auch die Frage, ob es erforderlich ist, die Schulaufsichtsbehörde über Ordnungsmaßnahmen zu informieren, muß in diesem Zusammenhang diskutiert werden.

Gegen eine Beratung solcher Fälle in Klassenkonferenzen, an denen außer den unterrichtenden Lehrern und dem Schulleiter keine Dritten teilnehmen, ist datenschutzrechtlich nichts einzuwenden, wenn ein Meinungs- und Informationsaustausch zwischen allen den betroffenen Schüler unterrichtenden Lehrern aus pädagogischen Gründen erforderlich erscheint. Diskutiert werden muß auch, ob es zulässig und sinnvoll ist, in eindeutigen Fällen auch ein "Opfer", z. B. den durch eine massive Aggression geschädigten Mitschüler, bzw. dessen Eltern von der Ordnungsmaßnahme zu informieren, schon um ihnen die Angst vor einer weiteren Konfrontation zu nehmen. Eine Beratung auf Schul-, Gesamtlehrer- oder Fachkonferenzen verbietet sich deshalb, weil sie nach dem Schulgesetz bzw. den betreffenden Konferenzordnungen nicht zu den für diese Konferenzarten festgelegten Inhalten gehören. Unzulässig ist es auch, getroffene Maßnahmen vor der Klasse zu verkünden oder auf Elternabenden zu behandeln. Selbst wenn der Name des Schülers nicht genannt wird, kann der Personenbezug in diesem überschaubaren Kreis hergestellt werden.

7.3 Bekanntgabe des Zensurenspiegels und des Klassendurchschnitts

"Aus datenschutzrechtlichen Gründen" werden an einigen Schulen keine "Zensurenspiegel", also Statistiken über die Noten einer Klassenarbeit, mehr erstellt. Ein Vater bezweifelte diese angeblichen datenschutzrechtlichen Gründe: Ihn hatte die Antwort der Schule schon deswegen nicht überzeugt, weil er den Personenbezug bei Zensurenspiegeln nicht zu erkennen vermochte.

Statistiken über kleine Gruppen lassen oft Rückschlüsse auf bestimmte Personen zu, jedenfalls wenn die Gruppenmitglieder einander kennen oder gar - wie hier - einen wesentlichen Teil des Tages gemeinsam in der Schule verbringen. Gleichwohl gibt es aus datenschutzrechtlicher Sicht keine Bedenken gegen die Bekanntgabe des Zensurenspiegels, und keinesfalls darf "der Datenschutz" vorgeschoben werden, um den Lehrer einer Kenntnisnahme seiner Benotungspraxis durch Eltern und Schüler zu entziehen.

Für den Datenschutz an den öffentlichen Schulen in Sachsen gilt das Sächsische

Datenschutzgesetz. Bei der Bekanntgabe des Zensurenspiegels vor der Klasse handelt es sich um eine Übermittlung personenbezogener Daten an nicht-öffentliche Stellen (§ 15 SächsDSG). Die Datenübermittlung ist gemäß § 15 Abs. 1 Nr. 1 SächsDSG u. a. zulässig, wenn sie zur Aufgabenerfüllung der Schule erforderlich ist und die Zweckbindung der Daten eingehalten wird. Diese Voraussetzungen sind hier erfüllt:

Zensuren drücken aus, wieweit ein Schüler die Lernanforderungen erfüllt, lassen aber nur einen eingeschränkten Rückschluß auf seinen Leistungsstand innerhalb der Klasse zu. Da Eltern ein Informationsrecht gegenüber der Schule haben, das sich aus Art. 6 Abs. 2 GG und Art. 22 Abs. 3 SächsVerf ableitet, ist die Bekanntgabe des Zensurenspiegels ein geeignetes Mittel, ihnen den gewünschten Leistungsvergleich zu ermöglichen, weil der Zensurenspiegel die Erfüllung der Lernanforderungen aus einem anderen Blickwinkel beleuchtet. Auch wird die Zweckbindung der Noten eingehalten. Dies habe ich dem Vater mitgeteilt.

Erst recht bestehen keine Bedenken, den Klassendurchschnitt bekanntzugeben, wie es der Erlaß des SMK zur "Angabe des Klassendurchschnitts unter Klassenarbeiten" vorsieht. Ein *Notendurchschnitt* ist kein personenbezogenes Datum mehr, so daß sich die Zulässigkeit seiner Bekanntgabe nicht nach dem Sächsischen Datenschutzgesetz beurteilt.

7.4 Bekanntgabe personenbezogener Daten an Schülerpraktikanten

Erhalten Schüler im Rahmen eines Praktikums bei öffentlichen Stellen Kenntnis von personenbezogenen Daten, ist zu beachten, daß sie Dritte i. S. d. § 3 Abs. 4 SächsDSG sind. Hierauf habe ich das SMK hingewiesen. Der dem § 3 Abs. 4 SächsDSG zugrundeliegende funktionale (aufgabenbezogene) Stellenbegriff geht davon aus, daß im datenschutzrechtlichen Sinne eine andere Stelle und damit ein Dritter vorliegt, sobald die Daten nicht mehr für die ursprüngliche, sondern für eine andere Aufgabe verwendet werden sollen. Dies ist der Fall, wenn beispielsweise Sozial- oder Polizeibehörden personenbezogene Daten im Rahmen ihrer konkreten Aufgabenerfüllung erheben und dann an Praktikanten für schulische Ausbildungszwecke weiterleiten. Die Praktikanten sind weder in den Betrieb noch in die konkrete Aufgabenerfüllung der Praktikumsstelle eingebunden. Sie absolvieren das Praktikum vielmehr zu dem "schulischen Zweck", sich die spätere Berufswahl zu erleichtern und sind damit "Dritte" i. S. d. § 3 Abs. 4 SächsDSG - mit der Folge, daß Datenübermittlungen an Schüler - in Ermangelung eines Spezialgesetzes - nur unter den engen Voraussetzungen des § 15 SächsDSG (Übermittlung an nicht-öffentliche Stellen) zulässig sind.

Um den Schutz besonders sensibler Daten sicherzustellen, wurde mir vom SMK in diesem Zusammenhang zugesagt, bei einer Änderung der Verwaltungsvorschrift "Betriebspraktika" festzulegen, daß Schüler im Rahmen von Betriebspraktika nicht in sensiblen Bereichen (z. B. Polizei, Sozialbehörden, Personalreferaten) eingesetzt werden dürfen. Davon abgesehen seien die Schulräte auf die geschilderte Problematik

hingewiesen und dienstlich angewiesen worden, entsprechend zu verfahren.

7.5 Veröffentlichung von Abiturientenlisten in Tageszeitungen

Ein Vater beklagte sich darüber, daß in mehreren Tageszeitungen eine Liste mit Abiturienten, zu denen sein Sohn gehörte, veröffentlicht wurde, ohne daß die Schüler um Einwilligung gebeten worden sind.

Die Schulen dürfen Daten an eine nicht-öffentliche Stelle gemäß § 15 Abs. 1 Nr. 1 SächsDSG übermitteln, wenn sie für die Aufgabenerfüllung der Schule erforderlich sind. Weil diese Voraussetzung nicht erfüllt ist, kommt nur § 15 Abs. 1 Nr. 2 SächsDSG in Betracht. Danach ist die Übermittlung 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.

Der Zeitung wird man ein berechtigtes Interesse an der Veröffentlichung dieser Listen, die im lokalen Bereich auf großes Interesse der Leser stoßen werden, nicht absprechen können. Auch werden die meisten Abiturienten keine Einwände gegen die Veröffentlichung haben; sie werden sie im Gegenteil sehr begrüßen. Anderseits kann eine Veröffentlichung auch unwillkommen sein, beispielsweise weil der Schüler das Abitur nicht bestanden hat und demzufolge sein Name in der Liste fehlt oder sein Name erscheint, obwohl er bereits im vorhergehenden Jahr das Abitur hätte bestehen müssen. In diesen Fällen hätte er durchaus ein schutzwürdiges Interesse, nicht bloßgestellt zu werden.

Ziel des Datenschutzes ist es nicht, eine alte Tradition zu zerstören oder durch unangemessene bürokratische Hürden zu behindern. Es muß jedoch ein Weg gefunden werden, dem eindeutigen Wortlaut des Gesetzes Genüge zu tun. Ich habe daher das SMK um Vorschläge gebeten, wie berechtigten entgegenstehenden Interessen besser als bisher Rechnung getragen werden kann.

Das SMK hat mir geantwortet, die Oberschulämter seien bereits im Herbst 1995 darüber unterrichtet worden, daß eine Veröffentlichung der Listen nur zulässig ist, wenn die Schüler (und Eltern) informiert wurden und Gelegenheit zum Widerspruch bestand. Die Anhörung gemäß § 15 Abs. 3 SächsDSG zur Datenübermittlung ist aktenkundig zu machen. Eine schriftliche Einwilligung der Betroffenen wird empfohlen.

Das SMK sagte zu, die Oberschulämter erneut auf die Rechtslage hinzuweisen. Einem mir vorgelegten Entwurf einer Information für die Oberschulämter habe ich gern zugestimmt.

7.6 Überwachung der Schulpflicht

Die Erziehungsberechtigten sind dafür verantwortlich, daß ihre schulpflichtigen Kinder eine Schule besuchen (§ 13 Abs. 1 SchulG). Diese Schulpflicht kann auch durch den Besuch einer Schule in freier Trägerschaft erfüllt werden. Auf die Pflicht, ein schulpflichtig gewordenes Kind zum Schulbesuch anzumelden, weisen zu Beginn eines jeden Schuljahres die Zeitungen hin. In Sachsen können die Eltern nicht direkt angeschrieben werden, weil dies eine spezielle Auswertung des Einwohnermelderegisters voraussetzt und dafür die rechtlichen Voraussetzungen fehlen. So kann es geschehen, daß schulpflichtige Kinder nicht zum Schulbesuch angemeldet werden, ohne daß eine Behörde das merkt.

Der Erlaß des SMK vom 18. Juli 1996 sowie die Maßnahmen der Oberschulämter Dresden und Chemnitz zur Überwachung der Schulpflicht haben zu zahlreichen Problemen geführt. Es ist mir nicht gelungen, sie zu lösen, weil die vom SMK erbetenen Stellungnahmen erst nach Monaten eingegangen sind und nur ansatzweise Aufklärung gebracht haben. Auch meine Gesprächsangebote wurden ignoriert, so daß meine Bemühungen um Klärung des Sachverhalts, von Zusammenhängen und Hintergründen scheitern mußten.

Die Probleme im einzelnen:

1. *Mitteilungen der Schulen in freier Trägerschaft über die als Erstkläßler aufgenommenen Schüler*

   Mit dem o. a. Erlaß hat das SMK folgendes angeordnet: "Damit ein Nachweis über die Erfüllung der Schulpflicht an einer Schule in freier Trägerschaft gegeben ist, sollte die aufnehmende Schule die staatliche Grundschule diesbezüglich unterrichten."

   Ich habe diese Anweisung kritisiert, weil ich keine Rechtsvorschrift sehe, welche die Schulen in freier Trägerschaft verpflichtet, einen als Erstkläßler aufgenommenen Schüler der Grundschule zu melden, in deren Schulbezirk er wohnt. Hinzu kommt, daß der Umgang mit diesen Daten an der Grundschule, insbesondere Weitergabe und Löschung, unklar sind.

   Der Nachweis, daß die Schulverwaltung durch die Mitteilungen in die Lage versetzt würde, zu überwachen, daß alle Kinder ihrer Schulpflicht nachkommen, ist auch nicht ansatzweise geführt.

   Hierzu habe ich keine Stellungnahme erhalten.

2. *Feststellung der Schulfähigkeit durch Grundschulleiter für Schüler, die eine Schule in freier Trägerschaft besuchen wollen*

Der o. a. Erlaß ordnet außerdem an, daß die Feststellung der Schulfähigkeit in der Grundschule des Wohnbezirks zu erfolgen hat, weil nach Auffassung des SMK der Leiter dieser Grundschule gemäß § 3 Abs. 4 SchulG darüber zu entscheiden hat, ob ein Kind die Voraussetzungen für den Besuch der vorgesehenen Ersatzschule erfüllt. Ich habe bezweifelt, daß die Grundschule die "richtige" datenverarbeitende Stelle ist, insbesondere deshalb, weil die sich an die Entscheidung des Grundschulleiters anschließende Datenverarbeitung nicht geregelt ist. Systemgerecht wäre es in meinen Augen, wenn der Leiter der Ersatzschule die Entscheidung auf der Grundlage der schulärztlichen Untersuchung zu treffen hätte. Dem steht das Argument entgegegen, daß er keinen Verwaltungsakt erlassen kann.

Möglicherweise besteht eine Regelungslücke: § 3 Abs. 1 SchulG besagt, daß für Schulen in freier Trägerschaft das Schulgesetz nur Anwendung findet, soweit dies ausdrücklich bestimmt ist, und daß im übrigen das Gesetz über die Schulen in freier Trägerschaft gilt. Das Schulgesetz regelt in § 26 Abs. 2 zwar ausdrücklich, daß die Schulpflicht auch durch den Besuch einer Schule in freier Trägerschaft erfüllt wird, nicht aber ausdrücklich, daß die Entscheidung über die Schulfähigkeit in diesem Falle beim Grundschulleiter liegt (s. § 27 Abs. 4 SchulG). Auch anhand des Gesetzes über die Schulen in freier Trägerschaft läßt sich diese Frage nicht eindeutig klären, denn es besagt - in § 4 Abs. 3 Satz 2 SächsFrTrSchulG - lediglich, daß die für die Schulpflicht geltenden Bestimmungen (§§ 26 bis 31 SchulG) zu *beachten* sind.

Dies ist keine normenklare Regelung. Die in § 19 Nr. 4 SächsFrTrSchulG vorgesehene Rechtsverordnung könnte Klarheit schaffen. Denkbar wäre auch eine Klarstellung im Schulgesetz oder im Gesetz über Schulen in freier Trägerschaft.

Zu dieser Problematik sowie zur Klärung von Fragen, die mit der datenschutzrechtlichen Praxis im derzeitigen Verfahren zusammenhängen, habe ich um ein Gespräch gebeten. Die Bitte ist unbeantwortet geblieben.

3. *Anforderung von Schülerlisten durch Schulämter und Oberschulämter bei den Schulen in freier Trägerschaft*

Zumindest die Oberschulämter Chemnitz und Dresden haben die Schulen in freier Trägerschaft aufgefordert, zu Beginn eines jeden Schuljahres Namenslisten aller Schüler zu übergeben. Mehrere Schulen in freier Trägerschaft haben darin eine Verletzung des Persönlichkeitsrechts ihrer Schüler gesehen und sich an mich gewandt.

Die Anforderung der Schülerlisten wurde vom Oberschulamt Dresden damit begründet, die Listen dienten der Schulpflichtüberwachung, sowohl in Einzelfällen als auch zur Vorbereitung einer sachsenweiten Schulpflichtüberwachung. Diese Begründung habe ich nicht akzeptiert, weil mit derartigen Listen keine Schulpflichtüberwachung möglich ist und die Listen deshalb nicht erforderlich sein

können, und zwar aus folgenden Gründen:

Eine sachsenweite Schulpflichtüberwachung ist nur denkbar, wenn zu einem Stichtag die Namen aller schulpflichtigen Kinder (Soll-Bestand) mit allen tatsächlich eine Schule besuchenden Kindern (Ist-Bestand) abgeglichen würden, und zwar unabhängig davon, ob es sich um Regelschüler, Förderschüler oder Schüler einer Schule in privater Trägerschaft handelt. Außerdem müßten die vom Schulbesuch zurückgestellten Kinder einbezogen werden. Für einen solchen Abgleich fehlen zur Zeit die gesetzlichen Grundlagen, so daß das angestrebte Ziel allein mit Schülerlisten nicht erreicht werden kann. Sollte der Gesetzgeber es für nötig halten, die Erfüllung der Schulpflicht zu überwachen, so werde ich eine gesetzliche Regelung gerne beratend begleiten.

Als Antwort habe ich eine Stellungnahme erhalten, die sich mit der Aufsichtsbefugnis von Schulaufsichtsbehörden gegenüber Schulen in freier Trägerschaft befaßt. Das war hier ersichtlich nicht das Problem. Ob das SMK etwas veranlaßt hat, damit allen Schulen in freier Trägerschaft die Schülerlisten zurückgegeben werden, hat es mir nicht mitgeteilt. Das Oberschulamt Dresden hat zumindest seine diesbezügliche Absicht bekundet. Von Betroffenen habe ich erfahren, daß Schülerlisten zurückgegeben worden seien.

4. *Anmeldung an der Grundschule, bevor ein Kind eine Schule in freier Trägerschaft besuchen darf*

Ein Oberschulamt hat den Erlaß des SMK vom 18. Juli 1996 so aufgefaßt, daß Schulen in freier Trägerschaft Erstkläßler erst dann aufnehmen dürfen, wenn sie zuvor an der Grundschule des Wohnbezirks *angemeldet* wurden. Dies wurde den Schulen in freier Trägerschaft mitgeteilt. Möglicherweise verfügen Grundschulen nun über Anmeldedaten von Schülern, die eine Schule in freier Trägerschaft besuchen. Abgesehen davon, daß ein Schüler nicht zugleich an zwei Schulen angemeldet sein kann, ist die Speicherung dieser Daten unzulässig, weil sie für die Aufgabenerfüllung der Grundschule nicht erforderlich sind.

Auch zu diesem Problem war vom SMK keine Stellungnahme zu erhalten.

8 Justiz

8.1 Referentenentwurf zur Änderung des Strafvollzugsgesetzes

In meinem 4. Tätigkeitsbericht (8.2.1) habe ich kritisiert, daß es im Bereich des Strafvollzuges an bereichsspezifischen Rechtsgrundlagen für die Verarbeitung personenbezogener Daten fehlt. Das Strafvollzugsgesetz in seiner jetzigen Fassung gibt mit seinen Generalklauseln lediglich vage Zulässigkeitskriterien vor, ohne Art und Umfang der Datenverarbeitung klar und für den Einzelnen erkennbar zu umreißen. Dieses Defizit soll nun durch eine Ergänzung des Strafvollzugsgesetzes ausgeglichen werden. Zum "Vorläufigen Referentenentwurf eines Vierten Gesetzes zur Änderung des Strafvollzugsgesetzes" (Stand 10. April 1996) habe ich gegenüber dem SMJus Stellung genommen.

Zu begrüßen ist, daß die Regelung des § 29 Abs. 2 Strafvollzugsgesetz, wonach Schreiben von Gefangenen an Volksvertretungen des Bundes und der Länder sowie an deren Mitglieder nicht überwacht werden, nach dem Referentenentwurf auch auf Schreiben, die an Datenschutzbeauftragte gerichtet sind, ausgedehnt werden soll. In diesem Zusammenhang habe ich angeregt, auch den Briefverkehr *von* diesen Stellen an Gefangene nicht zu überwachen. Die Briefüberwachung belastet die - für die Resozialisierung dringend notwendige - Kommunikation des Gefangenen mit der Außenwelt. Deshalb ist besonders sorgfältig zu prüfen, ob die Voraussetzungen einer Überwachung, nämlich Gründe der Behandlung oder Sicherheit oder Ordnung (§ 29 Abs. 3 StVollzG), vorliegen. Weil diese Voraussetzungen bei Behördenbriefen wohl in aller Regel nicht gegeben sind, habe ich vorgeschlagen, Behördenpost von einer Briefkontrolle auszuschließen. Sichergestellt werden muß bei diesen Briefen nur, daß sie auch tatsächlich vom Absender stammen. Dies kann in den meisten Fällen durch Absprachen mit den in § 29 Abs. 2 des Referentenentwurfs genannten Behörden zumutbar gewährleistet werden. Wie ich bereits in meinem 4. Tätigkeitsbericht (8.2.5) ausgeführt habe, wird im Freistaat Sachsen beim Postverkehr meiner Behörde mit Gefangenen bereits entsprechend verfahren. Danach werden meine Schreiben an Gefangene nicht überwacht, wenn ich um eine ungeöffnete Weiterleitung bitte. Meine Anregung, dies im Strafvollzugsgesetz zu regeln, hat das SMJus in das Gesetzgebungsverfahren eingebracht.

Eine datenschutzrechtliche Verbesserung sehe ich auch darin, daß künftig die Gefangenen nicht nur bei Haftantritt, sondern auch bei ihrer Entlassung ausdrücklich darüber belehrt werden müssen, daß sie die Vernichtung ihrer erkennungsdienstlichen Unterlagen verlangen können. In Sachsen wird allerdings bereits jetzt so verfahren (vgl. 4. Tätigkeitsbericht unter 8.2.2). In diesem Zusammenhang stellt sich jedoch die Frage, warum die Vernichtung der Lichtbilder vom Antrag des Gefangenen abhängig sein soll: Weil es nach § 86 Abs. 3 Satz 2 StVollzG der Gefangene bereits jetzt in der Hand hat, zu bestimmen, daß die erkennungsdienstlichen Unterlagen vernichtet werden, kommt als Aufbewahrungsgrund die Aufgabenerfüllung der JVA nicht in Betracht. Ich habe deshalb das SMJus gebeten, sich dafür einzusetzen, daß die

Lichtbilder generell - auch ohne Antrag des Gefangenen - nach seiner Entlassung vernichtet werden; ich vermute, daß mein Vorschlag dort aufgegriffen wird.

Schließlich habe ich das SMJus gebeten, sich für eine Regelung einzusetzen, wonach personenbezogene Daten auch innerhalb einer Anstalt nur weitergegeben werden dürfen, "soweit dies zur Erfüllung der den Vollzugsbediensteten jeweils obliegenden Aufgaben erforderlich ist". Nach dem Text des Referentenentwurfs dürften Daten innerhalb der Justizvollzugsanstalt schon dann übermittelt werden, "wenn dies für ein geordnetes Zusammenleben in der Anstalt erforderlich ist". Eine solche vage und den konkreten Verwendungszweck offen lassende Formulierung könnte den falschen Eindruck erwecken, daß Daten, die zu Vollzugszwecken einmal rechtmäßig erhoben wurden, anschließend anstaltsintern frei verfügbar sind. Bereits in meinem 4. Tätigkeitsbericht (8.2.1) habe ich eine differenzierte Regelung des Zugangs zu den personenbezogenen Daten der Gefangenen gefordert. Auch diese Empfehlung hat das SMJus im Gesetzgebungsverfahren eingebracht.

8.2 Entwurf eines Gesetzes zum Schutz kindlicher Zeugen

Ziel eines Gesetzentwurfes des Bundesrates ist es, die psychischen Belastungen zu vermindern, denen ein Kind, das Opfer einer Straftat wurde, durch eine Vernehmung als Zeuge in der Hauptverhandlung ausgesetzt ist. Das soll dadurch erreicht werden, daß seine Vernehmung außerhalb des Sitzungssaales - in „vertraulicher Atmosphäre“ - stattfindet und über Video direkt in den Gerichtssaal übertragen wird. Anlaß für diesen Gesetzentwurf waren Strafprozesse u. a. in Mainz wegen sexuellen Mißbrauchs von Kindern. Den Kindern soll ein erneute Konfrontation mit dem Täter erspart bleiben.
Der Entwurf berührt intensiv das Persönlichkeitsrecht und wirft strafprozessuale Probleme auf, die kaum lösbar sind.
Schwerpunkt meiner Kritik ist, daß der Entwurf den Versuch unternimmt, den im Strafprozeß geltenden Grundsatz der Unmittelbarkeit zu durchbrechen. Belastete, ängstliche Zeugen werden aus dem realen Prozeßgeschehen herausgelöst, und es werden von ihnen - oft sehr intime - Daten unter Vorspiegelung einer nicht realen Situation erhoben. Es gehört zu den datenschutzrechtlichen Grundsätzen, daß der Betroffene bei der Datenerhebung möglichst genau darüber informiert sein muß, auf welche Weise, in welcher Situation und zu welchem Zweck seine Daten verwendet und übermittelt werden. Dem Zeugen darf deshalb kein geschöntes und daher falsches Bild von der wirklichen Verwendung seiner Daten vermittelt werden. Auch der kindliche Zeuge muß realistisch erkennen können, wer Datenempfänger ist und zu welchem Zweck seine Daten aktuell verwendet werden. Es gehört zur Würde des Zeugen, daß er in Anwesenheit aller Beteiligten sein Vernehmungsverhalten gerade auf diese Situation einrichten und ausrichten darf.
Zudem enthält die StPO - wie ich aus Erfahrung weiß: ausreichende - Vorkehrungen, mit denen ein Strafrichter es unterbinden kann, daß ein Kind als Opfer und Zeuge "in die Mangel genommen" wird.

Das SMJus habe ich von meinen Bedenken unterrichtet.

8.3 Entwurf einer Verwaltungsvorschrift für Straftäter in der Führungsaufsicht

Straftäter, bei denen mit einem Rückfall zu rechnen ist, werden, sobald sie sich in Freiheit befinden, unter bestimmten gesetzlichen Voraussetzungen der Führungsaufsicht unterstellt. Die Führungsaufsichtsstelle, d. h. ein Richter und ein Bewährungshelfer, leisten Resozialisierungshilfe, gleichzeitig überwachen sie den Verurteilten.

Das SMJus hat eine Verwaltungsvorschrift entworfen, deren Ziel es ist, die Zusammenarbeit der für die Strafvollstreckung und die Führungsaufsicht zuständigen Stellen zu regeln, und zwar in bezug auf besonders überwachungs- und betreuungsbedürftige Straftäter. Darunter sind laut Entwurf solche Verurteilte zu verstehen, deren erneute Straffälligkeit erhebliche Gefahren für Leib und Leben anderer mit sich bringen würde.

Strafvollstreckung und Führungsaufsicht ist immer mit dem Austausch sehr sensibler personenbezogener Daten verbunden. So begrüßenswert es ist, den damit befaßten Stellen eine Verhaltensrichtlinie an die Hand zu geben, so wichtig ist es auch, daß diese Richtlinie den gesetzlichen Vorgaben entspricht. Der Entwurf berücksichtigt das noch nicht in ausreichendem Maße.

- Der Entwurf sieht eine "enge und vertrauensvolle Zusammenarbeit aller Stellen" vor, die mit der Betreuung und Aufsicht der Verurteilten befaßt sind. Hierbei wird nicht beachtet, daß die Zusammenarbeit dieser Stellen im Gesetz bereits genau geregelt ist. Eine darüber hinausgehende generelle enge Zusammenarbeit und Entscheidung in gemeinsamer Absprache ist gesetzlich gerade nicht vorgesehen, da dies dem Sinn und Zweck der Führungsaufsicht sowie der Aufgabenzuweisung der einzelnen Stellen widerspräche.

- Die im Entwurf vorgesehene Regelung hinsichtlich der polizeilichen Ausschreibung entspricht nicht der gesetzlichen Regelung. Gemäß § 463 a Abs. 2 StPO kann die Aufsichtsstelle für die Dauer der Führungsaufsicht anordnen, daß der Verurteilte zur Beobachtung (bei polizeilichen Kontrollen) ausgeschrieben wird. Diese langfristige bundesweite Datenerfassung über eine Person greift tief in das Recht des Einzelnen auf informationelle Selbstbestimmung ein. Um so strenger müssen die Voraussetzungen für den Einsatz einer solchen Maßnahme gefaßt werden. Während das Gesetz die Anordnung in das Ermessen der Aufsichtsstelle stellt, enthält die Verwaltungsvorschrift hingegen eine Soll-Vorschrift, d. h. die Aufsichtsstelle hat grundsätzlich die polizeiliche Ausschreibung anzuordnen, nur bei begründeten Ausnahmefällen nicht. Dies ist eine Abweichung vom Gesetz.

- Während der Führungsaufsicht kann dem Verurteilten mit seiner Einwilligung die Weisung erteilt werden, sich einer Heilbehandlung oder Entziehungskur zu

unterziehen. In diesem Zusammenhang sieht der Entwurf vor, daß bei dem Verurteilten intensiv darauf hinzuwirken sei, seinen Arzt von der ärztlichen Schweigepflicht zu entbinden. Diese Regelung halte ich für unvereinbar mit dem Gedanken der Strafbewehrung in den einschlägigen Vorschriften des Strafgesetzbuchs: Zwanghafte Eingriffe in das Vertrauensverhältnis zwischen behandelndem Arzt und Patient müssen - wenn sie nicht strafbar sein sollen - in jedem Einzelfall gerechtfertigt sein. Sie dürfen nicht per Verwaltungsvorschrift pauschal angeordnet werden.

8.4 Reichweite der Kontrollbefugnisse des Sächsischen Datenschutzbeauftragten

Gemäß § 24 Abs. 1 SächsDSG kontrolliert der Sächsische Datenschutzbeauftragte bei den öffentlichen Stellen die Einhaltung des Sächsischen Datenschutzgesetzes und anderer Vorschriften über den Datenschutz. Nach § 24 Abs. 2 SächsDSG unterliegen Gerichte seiner Kontrolle nur, soweit sie in Justizverwaltungsangelegenheiten tätig werden (vgl. 1. Tätigkeitsbericht unter 8.1).
§ 24 Abs. 2 SächsDSG hat klarstellende Funktion. Das Prinzip der Gewaltenteilung, das seine Ausprägung in Art. 92 i. V. m. Art. 97 Abs. 1 GG gefunden hat, garantiert den Richtern in ihrer Eigenschaft als Rechtsprechungsorgan Unabhängigkeit. Insoweit, und nur insoweit, sind sie einer Kontrolle entzogen.
Gerichte üben aber nicht nur rechtsprechende Gewalt aus, sondern sie nehmen auch Verwaltungsaufgaben wahr, z. B. im Haushalts- und Personalwesen. Hierbei unterliegen sie, soweit sie personenbezogene Daten verarbeiten, der Kontrolle des Datenschutzbeauftragten.
Von dieser Grundlage ausgehend konnte die Auslegung des Begriffes "Justizverwaltungsangelegenheit" mit dem SMJus nunmehr - nach längerem Schriftwechsel - einvernehmlich geklärt werden.

8.5 Ergebnisse der Kontrolle der Justizvollzugsanstalt Waldheim

In meinem 4. Tätigkeitsbericht (8.2.1) habe ich über die Querschnittskontrolle der Datenverarbeitung der JVA Waldheim berichtet und dabei die Aufgeschlossenheit der Anstaltsleitung gegenüber den von mir aufgezeigten Problemkreisen hervorgehoben. Inzwischen hat mir die Anstaltsleitung mitgeteilt, daß fast alle meine Empfehlungen umgesetzt wurden.

So bekräftigt die JVA ihre Absicht, die anstaltsinterne Organisation so zu gestalten, daß sich die Vollzugsbediensteten nur insoweit von personenbezogenen Daten Kenntnis verschaffen dürfen, als dies zur Erfüllung der ihnen jeweils obliegenden Aufgaben erforderlich ist. Dies gilt insbesondere auch für den Zugriff auf die Gefangenenpersonalakten. Die Einhaltung dieses Grundsatzes soll in der JVA Waldheim dadurch sichergestellt werden, daß jede Einsichtnahme in Gefangenenpersonalakten von den einsichtnehmenden Bediensteten protokolliert wird. Die Protokollierung muß den Grund für die Einsichtnahme aufführen, damit

nachträglich stichprobenweise kontrolliert werden kann, ob die Akteneinsicht zur Aufgabenerfüllung erforderlich war. Das halte ich für vorbildlich.

Aufgegriffen wurden daneben auch weitere Anregungen. So wird beispielsweise das in der Justizvollzugsanstalt geführte Paketscheinbuch nunmehr nach einem Jahr vernichtet. Ein überflüssiger Vordruck, der im Zusammenhang mit der Besuchsüberwachung genutzt wurde, wird nicht mehr verwendet. Die Lichtbilder der Gefangenen werden nur noch in begrenzter Zahl an zentraler Stelle aufbewahrt (z. B. für Hausausweise, Freigängerausweise). Bereits vor meinem Kontrollbesuch enthielten die Gefangenenpersonalakten der Justizvollzugsanstalt Waldheim keinen Hinweis auf eine AIDS-Erkrankung. Sollte sich ein solcher Hinweis bei den Zugangsunterlagen finden, wird er durch die Vollzugsgeschäftstelle unleserlich gemacht. Weiterhin wurde meine Auffassung geteilt, daß Daten aus abgeschlossenen Gefangenenpersonalakten (z.B. Lichtbilder der Gefangenen) nur noch in Ausnahmefällen an dritte Stellen übermittelt oder sonst genutzt werden dürfen. Wegen des zum Zeitpunkt meiner Kontrolle fehlenden Datenschutzkonzepts hat sich die JVA Waldheim an das SMJus gewandt, damit ein landesweit abgestimmtes Konzept für die sächsischen Justizvollzugsanstalten erstellt werden kann.

8.6 Mitteilung der Anklageschrift an Dienstvorgesetzte

Anklagen gegen Beschäftigte des öffentlichen Dienstes werden von der Staatsanwaltschaft regelmäßig als Abdruck dem unmittelbaren Vorgesetzten des Beschäftigten zugesandt, damit dieser beurteilen kann, ob zur Vermeidung weiterer Verfehlungen arbeits- oder dienstrechtliche Maßnahmen ergriffen werden müssen.

Hierfür ist eine gesetzliche Grundlage erforderlich.
Zwar sieht Nr. 15 Abs. 1 Buchst. b i. V. m. Abs. 3 MiStra eine Mitteilung der Erhebung der öffentlichen Klage an den unmittelbaren Dienstvorgesetzten vor, jedoch kommt der MiStra als bloßer Justizverwaltungsvorschrift eine befugnisbegründende Normqualität nicht zu. Zudem ist sie im Freistaat Sachsen nicht durch einen entsprechenden Erlaß eingeführt worden.
Weil bereichsspezifische Regelungen fehlen, ist als Rechtsgrundlage für die Datenübermittlung die Auffangvorschrift des § 13 SächsDSG heranzuziehen. Danach hat eine Interessenabwägung zu erfolgen, und zwar zwischen dem Interesse des Diensthern an einem ungestörten Ablauf des Dienstverhältnisses und dem Interesse des Beschäftigten an der Wahrung seines Rechtes auf informationelle Selbstbestimmung sowie seines Rechtes auf ein faires Verfahren, wozu insbesondere die Unschuldsvermutung zählt, denn es wurde noch kein Urteil gefällt.

Die Staatsanwaltschaft kann demnach in einer einzelfallbezogenen Interessenabwägung zu dem Ergebnis kommen, die Anklageschrift überhaupt nicht zu übersenden, sie nur in Auszügen zu übermitteln oder dem Dienstvorgesetzten die vollständige Anklageschrift zukommen zu lassen. Eine 'automatische' Übersendung der Anklageschrift wäre unzulässig.

Ich habe die Staatsanwaltschaft auf diese Problematik aufmerksam gemacht und um Beachtung der dargestellten Grundsätze gebeten.

8.7 Lichtbildvorlage im Ermittlungsverfahren

In strafrechtlichen Ermittlungsverfahren werden Zeugen zur Ermittlung des Täters Lichtbilder des Tatverdächtigen zusammen mit Lichtbildern Unverdächtiger vorgelegt, um eine möglichst unbeeinflußte Aussage des Zeugen zu erhalten.
Dabei kann in das Recht auf informationelle Selbstbestimmung eingegriffen werden, denn Unverdächtige, die zu dem konkreten Verfahren in keiner Beziehung stehen, werden mittels ihres Lichtbildes in die Ermittlungen einbezogen. Der Zeuge erfährt, daß diese Personen, die er unter Umständen sogar kennt (wie übrigens der Fall eines Petenten gezeigt hat), früher schon einmal in ein Verfahren verwickelt waren, denn aus dieser Zeit hat die Polizei ihre Lichtbilder. Ein solcher Eingriff ist nur auf gesetzlicher Grundlage zulässig. Diese fehlt.

Die Strafprozeßordnung enthält als spezialgesetzliche Regelung keine entsprechenden Vorschriften. Insbesondere kann § 81 b 2. Fall StPO nicht herangezogen werden. Diese Vorschrift ermächtigt nicht dazu, erkennungsdienstliche Unterlagen in der Weise zu verwenden, daß die Lichtbilder von im konkreten Verfahren Unverdächtigen als "Wahllichtbildvorlage" genutzt werden.
Auch aus dem Legalitätsprinzip, das in den §§ 152 Abs. 2, 160 StPO seinen Ausdruck findet, kann sich nichts anderes ergeben. § 160 StPO ist zu allgemein gehalten und wird dem Abwägungsgebot nicht gerecht. Stets ist eine Interessenabwägung durchzuführen. Kriterien, die in die Abwägung einzustellen sind, sind unter anderem die Schwere des in Frage stehenden Deliktes, das Gewicht der verletzten Rechtsgüter und der Grad der Gefährdung, die von dem zu ermittelnden Täter ausgeht.

Ich habe die Problematik mit dem Sächsischen Staatsministerium der Justiz erörtert, das inzwischen eine entsprechende Prüfbitte mit dem Ziel der Schaffung klarer gesetzlicher Regelungen in die Beratungen des Bundesrates zum Strafverfahrensänderungsgesetz eingebracht hat.

8.8 Mitteilung von Patientendaten im Rahmen eines Bußgeldverfahrens gegen einen Arzt

Begeht ein Arzt bei Ausübung seiner Tätigkeit Ordnungswidrigkeiten, kann die Tat ganz ausnahmsweise gerechtfertigt sein. Er erhält zum Beispiel einen Notruf und muß nachweislich so schnell wie möglich zu seinem Patienten, weswegen er einen Rotlichtverstoß auf einer leeren Kreuzung begeht. Um dies überprüfen zu können, muß das Gericht jedoch Kenntnis von Daten des Patienten erhalten, zumindest von dessen Namen und Adresse, um ihn als Zeugen zu vernehmen.
Zu seiner Verteidigung muß der Arzt also diese Daten bekanntgeben. Damit verstößt er jedoch gegen seine Schweigepflicht. Die Weitergabe auch lediglich von Namen und

Anschrift des Patienten erfüllt den Tatbestand des § 203 StGB, denn schon die bloße Tatsache, einen bestimmten Arzt aufgesucht zu haben, ist als Geheimnis anzusehen, da im Berufs- und Privatleben gesundheitlichen Daten ein hoher Stellenwert zukommt und deshalb bereits die Kenntnis von der Tatsache, daß ein Arzt aufgesucht wurde, nachteilige Folgen haben kann. Diese Schweigepflicht darf nur ausnahmsweise und unter sehr engen Voraussetzungen durchbrochen werden.
Der Arzt muß also eine Einwilligung seines Patienten einholen, daß er ihn als Zeugen benennen darf. Erteilt der Patient diese Einwilligung nicht, muß das Gericht z. B. auf die Aussage einer Sprechstundenhilfe zurückgreifen; es ist nicht gehindert, dem Arzt zu glauben.

8.9 Personalfragebogen für die Berufung zum ehrenamtlichen Richter

Im Freistaat Sachsen sind zur Zeit 615 ehrenamtliche Richter in der Verwaltungsgerichtsbarkeit tätig. Die Kreise und kreisfreien Städte stellen eine Vorschlagsliste auf, aus der ein Wahlausschuß die erforderliche Zahl von ehrenamtlichen Richtern für vier Jahre wählt.
Diese Vorschlagsliste enthält neben Namen und Wohnanschrift auch Angaben zum Geburtsdatum, Geburtsort, Familienstand, zur Staatsangehörigkeit, zum Beruf sowie zu einer früheren ehrenamtlichen Richtertätigkeit und Angaben darüber, seit welchem Zeitpunkt man in der Gemeinde wohnhaft ist.
Ich habe diese Vorschlagsliste auf ihre Vereinbarkeit mit den datenschutzrechtlichen Vorschriften hin überprüft:
Die Erhebung dieser Daten findet ihre Grundlage in den §§ 19 ff. VwGO, die das Verfahren zur Berufung der ehrenamtlichen Richter regeln. Diese Vorschriften stehen im Einklang mit dem sich aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG ergebenden Recht auf informationelle Selbstbestimmung. Ehrenamtliche Richter müssen als Kontrollorgane von der Öffentlichkeit legitimiert sein. Diesen Gedanken beachtet das in den §§ 26 bis 30 VwGO beschriebene Verfahren. Denn die Öffentlichkeit wirkt durch den Kreistag bzw. Gemeinderat sowie durch den Wahlausschuß an der Wahl mit. Damit diese Gremien ihren Aufgaben gerecht werden können, müssen ihnen entsprechende personenbezogene Daten der eventuell zu berufenden ehrenamtlichen Richter bekannt gemacht werden. Die in der Vorschlagsliste aufgeführten Daten sind hierbei auf ein unerläßliches Maß beschränkt worden.

8.10 Noch einmal: Rechtsanwaltskammer verlangt Offenbarung von Mandantennamen

Will ein Rechtsanwalt eine Fachanwaltsbezeichnung führen, muß er der Rechtsanwaltskammer nachweisen, daß er besondere Kenntnisse und Erfahrungen auf diesem Rechtsgebiet erworben hat.
Gemäß § 9 Rechtsanwaltsfachbezeichnungsgesetz (RAFachBezG) ist dieser Nachweis in der Regel erbracht, wenn der Anwalt im Fachgebiet eine bestimmte Anzahl von Fällen selbständig bearbeitet hat. Um dies nachzuprüfen, verlangte die Sächsische Rechtsanwaltskammer im Bereich Steuerrecht die Vorlage einer Liste von 50

Mandanten sowie deren Steuernummer, anhand deren wohl einzelne Akten stichprobenweise überprüft werden sollten. Dieses Verfahren ist unzulässig, weil zur Prüfung der Fachanwaltsbefähigung die Übermittlung anonymisierter Akten völlig ausreicht. Zudem kann eine Einwilligung der Mandanten zur Weitergabe seiner Daten an die Rechtsanwaltskammer eingeholt werden. Wie bereits in meinem 4. Tätigkeitsbericht (8.5) dargestellt, habe ich die Rechtsanwaltskammer hierauf hingewiesen. Das SMJus habe ich gebeten, im Rahmen seiner Rechtsaufsicht entsprechende Maßnahmen zu veranlassen. Es hat daraufhin die Rechtsanwaltskammer angewiesen, folgendes Verfahren einzuhalten: Der antragstellende Rechtsanwalt wird auf seine Schweigepflicht hingewiesen. Akten, die er der Rechtsanwaltskammer vorzulegen hat, sind zu anonymisieren, oder es ist die Einwilligung der Betroffenen einzuholen.
Aus gegebenem Anlaß werde ich die Einhaltung dieser Weisung im Auge behalten.

Leider mußte ich aus Anlaß einer Eingabe feststellen, daß diese verbindliche Weisungslage noch immer nicht von sämtlichen Gremien der Rechtsanwaltskammer beachtet wird. So forderte der Vorsitzende eines Fachausschusses einen antragstellenden Rechtsanwalt auf, seine eingereichten Unterlagen zu vervollständigen, und zwar seine "Angaben lieber zu ausführlich als zu knapp zu gestalten". Zu den "Angaben" gehörten laut beigefügtem Hinweisblatt auch die "Namen der Mandanten und des Gegners". Auf meine daraufhin an die Rechtsanwaltskammer gerichtete Bitte um Klarstellung erhielt ich eine ausweichende Antwort, die erkennen läßt, daß der Vorstand der Kammer die Tragweite der rechtsaufsichtlichen Weisung des SMJus noch immer nicht erkannt hat.
Eine Beanstandung bereite ich vor.

8.11 Vorkaufsrecht der Gemeinden

Steht einer Gemeinde beim Kauf von Grundstücken ein gesetzliches Vorkaufsrecht nach § 24 ff. BauGB zu, so hat der Verkäufer der Gemeinde den Inhalt des Kaufvertrages unverzüglich mitzuteilen. Die Gemeinde kann dann binnen zweier Monate das Vorkaufsrecht ausüben. Damit hierbei datenschutzrechtliche Belange ausreichend berücksichtigt werden, halte ich ein zweistufiges Verfahren für geboten:

Zur Prüfung des Bestehens eines Vorkaufsrechtes erhält die Gemeinde zunächst nur bestimmte Mindestangaben über die Art des Vertrages, die Vertragsparteien und die katastermäßige Bezeichnung des Grundstückes sowie einen Hinweis darauf, ob das Grundstück bebaut ist oder nicht. Erst wenn die Gemeinde an der Ausübung des Vorkaufsrechtes interessiert ist, erhält sie auf Anforderung den vollständigen Vertragsinhalt.

Weil Kaufverträge über Grundstücke nach § 313 BGB der notariellen Beurkundung bedürfen und der Notar nach § 28 BauGB auch die Aufgabe der Mitteilung an die Gemeinde zu übernehmen hat, habe ich mich an die Notarkammer Sachsen gewandt. Die Kammer teilte mir mit, daß die Anwendung des zweistufigen Verfahrens von der

Haltung der jeweiligen Gemeinde abhänge. Manche Gemeinde stelle sich auf den Standpunkt, das zweistufige Verfahren verzögere die Ausübung des Vorkaufsrechtes, deshalb fordere sie stets die Übermittlung des vollständigen Kaufvertrages.
Ich werde versuchen, hier einvernehmlich eine datenschutzgerechte Lösung zu finden.

9 Wirtschaft und Arbeit

9.1 Straßenverkehrswesen

9.1.1 Gesetzentwurf zur Änderung des Straßenverkehrsgesetzes und anderer Gesetze

Neben den bisher schon beim Kraftfahrt-Bundesamt vorhandenen *zentralen* Dateien, nämlich dem Fahrzeugregister (hier werden z. B. die Daten sämtlicher Kfz-Halter gespeichert) und dem Verkehrszentralregister (hier werden u. a. alle verkehrsbedingten Straftaten und Ordnungswidrigkeiten erfaßt) soll ein weiteres zentrales Auskunftsregister, nämlich das zentrale Fahrerlaubnisregister, eingeführt werden. Registriert werden sollen Daten zu allen Fahrerlaubnisinhabern (z. B. Familienname, Vorname, Tag der Geburt, nicht jedoch die Anschrift), zur Fahrerlaubnis (z. B. Umfang) und zur Länge der Probezeit. Zugriffsberechtigt sollen u. a. die Strafverfolgungsbehörden und die Bußgeldstellen im Inland und europäischen Ausland sein. Die örtlichen Fahrzeugregister sollen frühestens ab dem Jahr 2006 entfallen.

Im Gegensatz zum Bundesbeauftragten für den Datenschutz, der den Wegfall der örtlichen Fahrerlaubnisregister zugunsten eines Zentralregisters für einen datenschutzrechtlichen Fortschritt hält (keine Doppelspeicherung, kein Rückgriff auf die aktuellen Anschriften), habe ich mich im Einvernehmen mit den meisten Landesbeauftragten für den Datenschutz hierzu sehr kritisch geäußert. Ich bezweifle, ob eine solche zentrale Erfassung eines sehr großen Teils der Bevölkerung wirklich zur Aufgabenerfüllung der zugriffsberechtigten Stellen erforderlich und angemessen ist. Zudem habe ich auf die große Mißbrauchsgefahr der zentralen Erfassungsstelle hingewiesen. Auch nach der Lektüre der Begründung sind mir die Argumente noch schleierhaft.

Die Bedenken blieben jedoch unberücksichtigt. Der Bundesrat hat dem Entwurf bereits zugestimmt.

9.1.2 Eignungsprüfung bei Neuerteilung einer Fahrerlaubnis

Die Fahrerlaubnisbehörden verlangen im Verfahren der Neuerteilung einer Fahrerlaubnis von den Antragstellen detaillierte Angaben zum Gesundheitszustand und zu strafrechtsrelevanten Sachverhalten. Solche Datenerhebungen sind nicht in den insoweit abschließenden Datenverarbeitungsvorschriften des Straßenverkehrsgesetzes und der Straßenverkehrs-zulassungsordnung vorgesehen und daher unzulässig.

Das SMWA, das ich davon unterrichtet habe, hat daraufhin die Fahrerlaubnisbehörden angewiesen, nur noch folgende Fragen zu stellen:
1. "Sind Sie vorbestraft?"
2. "Haben Sie Krankheiten oder körperliche Leiden, die Ihre Fahreignung

beeinträchtigen können?"
Begründet wurde diese Weisung (sinngemäß) damit, daß die Reduzierung auf zwei Fragen einerseits dem Datenschutz entgegenkomme, andererseits die Selbstauskunft durch die straßenverkehrsrechtlichen Vorschriften nicht ausgeschlossen sei.

In einem konstruktiven Gespräch mit dem SMWA konnte ich klären, daß dies ein unrichtiger Ansatz ist: Artikel 33 Satz 3 SächsVerf verlangt für die Verarbeitung personenbezogener Daten (hierzu zählt auch das Erheben) ohne Zustimmung des Betroffenen eine ausdrückliche gesetzliche *Erlaubnis*. Mangelt es hieran, greift der Grundrechtsschutz von Artikel 33. Jede Verarbeitung personenbezogener Daten ist dann *verboten* (Verbot mit Erlaubnisvorbehalt). Zudem habe ich darauf hingewiesen, daß die Fahrerlaubnisbehörden strafrechtsrelevante Daten im Rahmen der Eignungsprüfung durch Anfrage beim VZR (vgl. § 13 c StVZO) oder durch Vorlage eines Führungszeugnisses (vgl. § 8 Abs. 3 StVZO) erhalten dürfen. Nur wenn diese Datenerhebungsvorschriften beachtet werden, ist sichergestellt, daß ausschließlich solche Verurteilungen zur Frage der Fahrtauglichkeit berücksichtigt werden, die im VZR/BZR noch nicht getilgt sind, also dem Betroffenen im Rechtsverkehr zulässigerweise vorgehalten werden dürfen (Stichwort: „Bewährungsgedanke“). Zwar enthält das Führungszeugnis viele Vorstrafen, die auf den ersten Blick keinerlei Einfluß auf die Fahreignung des Betroffenen haben, also - so könnte man meinen - zur Aufgabenerfüllung der Fahrerlaubnisbehörden nicht erforderlich sind. Eine solche Sichtweise ist aber unrichtig. Es ist gerade Aufgabe der Fahrerlaubnisbehörden (und steht in ihrem pflichtgemäß auszuübenden Ermessen), selbst zu entscheiden, ob und welche Straftaten Rückschlüsse auf die Nichteignung des Betroffenen zulassen.
An gesundheitsrelevanten Daten dürfen Sehtestbescheinigungen (vgl. § 9 a StVZO) und im Einzelfall ein in § 12 Abs. 1 StVZO näher bezeichnetes Gutachten gefordert werden.

Durch die undifferenzierte Frage nach Vorstrafen und der Frage nach dem Gesundheitszustand würden diese Vorschriften umgangen.

Meine Auffassung wird im Ergebnis durch die Kommentierung von Jagusch/Hentschel, Straßenverkehrsrecht, Rdnr. 2 zu § 9 StVZO, gestützt. Hiernach berechtigt die allgemeine Ermittlungsvorschrift des § 9 StVZO nicht dazu, "den Bewerber über der Behörde unbekannte eignungsmindernde oder -ausschließende Tatsachen, z. B. über körperliche Gebrechen, zu befragen".

Das SMWA hat zugesagt, die Weisung nochmals kritisch rechtlich zu prüfen und einstweilen nicht auf deren Einhaltung zu drängen. Ich werde die weitere Entwicklung beobachten.

9.1.3 Verlängerung der Fahrerlaubnis zur Fahrgastbeförderung ab dem 50. Lebensjahr

Das Bundesverwaltungsgericht (Urteil vom 17. Mai 1995 - 11 c 2.94) hat entschieden, daß die Fahrerlaubnisbehörden für die Verlängerung einer Fahrerlaubnis zur Fahrgastbeförderung kein Gutachten einer amtlich anerkannten medizinisch-psychologischen Untersuchungsstelle fordern dürfen, wenn Eignungsbedenken allein aufgrund des fortgeschrittenen Alters der Antragsteller (hier: 50 Jahre) bestehen. In diesen Fällen ist es lediglich zulässig, einen (ärztlichen) Nachweis über verkehrsrelevante Fähigkeiten (z. B. Belastbarkeit, Reaktionsvermögen) zu verlangen.

Aus Gründen der Rechtssicherheit und zum Schutz des Persönlichkeitsrechts der Betroffenen hat das SMWA zugesagt, die Fahrerlaubnisbehörden auf Beachtung dieses (teilweise fehlinterpretierten) Urteils ausdrücklich hinzuweisen und die Eignungsrichtlinien dem Urteil anzupassen.

9.1.4 Übermittlung von Kfz-Halterdaten ins Ausland

Aus dem benachbarten Ausland bat ein Petent eine sächsische Fahrerlaubnisbehörde um einfache Registerauskunft (Name und Anschrift des Halters). Er begründete dies damit, daß der Fahrer des PKW seine Garagenauffahrt beschädigt habe; er erwäge eine Schadensersatzklage.

Die Fahrerlaubnisbehörde verweigerte die Auskunft zunächst unter Hinweis auf § 37 Abs. 1 StVG, wonach Datenübermittlungen ins Ausland nur zur Erfüllung internationaler Verpflichtungen zulässig sind, und bat mich um datenschutzrechtliche Bewertung.

Ich habe der Fahrerlaubnisbehörde mitgeteilt, daß hier nicht § 37 Abs. 1 StVG, sondern § 39 Abs. 1 StVG einschlägig sei. Hiernach ist die einfache Registerauskunft zulässig, wenn die Daten u. a. zur Geltendmachung von Rechtsansprüchen im Zusammenhang mit der Teilnahme am Straßenverkehr benötigt werden (was hier der Fall war); dabei ist es gleichgültig, ob die Frage aus dem In- oder Ausland kommt. Die Vorschrift des § 37 StVG ist keine gegenüber § 39 StVG vorrangige und abschließende Regelung zur Frage der Zulässigkeit von Datenübermittlungen ins Ausland. Die Fahrerlaubnisbehörde hat daraufhin die Auskunft erteilt.

Das SMWA, das ich um Stellungnahme gebeten habe, teilt meine Auffassung.

9.1.5 Datenverarbeitung durch Private bei Geschwindigkeitsüberwachungen

Das steigende Verkehrsaufkommen fördert bei den zuständigen staatlichen Stellen die Bereitschaft, Private mit der Wahrnehmung von Hilfsaufgaben bei der Ahndung von Verkehrsverstößen zu betrauen. In Betracht kommen das Entwickeln von Filmen und das Installieren von Meßgeräten. Gegen eine auf diese Tätigkeiten beschränkte

Wahrnehmung staatlicher Aufgaben durch Private habe ich aus verfassungsrechtlicher Sicht keine Bedenken:

Gemäß Art. 33 Abs. 4 GG ist die Ausübung hoheitsrechtlicher Befugnisse als ständige Aufgabe in der Regel Angehörigen des öffentlichen Dienstes zu übertragen, die in einem öffentlich-rechtlichen Dienst- und Treueverhältnis stehen.
Es obliegt dem Gesetzgeber, diejenigen Aufgaben zu bestimmen, die er von nichtbeamteten Personen wahrnehmen lassen will (BVerwGE 57, 55, 60). Würde die ständige Ausübung hoheitlicher Befugnisse (also der Erlaß eines Verwaltungsaktes) in größerem Umfang auf Nichtbeamte übertragen, so wäre dies mit dem Grundgesetz nicht vereinbar (BVerfGE 9, 268, 284). Da der Staat das unteilbare Gewaltmonopol besitzt, kann zwar die eigentliche Verfolgungskompetenz des Staates nicht durch eine entsprechende Ermächtigung auf Private übertragen werden.
Die Leistung untergeordneter Hilfsdienste aber ist nicht als ständige Ausübung hoheitsrechtlicher Befugnisse anzusehen. Die Mitwirkung eines Privaten ist zulässig, soweit ihm nicht die Herrschaft über den Verfahrensablauf der Verfolgung übertragen wird, sondern diese beim Staat verbleibt, dem Privaten also keine Entscheidungsbefugnisse eingeräumt werden. Er darf auch nicht die Ermittlungen in der Weise führen, daß allein aufgrund der von ihm selbständig und eigenverantwortlich ermittelten Tatsachengrundlage eine Entscheidung der Behörde ergeht. Der festgestellte Lebenssachverhalt ist Grundlage der Entscheidung, so daß dessen Ermittlung in der Verantwortung des Staates bleiben muß. Der Staat begibt sich dieser Verantwortung aber nicht, wenn er Private zu Hilfsdiensten im technischen Bereich heranzieht, z. B. bei der Bereitstellung und Aufstellung von Überwachungsgeräten. Hingegen fällt die Entscheidung, das Gerät im Einzelfall in Betrieb zu nehmen, bereits in den Bereich der Ermittlungstätigkeit, weswegen sie nicht einem Privaten überlassen werden darf.

Die "Aufbereitung" von Daten, die bei Verkehrsüberwachungen erhoben werden, stellt sich so lange als eine reine Hilfstätigkeit dar, als mit der Aufbereitung keine Auswertung verbunden ist, sondern lediglich Filme entwickelt oder Fotoabzüge hergestellt werden. Diese Hilfstätigkeit ist Datenverarbeitung, da personenbezogene Daten auf einem Datenträger zum Zweck ihrer weiteren Verarbeitung erfaßt werden. Führt diese Verarbeitung im Sinne einer reinen Hilfstätigkeit statt der Ordnungsbehörde oder Staatsanwaltschaft ein privater Dritter durch, liegt eine Datenverarbeitung im Auftrag vor. Somit ist § 7 SächsDSG einschlägig, der die datenschutzrechtlichen Erfordernisse im Auftragsverhältnis regelt.

9.2 Gewerberecht

9.2.1 Rechtliche Entwicklung

Im 4. Tätigkeitsbericht bin ich kurz auf die seit Dezember 1995 bestehende Rechtslage eingegangen und habe die wesentlichen Änderungen der Gewerbeordnung erwähnt.

Zahlreiche Anfragen mit datenschutzrechtlichem Bezug zur Gewerbeordnung veranlassen mich, etwas ausführlicher auf die mit der Gesetzesnovelle einhergegangenen Datenschutzaspekte einzugehen.

Mit dem Gesetz zur Änderung der Gewerbeordnung und sonstiger gewerberechtlicher Vorschriften vom 23.11.1994 (BGBl. I S. 3475) sind von den Datenschutzbeauftragten lange geforderte Datenschutzregelungen - allerdings nicht voll befriedigend - in die Gewerbeordnung aufgenommen worden. Dieser Teil der novellierten GewO ist am *1. Dezember 1995* in Kraft getreten. Ergänzend hat das Sächsische Staatsministerium für Wirtschaft und Arbeit am 6.10.1995 die ebenfalls ab *1. Dezember 1995* gültige Verwaltungsvorschrift zur Durchführung der §§ 14, 15 und 55 c der Gewerbeordnung (GewAnzVwV) erlassen.

Hervorzuheben sind die Regelungen in *§ 11 GewO* über Erhebung, Verarbeitung und Nutzung von Daten.

§ 11 GewO (auszugsweise):

(1) Die zuständige öffentliche Stelle darf personenbezogene Daten des Gewerbetreibenden und solcher Personen, auf die es für die Entscheidung ankommt, erheben, soweit die Daten zur Beurteilung der Zuverlässigkeit und der übrigen Berufszulassungs- und -ausübungskriterien bei der Durchführung gewerberechtlicher Vorschriften und Verfahren erforderlich sind. Erforderlich können insbesondere auch Daten sein aus bereits abgeschlossenen oder sonst anhängigen
1. gewerberechtlichen Verfahren, Straf- oder Bußgeldverfahren,
2. Vergleichs- oder Konkursverfahren,
3. steuer- und sozialversicherungsrechtlichen Verfahren oder
4. ausländer- und arbeitserlaubsnisrechtlichen Verfahren.

(2) Die für Zwecke des Abs. 1 erforderlichen Daten sind beim Betroffenen zu erheben. Ohne seine Mitwirkung dürfen sie nur erhoben werden, wenn
1. die Entscheidung eine Erhebung bei anderen Personen oder Stellen erforderlich macht oder
2. die Erhebung beim Betroffenen einen unverhältnismäßigen Aufwand erforderlich machen würde und keine Anhaltspunkte dafür bestehen, daß überwiegende schutzwürdige Interessen des Betroffenen beeinträchtigt werden ..."

Zu begrüßen ist insbesondere, daß die Daten nunmehr grundsätzlich beim Betroffenen selbst zu erheben sind.

Ebenfalls hervorzuheben sind die in *§ 14 GewO* getroffenen Regelungen, welche Gewerbetreibendendaten zu welchen Zwecken an öffentliche und nicht-öffentliche Stellen übermittelt werden dürfen.

Insbesondere zählt § 14 *Abs. 5* GewO (abschließend) die Stellen auf, an welche die

Gewerbebehörden *regelmäßig* Daten aus den Gewerbeanzeigen übermitteln dürfen. Das sind konkret
- Industrie- und Handelskammer
- Handwerkskammer
- Staatliches Umweltfachamt
- Gewerbeaufsichtsamt
- Eichamt
- Arbeitsamt
- Landesverband Bayern und Sachsen der gewerblichen Berufsgenossenschaften
- AOK
- Registergericht
- auf der Grundlage des § 138 AO das Finanzamt.

Die Datenübermittlung erfolgt zur gesetzlichen Aufgabenerfüllung der Empfänger. Es werden jeweils nur die erforderlichen Daten (also nicht die komplette Gewerbeanzeige) übermittelt.

An andere öffentliche Stellen - als die vorgenannten - dürfen keine *regelmäßigen* Datenübermittlungen erfolgen.

Dies schließt allerdings nicht aus, daß öffentliche Stellen (außer öffentlich-rechtliche Wettbewerbsunternehmen) *fallweise* nach § 14 Abs. 6 GewO als sog. *einfache Gewerbeauskunft* die Gewerbetreibendendaten
1. Name (des Gewerbetreibenden),
2. betriebliche Anschrift,
3. angezeigte Tätigkeit

erhalten dürfen, soweit dies zur Aufgabenerfüllung des Datenempfängers erforderlich ist.

Weitere Daten aus der Gewerbeanzeige dürfen öffentlichen Stellen nur übermittelt werden, wenn
1. dies zur Abwehr erheblicher Nachteile für das Gemeinwohl oder einer sonst unmittelbar drohenden Gefahr für die öffentliche Sicherheit erforderlich ist *oder*
2. die Empfänger die Daten beim betroffenen Gewerbetreibenden nur mit unverhältnismäßig hohem Aufwand erheben können *oder* von einer solchen Datenerhebung nach der Art der Aufgabe, zu der die Daten erforderlich sind, abgesehen werden muß

und kein Grund zu der Annahme besteht, daß das schutzwürdige Interesse des Gewerbetreibenden überwiegt.

§ 14 Abs. 7 GewO befaßt sich mit der regelmäßigen oder fallweisen Weitergabe (*auch Online*) von Gewerbetreibendendaten *innerhalb* der Verwaltungseinheit, der die Gewerbebehörde angehört.

Die Gewerbeanzeigen werden seit jeher innerhalb der Verwaltung einer Kommune den sachlich betroffenen Ämtern zugeleitet (z. B. Bauamt, Lebensmittelüberwachungsbehörde), die zur Durchführung der in ihre Zuständigkeit fallenden Aufgaben zumindest die drei in Absatz 6 Satz 1 genannten Grunddaten benötigen. Dies wird durch Absatz 7 Satz 1 weiterhin zugelassen.

Die Einrichtung eines automatisierten Abrufverfahrens wird in den neueren Datenschutzgesetzen der Länder vom Vorliegen einer besonderen bundes- oder landesrechtlichen Ermächtigungsnorm abhängig gemacht. Da ein bundesweites Bedürfnis für ein automatisiertes Abrufverfahren für die Ämter innerhalb einer Kommune besteht, wird diese Möglichkeit durch Satz 2 eröffnet. Die Sätze 3 bis 5 enthalten Vorschriften über die Protokollierung der Abrufe. Die Protokollierung dient der nachträglichen Überprüfung, ob die Abrufe zulässig waren. Die Pflicht der am Abrufverfahren beteiligten Stellen, die nach § 9 SächsDSG erforderlichen technischen und organisatorischen Maßnahmen zu ergreifen, bleibt hiervon unberührt.

§ 14 Abs. 8 GewO dürfte die für den nicht-öffentlichen Bereich bedeutsamste Vorschrift sein. Geregelt wird nämlich, unter welchen Voraussetzungen Private Daten über Gewerbetreibende von der Gewerbebehörde erhalten dürfen.

Nicht-öffentlichen Stellen dürfen aus der Gewerbeanzeige als *einfache Gewerbeauskunft* die drei Grunddaten
1. Name,
2. betriebliche Anschrift,
3. angezeigte Tätigkeit

übermittelt werden, wenn der Auskunftsbegehrende ein *berechtigtes Interesse glaubhaft macht. Berechtigtes Interesse* ist jedes von der Rechtsordnung erlaubte Interesse, also auch ein *wirtschaftliches* Interesse (zum Begriff "Glaubhaftmachen" nachstehend unter 9.2.2).

Zulässig sind unter dieser Voraussetzung sowohl *Einzelauskünfte* als auch *Gruppenauskünfte*, z. B. an Berufsverbände, Adreßbuchverlage, Markt- und Meinungsforschungsinstitute, Versicherungen, Handelsauskunfteien, Inkassobüros usw.

Dies ist ein - aus datenschutzrechtlicher Sicht - bedauerlicher Rückschritt gegenüber der bis 30. November 1995 geltenden Rechtslage. Seinerzeit durften *Gruppenauskünfte* nur mit *ausdrücklicher Zustimmung* der Gewerbetreibenden und nur zum Zwecke der Werbung oder Meinungsforschung erteilt werden. Heute - und das hat der Bundesgesetzgeber zu vertreten - wird dem Recht auf informationelle Selbstbestimmung der Gewerbetreibenden ein schlechter Dienst erwiesen. Dem Schutz der drei Grunddaten (Name, betriebliche Anschrift, angezeigte Tätigkeit) wird wenig Bedeutung beigemessen.

Wünschen nicht-öffentliche Stellen *weitere* Daten (außer den drei Grunddaten),

werden allerdings höhere (dennoch nicht voll befriedigende) Anforderungen an eine Auskunftserteilung gestellt.

Nach § 14 Abs. 8 Satz 2 GewO ist die Übermittlung weiterer Daten nämlich nur zulässig, wenn der (private) Auskunftsbegehrende ein *rechtliches Interesse*, insbesondere zur Geltendmachung von Rechtsansprüchen (z. B. vollstreckbarer Titel), an der Kenntnis der zu übermittelnden Daten glaubhaft macht *und* kein Grund zu der Annahme besteht, daß das schutzwürdige Interesse des Gewerbetreibenden überwiegt (zum Begriff "Glaubhaftmachen" nachstehend unter 9.2.2).

Als datenschutzrechtliches Defizit ist es zu werten, daß der Gewerbetreibende *nicht* ausdrücklich *vor* solchen *erweiterten* Gewerbeauskünften anzuhören und *nach* erteilter Auskunft zu unterrichten ist. Nach meinem Dafürhalten kann die Frage, ob schutzwürdige Interessen des Betroffenen einer Auskunftserteilung entgegenstehen, nur nach Anhörung des Gewerbetreibenden ausreichend beantwortet werden.

Wegen dieses Mangels ist es m. E. bedeutsam zu wissen, daß eine Gewerbeanzeigen-datei bzw. -kartei kein *öffentliches* Register ist. Ob Auskunft erteilt wird oder nicht, steht im pflichtgemäßen Ermessen der Gewerbebehörde. Fehlerfreie Ermessensausübung setzt voraus, daß die Behörde ihre Ermessensentscheidung aufgrund einer *einwandfreien und erschöpfenden* Ermittlung des entscheidungserheblichen Sachverhalts getroffen und alle für die Ermessensausübung nach dem Zweck der Ermächtigungsnorm (die Gewerbebehörde "darf") wesentlichen Gesichtspunkte tatsächlicher und rechtlicher Art spätestens zum Zeitpunkt der (letzten) Entscheidung berücksichtigt hat.

Nimmt eine Gewerbebehörde diesen Grundsatz ernst, wird sie den Gewerbetreibenden (auch ohne ausdrückliche Regelung im Gesetz) vor der Auskunftserteilung anhören, um abwägen zu können, ob schutzwürdige Interessen des Betroffenen die Interessen des Auskunftsbegehrenden überwiegen. Sollte die Auskunft nach dieser Abwägung zugunsten des Auskunftsbegehrenden ausfallen, halte ich auch eine (nachherige) Unterrichtung des Gewerbetreibenden über die erteilte Auskunft für tunlich, um diesem den Rechtsweg zu eröffnen (Art. 19 Abs. 4 GG).

Mit diesen Ausführungen habe ich beileibe nicht sämtliche datenschutzrelevanten Sachverhalte des Gewerberechts erörtern können. Das Recht auf informationelle Selbstbestimmung wird in zahlreichen anderen Vorschriften über die Verarbeitung von Gewerbetreibendendaten berührt. Beispielsweise durch
- § 35 GewO - Gewerbeuntersagungsverfahren,
- §§ 149 ff. GewO - Gewerbezentralregister,
- erlaubnispflichtige Gewerbe und Zuverlässigkeitsprüfungen,
- Handwerks- und Lehrlingsrolle,
- Beitragsbemessung (steuerrelevante Daten - Meßbeträge) der Kammern.

9.2.2 Nochmals: Zum Begriff "Glaubhaftmachen"

Nach § 14 Abs. 8 GewO dürfen aus der Gewerbeanzeige an nicht-öffentliche Stellen "Name, betriebliche Anschrift und angezeigte Tätigkeit" des Gewerbetreibenden nur dann übermittelt werden, wenn der Auskunftsbegehrende ein berechtigtes Interesse an der Kenntnis der Daten *glaubhaft macht.* In Abschnitt 9.2.4 des 4. Tätigkeitsberichts habe ich ausgeführt, daß der Begriff "Glaubhaftmachen" das Schildern eines *nachprüfbaren Sachverhalts* voraussetzt. Dies hat teilweise unter den Gewerbeämtern zu Unsicherheit geführt, welchen Umfang dieser Sachverhalt haben muß und ob (und ggf. wie) er belegt werden muß.

Zur Klarstellung habe ich folgende Auslegungshinweise gegeben, unter welchen Voraussetzungen ein Interesse glaubhaft gemacht ist:

a) Materiell muß - kurz und knapp aber nachvollziehbar - ein Lebenssachverhalt geschildert werden, der die Erforderlichkeit der Kenntnis jedes erbetenen Einzeldatums ersichtlich werden läßt.
b) Formell muß dieser Sachverhalt so weit nachgewiesen werden, daß der Behörde seine Wahrscheinlichkeit vermittelt wird; ein voller Beweis ist also nicht nötig. Die Behauptung muß aber in angemessener Weise bekräftigt werden. Eine Glaubhaftmachung vor Gericht kann durch Urkunden, eidesstattliche Versicherung, anwaltschaftliche Versicherung etc. geschehen (§ 294 ZPO). Vor einer Behörde können andere Bekräftigungsmittel, z. B. schriftliche Erklärung an Dritte, Briefwechsel, Schilderung des eigenen Geschäftszweigs durch Briefbogen etc. ausreichen. Einfache, alltägliche Sachverhalte bedürfen einer schwächeren Bekräftigung; gleiches gilt für die Frage nach Daten mit geringem Schutzniveau.

9.2.3 Weitergabe von Gewerbeanzeigen an die AOK

Nach § 14 Abs. 5 Nr. 7 GewO erfolgt eine regelmäßige Weitergabe der Gewerbeanzeigen an die AOK für den Einzug der Sozialversicherungsbeiträge *und für die Weiterleitung an die anderen in ihrem Zuständigkeitsbereich tätigen Krankenkassen zu dem gleichen Zweck.* Diese Vorschrift, die am 1. Dezember 1995 in Kraft getreten ist, dürfte durch das seit 1. Januar 1996 bestehende Krankenkassenwahlrecht der Versicherungspflichtigen überholt sein. Die Basisfunktion der AOK ist seither weggefallen.

Der IKK-Landesverband Sachsen teilte mir seine - wohl nicht unberechtigten - Bedenken gegen den mit o. a. Bestimmung verbundenen Informations- und Wettbewerbsvorsprung der AOK gegenüber den anderen Kassen mit und schlug vor, daß künftig eine "neutrale" Institution mit der Verteilung der Gewerbeanzeigen betraut wird.

Wegen der erforderlichen Gesetzesänderung habe ich mich an die Staatsministerien für Wirtschaft und Arbeit und für Soziales, Gesundheit und Familie gewandt, um eine Änderung des § 14 Abs. 5 Nr. 7 GewO durch den Bundesgesetzgeber zu erreichen. Mir

wurde mitgeteilt, daß das Bundesministerium für Gesundheit ebenfalls eine Änderung der Vorschriften für angezeigt hält, nach denen die zuständigen Behörden die Daten von Gewerbeanzeigen der AOK zuzuleiten haben, die von dort an die anderen im Zuständigkeitsbereich tätigen Krankenkassen weitergeleitet werden. Die notwendige Ressortabstimmung sei im Herbst 1996 mit dem Ziel der Gesetzesänderung eingeleitet worden. Ein Ergebnis bleibt abzuwarten.

9.2.4 Auskunft über türkische Gewerbetreibende an die Polizei

Sächsische Polizeibehörden haben die Gewerbeämter aufgefordert, Anschriften von ausländischen, insbesondere türkischen Gewerbetreibenden mitzuteilen, damit die Betroffenen wirkungsvoll vor PKK-Anschlägen geschützt werden können.
Ein Bürgermeister verweigerte im Hinblick auf § 14 GewO die Gewerbeauskünfte; wie ich meine, zu Recht.

Nach § 14 Abs. 6 GewO darf die Gewerbebehörde nämlich anderen öffentlichen Stellen *fallweise* Namen des Gewerbetreibenden, betriebliche Anschrift und die angezeigte Tätigkeit übermitteln, soweit dies zur Aufgabenerfüllung des Datenempfängers erforderlich ist. Weitere Daten (hier die Staatsangehörigkeit) aus der Gewerbeanzeige dürfen nur übermittelt werden, wenn

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

§ 14 Abs. 9 GewO erlaubt darüber hinaus weitere Datenübermittlungen für andere Zwecke nur, wenn die Kenntnis der zu übermittelnden Daten zur *Verfolgung* von Straftaten erforderlich ist oder eine besondere Rechtsvorschrift dies vorsieht.

Argumenten des von mir um eine Stellungnahme gebetenen Landeskriminalamtes, daß die Datenerhebung über ausländische Gewerbetreibende in erster Linie zur *vorbeugenden* Bekämpfung von Straftaten und insbesondere für die Erarbeitung polizeilicher Einsatz- und Präventionskonzepte erforderlich und deshalb gemäß § 37 Abs. 1 und Abs. 3 Nr. 1 SächsPolG i. V. m. § 14 Abs. 6 GewO zulässig sei, konnte ich mich nicht anschließen.

Eine Datenerhebung nach § 14 Abs. 6 Satz 2 Nr. 1, 2. Fall GewO setzt nämlich außer dem Vorliegen einer *fallweisen* - also einzelfallbezogenen - Übermittlung das Vorliegen einer *unmittelbar drohenden Gefahr* für die öffentliche Sicherheit voraus.
Eine *Gefahr* liegt vor, wenn nach den gegebenen Tatsachen in naher Zukunft eine Störung der öffentlichen Sicherheit und Ordnung zu befürchten ist, nicht aber, wenn

nach bloßen Vermutungen die entfernte Möglichkeit eines schädigenden Ereignisses gegeben ist (BVerfGE 87, 399, 409; VGH Mannheim NVwZ 1994, 88; BayVGH BayVBl. 1964, 220, 230). Ferner muß die Gefahr *unmittelbar bevorstehen*. Dies setzt voraus, daß die Gefahr *akut* ist, d. h. der Eintritt des Schadens muß sofort und fast mit Gewißheit zu erwarten sein (Wolff/Bachof, Verwaltungsrecht III, § 125 Rdnr. 29; ebenso VG Bremen NVwZ 1989, 895, 897).
Der Stellungnahme des LKA war nicht zu entnehmen, daß bei allen ausländischen Gewerbetreibenden eine solche unmittelbare Gefahr bevorsteht bzw. eine akute Gefährdungssituation eingetreten ist. Die erhobenen Daten sollen vielmehr der Erstellung von Lagebildern dienen, deren Analyse der Polizeiführung die Entwicklung von entsprechenden Einsatzkonzeptionen ermöglichen soll. Auch die allgemeine Aufzählung von bundesweiten Brandanschlägen auf türkische Einrichtungen begründet nicht das Vorliegen einer unmittelbar drohenden Gefahr für die betreffenden Bevölkerungsgruppen. Dies gilt auch für den Fall, daß in Sachsen in mehreren Verfahren ermittelt wird, bei denen ein Bezug zur PKK lediglich denkbar ist. Auch die Ermittlungen seitens des LKA in *einem* Fall gegen einen algerischen Staatsangehörigen, der im Verdacht stehen soll, mit der Islamischen Heilsfront (FIS) zusammengearbeitet zu haben, rechtfertigt eine umfassende Datenerhebung über alle algerischen Gewerbetreibenden nicht (Übermaßverbot).

Auch die Voraussetzungen der ersten Variante des § 14 Abs. 6 Satz 2 Nr. 1 GewO - die Abwehr erheblicher Nachteile für das Gemeinwohl - liegen nicht vor.
Ein erheblicher Nachteil für das Gemeinwohl setzt immer voraus, daß der Grad der Beeinträchtigung so intensiv ist, daß nicht nur Nachteile, sondern konkrete Schäden zu befürchten sind. Daß dieser Intensitätsgrad hier erreicht wurde, wurde durch allgemeine Hinweise auf "potentielle Gefahren für die deutsche Außenpolitik, Belastung bilateraler/multilateraler Beziehungen" jedenfalls nicht nachvollziehbar ausreichend dargelegt.

Ich habe deshalb nochmals betont, daß allgemeine präventive Maßnahmen eine Datenübermittlung nicht rechtfertigen, und auf die Verpflichtung der Polizei zur Datenlöschung hingewiesen (§ 49 SächsPolG i. V. m. § 19 Abs. 1 Nr. 1 SächsDSG).

Jeder ausländische Gewerbetreibende, der sich konkret bedroht fühlt, kann sich selbstverständlich schutzsuchend an die Polizei wenden.

9.3 Industrie- und Handelskammern; Handwerkskammern

9.3.1 Einstellung von Handelsregisterdaten durch die Industrie- und Handelskammern in das Internet

In einem anderen Bundesland beabsichtigte eine Industrie- und Handelskammer Handelsregisterdaten in das Internet einzustellen. Eine solche Maßnahme käme einem bundesweiten Handelsregister gleich. Solche Bemühungen hat der BGH bereits früher für unzulässig erklärt (Beschl. v. 12.7.1989, NJW 1989, 2818), weil der durch § 9 HGB vorgegebene Rahmen (einzelfallbezogene Einsichtnahme ins Handelsregister) gesprengt würde.

Auf meine Anfrage beim SMWA wurde mitgeteilt, daß die sächsischen Industrie- und Handelskammern derzeit nicht beabsichtigen, Handelsregisterdaten ins Internet einzustellen. Das ist gut so!

9.3.2 Übermittlung personenbezogener Daten durch die Industrie- und Handelskammern an die Zentrale zur Bekämpfung unlauteren Wettbewerbs e. V. Frankfurt am Main

Die "Wettbewerbszentrale", wie sie kurz genannt wird, wurde bereits 1912 von Berliner Kaufleuten als Verband i. S. v. § 13 Abs. 2 UWG gegründet und hat heute mehr als 1.300 Mitglieder, darunter sämtliche Industrie- und Handelskammern. Die Wettbewerbszentrale kann im Zusammenhang mit Verstößen gegen das UWG selbständig Unterlassungs- und Schadensersatzansprüche geltend machen und ist klagebefugt. Etwa 700 Wettbewerbsverfahren werden von ihr jährlich gerichtlich anhängig gemacht; ihre Erfolgsquote liegt seit Jahrzehnten bei etwa 90 % (gewonnene Prozesse).

Die Industrie- und Handelskammern sind zwar nach § 13 Abs. 2 Nr. 4 UWG ebenfalls zu vorstehenden Maßnahmen befugt; sie bedienen sich jedoch in aller Regel der in Fragen des unlauteren Wettbewerbes überaus erfahrenen Wettbewerbszentrale. Hierzu übermitteln die Industrie- und Handelskammern der Wettbewerbszentrale Namen und Anschriften derjenigen Gewerbetreibenden, bei denen ein Verstoß gegen das UWG vermutet wird. Außerdem werden diejenigen Tatsachen mitgeteilt, die den Verdacht eines Wettbewerbsverstoßes begründen sollen (z. B. Zeitungsanzeigen, Werbeblätter, Rundfunk- und Fernsehwerbung, aber auch Briefköpfe, Rabatte, Vertragsbedingungen).

Die Frage der Zulässigkeit solcher Datenübermittlungen wird gegenwärtig bundesweit mit unterschiedlichen Tendenzen erörtert. Das SMWA neigt dazu, von der Zulässigkeit der Datenübermittlungen, zumindest soweit es sich um Kammerzugehörige handelt, auszugehen.

Nach § 9 Abs. 4 IHK-Gesetz dürfen die Industrie- und Handelskammern zwar Name,

Firma, Anschrift und Wirtschaftszweig ihrer Kammerzugehörigen u. a. zu dem Wirtschaftsverkehr dienenden Zwecken an nichtöffentliche Stellen übermitteln (hier an die Wettbewerbszentrale). Ob dieser Übermittlung weiteres Material beigefügt werden darf, ist jedoch fraglich.

Ich unterstütze zwar grundsätzlich die Bekämpfung des unlauteren Wettbewerbs, gebe aber folgendes zu bedenken: Das Wettbewerbsrecht verbietet z. B. in §§ 1 und 3 UWG "sittenwidrige" Wettbewerbshandlungen und "irreführende Angaben", ohne diese Begriffe gesetzlich näher zu definieren. In den letzten Jahrzehnten ist dazu eine schier unübersehbare und für den einzelnen (kleinen) Marktteilnehmer kaum vorhersehbare Einzelfall-Rechtsprechung entstanden. Die Wettbewerbszentrale beschäftigt Spezialjuristen, die - auch aus wirtschaftlichen Gründen - vertragsstrafebewehrte Unterlassungserklärungen und Urteile erstreiten, die aus der Sicht der ihnen unterlegenen Gewerbetreibenden nicht nur positive Wirkungen auf einen fairen Wettbewerb haben. Werden von den Kammern nun Personalien zum Zwecke der Abmahnung und Prozeßführung an die Wettbewerbszentrale übermittelt - gleichgültig, ob auf deren Wunsch oder aus eigener Initiative - so werden diese Daten in einen ersichtlichen Zusammenhang mit Wettbewerbshandlungen - mögen diese auch teilöffentlich sein - gebracht. Die damit verbundene datenschutzrechtliche Problematik ist noch in der Diskussion.

Werden nicht nur Personalien i. S. d. § 9 Abs. 4 Satz 1 IHK-Gesetz, sondern damit verbunden außerdem die "den Verstoß begründenden Tatsachen" - so das SMWA - an die Wettbewerbszentrale übermittelt, so findet das im Gesetz keine Stütze. Die Kammern täten gut daran - zumal sie die gesetzliche Aufgabe haben, ihre Mitglieder zunächst zu beraten -, solche Daten nur im begründeten Ausnahmefall an die Wettbewerbszentrale zu melden, wenn andere Maßnahmen der Aufklärung, Beratung und Abmahnung erfolglos bleiben. So jedenfalls interpretiere ich den Grundsatz der Verhältnismäßigkeit.

9.4 Offene Vermögensfragen

9.4.1 Darf die GVO-Behörde dem Restitutionsantragsteller die Identität des Erwerbers bekannt geben?

(1) Eine kreisfreie Stadt wollte ein Grundstück veräußern, dessen Rückübertragung nach dem VermG von den Erben der seinerzeit Enteigneten beim LARoV beantragt war. Nach § 2 Abs. 1 GVO bedurfte das Rechtsgeschäft der Genehmigung. Zuständige Behörde zur Erteilung der Genehmigung war gemäß § 8 Abs. 1, 2. Fall GVO die Stadt selbst.

In ihrer Eigenschaft als GVO-Behörde bat die Stadt die Anmelder des (angeblichen) vermögensrechtlichen Anspruches, durch eine Zustimmung zur Genehmigung nach § 1 Abs. 2 Satz 1 Nr. 2 GVO den Weg für die Eigentumsübertragung frei zu machen. Eine

solche Zustimmung könne ohne Schaden erklärt werden, weil die Anspruchsanmelder im Falle eines für sie erfolgreichen Ausganges des vermögensrechtlichen Verwaltungsverfahrens einen Anspruch auf Auskehrung des Veräußerungserlöses hätten (vgl. auch § 1 Abs. 2 Satz 3 GVO). Wenn sie dazu nicht bereit seien, hätten die Anspruchsanmelder Gelegenheit, zu der Absicht der Behörde Stellung zu nehmen, die Genehmigung statt dessen dann - nach § 1 Abs. 2 Satz 2 GVO - deswegen zu erteilen, weil der nach § 30 Abs. 1 VermG gestellte Antrag als offensichtlich unbegründet erscheine.

Die Anmelder des vermögensrechtlichen Anspruches wollten vor ihrer Entscheidung, ob sie die Zustimmung erteilten oder verweigerten, wissen, wer das Grundstück erwerben und was er mit dem Grundstück machen wolle. Als die Stadt in ihrer Eigenschaft als GVO-Behörde diese Auskunft unter Berufung auf Datenschutzrecht verweigerte, die Restitutionsantragsteller darauf jedoch erwiderten, die Berufung auf Datenschutz sei lediglich vorgeschoben, wandte sich die Stadt an mich.
Ich mußte ihr antworten, daß sie als GVO-Behörde nicht durch Datenschutzrecht gehindert war, den Namen und die Anschrift des Erwerbers den Anspruchsanmeldern mitzuteilen. Die Gründe waren folgende:

(2) Die Restitutionsantragsteller waren Beteiligte des von der GVO-Behörde durchzuführenden Verwaltungsverfahrens (wenn nicht nach § 13 Abs. 1 Nr. 1 VwVfG als Antragsgegner, so doch jedenfalls nach § 13 Abs. 1 Nr. 4 i. V. m. Abs. 2 Satz 2 VwVfG). Deswegen hatte ihnen die GVO-Behörde ja auch Gelegenheit zur Stellungnahme gegeben, also rechtliches Gehör gewährt. Als Verfahrensbeteiligte hatten die Restitutionsantragsteller nach § 29 Abs. 1 Satz 1 VwVfG Anspruch auf Akteneinsicht, soweit die Kenntnis des Akteninhalts für die Rechtsverfolgung im Verfahren erforderlich war.

Für das Bestehen des Anspruchs auf Akteneinsicht reicht es aus, daß das geltend gemachte rechtliche Interesse bei überschlägiger Prüfung nicht offensichtlich rechtsmißbräuchlich wahrgenommen wird und ohne die Akteneinsicht - hier die Kenntnisgabe der Identität des Erwerbers - eine Beeinträchtigung rechtlicher Interessen möglich ist; es ist nicht etwa notwendig, daß diese Beeinträchtigung als sicher oder auch nur wahrscheinlich erscheinen muß (vgl. Stelkens/Bonk/Sachs Rdnr. 33 zu § 29 VwVfG, mit Nachweisen aus der Rechtsprechung).

Diese den Informationszugang, d. h. zugleich die Übermittlung personenbezogener Daten durch die Behörde an Private regelnde Vorschrift des VwVfG genießt gegenüber § 15 SächsDSG Spezialitätsvorrang (vgl. § 2 Abs. 4 Satz 1 SächsDSG).

Das Akteneinsichtsrecht nach dem VwVfG ist auch verfassungsrechtlich begründet: Es ist eine Form des rechtlichen Gehörs und Ausdruck des Grundrechts der freien Entfaltung der Persönlichkeit gemäß Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG (vgl. Knack-Clausen Rdnr. 3 und Kopp Rdnr. 2 zu § 29 VwVfG, jeweils unter Hinweis auf die Entscheidung BayVGH NVwZ 1990, 775). § 29 VwVfG soll die Transparenz der

Entscheidungsgrundlagen erhöhen und damit verhindern, daß der Beteiligte zum bloßen Objekt behördlichen Handelns gemacht wird. Als Ausdruck der Parteiöffentlichkeit des Verfahrens ist das Recht auf Akteneinsicht aus der Menschenwürde und dem Rechtsstaatsprinzip abgeleitet (Stelkens/Bonk/Sachs Rdnr. 3 zu § 29 VwVfG).

(Im Grunde genommen könnte man für das Ergebnis sogar auf dem Boden des allgemeinen Datenschutzrechts argumentieren: In das Verwaltungsverfahren als für dessen Durchführung zweckdienlich einbezogene personenbezogene Daten sind Daten sämtlicher durch die Beteiligung am Verwaltungsverfahren verbundener Personen, selbst wenn sie sich vordergründig nur auf eine von ihnen beziehen. Es sind Daten mit Mehrfachbezug. Damit bleibt man im Rahmen der Legaldefinitionen in § 3 Abs. 1 und Abs. 2 Nr. 4 SächsDSG.)

(3) Was nun die im vorliegenden Falle gewünschte Information betrifft, so gehört zu den Gegenständen, deren Kenntnis für die Rechtsverfolgung im Verfahren wichtig ist, sicher auch die Kenntnis der Identität eines tatsächlichen oder potentiellen anderen Verfahrensbeteiligten. Mit der Kenntnis der Identität anderer Verfahrensbeteiligter ausgestattet kann man, ggf. mit Hilfe von Zusatzwissen, sein Verhalten im Verwaltungsverfahren besser steuern. Wem als Verfahrensbeteiligtem vorenthalten wird, wer die anderen Verfahrensbeteiligten sind, der ist in seiner Möglichkeit, als Subjekt des Verfahrens gegenüber anderen Subjekten sein Handeln einzurichten, in einer nach dem Maßstab des fairen rechtsstaatlichen Verfahrens unangemessenen Weise eingeschränkt.

Hinzu kam im vorliegenden Fall, daß die Behörde durch den Hinweis auf einen möglichen Erlösherausgabeanspruch die Frage von dessen ggf. bestehender Werthaltigkeit in das Verwaltungsverfahren eingebracht hatte. Die Wahrscheinlichkeit, einen (Bereicherungs-) Anspruch auf Erlösherausgabe bei der Stadt realisieren zu können, ließ sich aber nicht ohne Beurteilung der Bonität des Erwerbers zutreffend einschätzen.

Schließlich ist aus der Sicht der Alteigentümer - das lehrt nun in den neuen Bundesländern leider manche Erfahrung - nicht auszuschließen, daß eine Gemeinde Grundstücke "noch schnell verkungelt", um sie nicht zurückgeben zu müssen, folglich ein Verkauf unter Wert stattfindet. Davon konnte zwar im vorliegenden Fall keine Rede sein. Jedoch soll die Kenntnis von der Person des Erwerbers solchen Verdacht gerade ausschließen. In den Fällen, in denen wie hier die entscheidende Behörde rechtlich identisch mit einem der Verfahrensbeteiligten (Grundstücksveräußerer) ist, muß ein großzügiger Maßstab gelten, um für die verfassungsrechtlich gebotene "Waffengleichheit" des Privaten im Verhältnis zur Behörde (vgl. Stelkens/Bonk/Sachs a.a.O.) zugunsten privater Verfahrensbeteiligter zu sorgen.

9.4.2 Zugang zu Auskünften der Gauck-Behörde im vermögensrechtlichen Verwaltungsverfahren

Ein ARoV hatte getan, was im Hinblick auf die Anspruchsbegründung nach § 1 Abs. 3 VermG oder auch im Hinblick auf den Anspruchsausschluß gemäß § 4 Abs. 2 Satz 1 VermG oft geschieht: Es hatte eine Auskunft des BStU eingeholt. Das Besondere war jedoch, daß in diesem ARoV die Übung galt, daß diese Auskunft nur dem Amtsleiter selbst zur Kenntnis gelangte, welcher dann dem sachbearbeitenden Bediensteten lediglich mitteilte, was aus der Auskunft für die Fallentscheidung folge - also das Vorliegen einer Machenschaft oder aber Redlichkeit beim Erwerb. Dementsprechend war die Auskunft des BStU in einem auch für den Sachbearbeiter verschlossenen Umschlag zur Akte genommen worden. Da war es einigermaßen folgerichtig, daß das betreffende ARoV den Verfahrensbeteiligten zwar mitteilte, welche Auswirkung es der Auskunft der Gauck-Behörde auf die beabsichtigte Entscheidung zukommen lassen wolle, die Auskunft selbst jedoch nicht zugänglich machen wollte. In dieser Weise verfuhr das Amt insbesondere auch im Abhilfeverfahren (§ 36 Abs. 1 Satz 4 VermG) und sogar auch noch, nachdem ihr eine Stellungnahme des BStU zugegangen war, aus der eindeutig hervorging, daß der BStU eine Weitergabe der von ihm dem ARoV gemachten Mitteilung "an die Verfahrensbeteiligten, die gemäß § 31 Abs. 2 und 3 VermG bei der Ermittlung des Sachverhaltes von Amts wegen mitzuwirken haben bzw. hinzuzuziehen sind" für nach dem StUG zulässig hielt.

Der Akteneinsichtsanspruch der Verfahrensbeteiligten gemäß § 29 Abs. 1 Satz 1 VwVfG (dazu ausführlicher vorstehend unter 9.4.1) gilt auch für den Teil der Verfahrens-Unterlagen (Akte), der vom BStU stammt. Der Akteneinsichtsanspruch ist auch nicht durch die Vorschrift des § 29 Abs. 2 VwVfG ausgeschlossen, der zufolge ausnahmsweise die ganze Akte oder einzelne ihrer Teile wegen der berechtigten Interessen der Beteiligten oder dritter Personen doch geheimzuhalten sind. In der Regel sind Beziehungen, welche Verfahrensbeteiligte oder deren Rechtsvorgänger zur Staatssicherheit gehabt haben, nach dem Vermögensgesetz gerade nicht 'Privatsache', sondern sie gehen in den Verfahrensgegenstand ein. Eine Ausnahme ist dann anzunehmen, wenn sich statt des Täter- bzw. Begünstigten-Verdachtes ergibt, daß die betreffende Person *Opfer* des MfS gewesen ist und daß die diesen Umstand nachweisenden Unterlagen Informationen aus dem Intimbereich des Betreffenden enthalten. An solchen Einzelheiten haben die (anderen) Beteiligten des Verfahrens kein berechtigtes Interesse, wenn aus den Unterlagen deutlich erkennbar ist, daß keinerlei Hinweise auf eine Systemnähe bestehen, die zum Erwerb von Vermögenswerten hätten ausgenutzt werden können. Da diese Einzelheiten, wenn sie denn vom BStU mitgeteilt worden sein sollten, auch von der Behörde selbst nicht benötigt werden, sähe ich in solchen Fällen kein Hindernis, daß die Behörde diese Einzelheiten in ihrer Originalakte selbst schwärzt - allerdings mit großer Vorsicht, weil jede nur mögliche rechtliche Betrachtungsweise im Rahmen des vermögensrechtlichen Verfahrens berücksichtigt werden muß und nicht präjudiziert werden darf.

Ich hielt es für sinnvoll, wenn dies ggf. zugunsten von Rechtsnachfolgern, meist

Abkömmlingen, auch bei solchen Daten geschieht, die sich auf bereits verstorbene Rechtsvorgänger beziehen.

Keine Grundlage für eine Einschränkung des Akteneinsichtsrechts aus § 29 Abs. 1 Satz 1 VwVfG ist entgegen der von dem betreffenden ARoV geäußerten Ansicht § 31 Abs. 3 Satz 1 VermG, der dem Antragsteller auf Verlangen einen Anspruch auf Auskunft der Behörde über alle Informationen gewährt, die zur Durchsetzung des Anspruchs erforderlich sind. Der Sinn dieser Vorschrift ist nicht etwa eine Einengung des nach allgemeinem Verwaltungsverfahrensrecht bestehenden Akteneinsichtsrechtes Beteiligter. Vielmehr soll die Regelung die Rechte des Antragstellers gegenüber dem Verwaltungsverfahrensrecht erweitern und nicht einschränken (allgemeine Ansicht, besonders deutlich Rädler/Raupach/Bezzenberger-Denes Rdnr. 40 zu § 31 VermG, insbesondere auch die Auffassung des LARoV Sachsen).

Folglich hat das ARoV die Verfahrensregeln verletzt; jeder Beteiligte hat das Recht, die Auskunft des BStU in ihrem gesamten Inhalt zur Kenntnis zu erhalten.

9.5 Sonstiges

9.5.1 Ausbildungskarte 1996 und 1997 im Freistaat Sachsen

Mit der Einführung einer Ausbildungskarte, die jeder Schulabgänger erhält, ist beabsichtigt, dem Lehrstellenmangel im Freistaat zu begegnen. Eine Nachfrage beim SMWA ergab, daß für sämtliche mit der Ausbildungskarte zusammenhängenden Datenverarbeitungsschritte (Erhebung, Speicherung, Übermittlung) das private Institut für Wirtschafts- und Sozialforschung e. V. WISOC in Chemnitz verantwortlich sei. Seinerzeit ging ich davon aus, daß meine Zuständigkeit nicht gegeben sei.

Durch die Bekanntmachung des Sächsischen Staatsministeriums des Innern über die Ausbildungskarte 1996 im Freistaat Sachsen vom 23. Mai 1996 (SächsABl. S. 561) bekam die Angelegenheit einen amtlichen Anstrich. Dem SMI teilte ich deshalb im Hinblick auf die Bekanntmachung meine vorläufige datenschutzrechtliche Einschätzung mit.

Auf der Ausbildungskarte 1996 werden nämlich personenbezogene Daten des Bewerbers und des Ausbildenden eingetragen, die schließlich (vom Bewerber) an das Arbeitsamt, Abteilung Berufsberatung, zu übermitteln sind, ohne daß hierfür eine Rechtsgrundlage ersichtlich ist. Auch Regelungen über die Freiwilligkeit an der Teilnahme sowie über Einwilligungen in die Datenverarbeitung sind nicht zu erkennen. Das gilt auch für die wohl beabsichtigte Weitergabe der Ausbildungskarten an das (private) Institut für Wirtschafts- und Sozialforschung e. V. WISOC in Chemnitz, wo die Auswertung der Karten erfolgen soll. Das vom SMI veröffentlichte Informationsblatt macht dabei nicht transparent, *woher* WISOC die Karten erhält und was dort mit den so erhaltenen Daten geschieht.

Nach § 4 SächsDSG ist die Verarbeitung personenbezogener Daten nur zulässig, wenn es das SächsDSG selbst oder eine andere Rechtsvorschrift erlaubt oder wenn der Betroffene eingewilligt hat. Deshalb erbat ich eine Stellungnahme in der mir auch das Auftragsverhältnis mit WISOC (§ 7 oder § 2 Abs. 2 SächsDSG) näher erläutert werden sollte.

Erst im Februar 1997 erfuhr ich vom SMI, daß man meine Anfrage zuständigkeitshalber ans SMWA abgegeben habe. Dorthin wandte ich mich, nachdem Anfragen aus der Bevölkerung zur Rechtmäßigkeit der Ausbildungskarte 1997 offensichtlich auf Irritationen hindeuteten. Bemängelt wurde von den Petenten, daß weder ein Hinweis auf eine verpflichtende Rechtsgrundlage noch auf die Freiwilligkeit ersichtlich sei.

Dem SMWA gegenüber habe ich darauf gedrungen, daß entgegen der Bekanntmachung des SMI über die Ausbildungskarte 1996 im Freistaat Sachsen die Ausbildungskarte 1997 nicht mehr wie bisher der Abteilung Berufsberatung des zuständigen Arbeitsamtes übersandt werden, sondern unmittelbar der WISOC, wo die Daten statistisch ausgewertet werden (bisher bin ich davon ausgegangen, daß der Jugendliche beim zuständigen Arbeitsamt als vermittelt registriert wird und daß danach eine anonyme Mitteilung vom Arbeitsamt an die WISOC erfolgt). Da auf diese Weise eine Fülle personenbezogener Daten betroffener Jugendlicher an die WISOC gelangen und über den Verbleib dieser Daten nichts bekannt ist, bat ich um Stellungnahme zu den am Verfahren beteiligten Stellen, zu deren gesetzlicher Legitimation zur Datenverarbeitung und zum Auftragsverhältnis mit der WISOC und zu der dortigen Datenverarbeitung.

Das SMWA hat erwidert, daß die Freiwilligkeit der Teilnahme - nach dortigem Verständnis - hinreichend durch entsprechende Hinweise in einschlägigen Kammerzeitschriften und dadurch gewährleistet sei, daß weder das Hinweisblatt für die Jugendlichen noch das Merkblatt der Ausbildungsbetriebe auf eine *Verpflichtung* zur Rücksendung schließen lasse. Eine Rücklaufquote von 21 % sei eindeutiges Indiz dafür, daß die Betroffenen die Aktion als "freiwillig" aufgefaßt hätten. Daß dem nicht so ist, beweisen die Eingaben besorger Eltern. Auch scheint mir, daß der Stellungnahme des SMWA die wesentlichen Grundsätze des Grundrechts nach Art. 33 der Sächsischen Verfassung fremd sind, so daß mich die Frage der Rechtmäßigkeit der Ausbildungskarte noch weiter beschäftigen wird.

9.5.2 Planfeststellung: Veröffentlichung personenbezogener Daten in Planfeststellungsverfahren

Zwischen den Landesbeauftragten und dem Bundesbeauftragten für den Datenschutz findet derzeit ein Meinungsaustausch statt, ob bei der Planveröffentlichung nach den Verwaltungsverfahrensgesetzen ein Grundstücksverzeichnis mit Namen, Vornamen und Anschrift der Grundstückseigentümer ausgelegt werden darf. Als Hauptargument

für die (personenbezogene) Auslegung von Grundstücksverzeichnissen wird vorgetragen, daß nur in diesem Fall das Einwendungsverfahren "praktikabel" durchgeführt werden könne. Dem SMWA, das über den Meinungsaustausch informiert wurde, habe ich mitgeteilt, daß ich dieses Argument nicht für überzeugend halte (vgl. 4. Tätigkeitsbericht unter 9.5):

Das Bundesverfassungsgericht hat in seinen Beschlüssen vom 14. Oktober 1987 (NJW 1988, 403) und vom 24. Juli 1990 (CR 1990, 798) festgestellt, daß es für eine ordnungsgemäße Begründung des Planfeststellungsbeschlusses genüge, daß die Einwendungen sachbezogen (und nicht *personenbezogen*) in die Begründung aufgenommen und mit dieser veröffentlicht werden. Ein Grund, warum die vorhergehende Phase der Planauslegung personenbezogen erfolgen soll, ist mir nicht ersichtlich. Insbesondere ist nicht nachvollziehbar, weshalb die Kenntnis der Eigentumsverhältnisse bei der Prüfung helfen soll (Stichwort: Praktikabilität), daß im Anhörungsverfahren erfolgreich Einwendungen erhoben werden können. In diesem Sinne hat bereits das Verwaltungsgericht München mit Beschluß vom 13.2.1980 - M 362 VII (also gut drei Jahre vor dem Volkszählungsurteil) entschieden und hervorgehoben, daß personenbezogene Angaben zu Grundstückseigentümern in öffentlichen Planungsunterlagen nicht erforderlich sind und dies als Verstoß gegen den Grundsatz der Gesetzmäßigkeit der Verwaltung bezeichnet.

Daher halte ich Bestrebungen in anderen Bundesländern, eine dem Paragraphen 73 Abs. 1 Satz 2 des baden-württembergischen Verwaltungsverfahrensgesetzes vergleichbare Vorschrift zu erlassen, wonach der Plan "Namen und Anschriften der betroffenen Eigentümer erkennen lassen" muß, für nicht mit dem Volkszählungsurteil (BVerfGE 65, 1 ff.) vereinbar: Einschränkungen des Grundrechts auf informationelle Selbstbestimmung sind hiernach nur durch oder aufgrund von Gesetzen zulässig, die dem Grundsatz der Verhältnismäßigkeit entsprechen. D. h. die (einschränkenden) Gesetze müssen - gemessen am Gesetzeszweck - geeignet, *erforderlich* und angemessen sein. Das Veröffentlichen personenbezogener Gundstücksverzeichnisse bei der Planauslegung ist jedoch - wie dargestellt - nach meiner bisherigen, von der Rechtsprechung gestützten Auffassung *nicht erforderlich*. Wenn wirklich überzeugende Argumente vorgetragen werden, daß personenbezogene Daten zur gerechten und schnellen Verfahrensabwicklung nötig sind, bin ich gern bereit, meinen Standpunkt zu ändern.

10 Soziales und Gesundheit

10.1 Gesundheitswesen

10.1.1 Sächsisches Ausführungsgesetz zum Krebsregistergesetz des Bundes; Staatsvertrag über das Gemeinsame Krebsregister

Am 6. März 1997 hat der Landtag das Sächsische Ausführungsgesetz zu dem am 1. Januar 1995 in Kraft getretenen Krebsregistergesetz des Bundes (KRG) verabschiedet (Sächsisches Krebsregistergesetz - SächsKRGAG; GVBl. S. 352).

Ich habe mich an der Erarbeitung des Gesetzes beteiligt. Die Gründe, warum ich mich - oft genug gegen den Widerstand meiner Kollegen aus den anderen Ländern sowie zeitweilig aus den Reihen der Sächsischen Staatsministerien des Innern und der Justiz - stets für die widerspruchsunabhängige Meldepflicht der Ärzte eingesetzt habe, die nunmehr Gesetz geworden ist, habe ich in meinen bisherigen Tätigkeitsberichten ausführlich dargelegt. Nach den bisherigen Erfahrungen ist nur eine solche widerspruchsunabhängige Meldepflicht der Ärzte geeignet, den erforderlichen hohen Vollständigkeitsgrad des Registers und damit dessen Funktion für die Gesundheits- und Umweltpolitik - der breiteren Öffentlichkeit sind Studien zum Vorkommen von Leukämie in der Umgebung kerntechnischer Anlagen bekannt - sowie für die medizinische Forschung zu gewährleisten. Zugleich befreit die widerspruchsunabhängige Meldepflicht den Arzt davon, in das Gespräch mit dem Patienten, der ohnehin mit seiner Krankheit schwer belastet ist, noch das Thema der Registrierung seines Falles zu epidemiologischen Zwecken hineinzutragen. Datenschutz ist, wie an diesem Beispiel klar wird, nicht der einzige Inhalt des Persönlichkeitsrechts.

Die Entscheidung für die widerspruchsunabhängige Meldepflicht konnte bei diesem zweiten Sächsischen Ausführungsgesetz zum Krebsregisterrecht des Bundes deswegen leichter fallen, weil das neue Krebsregistergesetz des Bundes für eine organisatorische Vorkehrung gesorgt hat, für die ich mich ebenfalls, und zwar sehr früh, eingesetzt habe: Das Krebsregister ist aufgeteilt in eine Vertrauensstelle - die die Namen der Patienten hat - und eine Registerstelle, bei der die medizinischen Daten epidemiologisch ausgewertet werden.

Ich hoffe - und bin überzeugt -, daß auch andere Bundesländer Sachsen auf diesem Weg folgen werden, zumal andere freiheitlich organisierte Staaten ebenfalls eine Meldepflicht eingeführt haben.

Ferner habe ich mich an den Vorarbeiten für einen Staatsvertrag über das Gemeinsame Krebsregister der sechs östlichen Bundesländer beteiligt, mit dem das DDR-Krebsregister fortgeführt wird. In diesen Staatsvertrag sollten auch alle Klauseln eingebaut werden, die nötig sind, damit die von Sachsen gewählten Besonderheiten,

also die widerspruchsunabhängige Meldepflicht, soweit sächsische Daten betroffen sind, für das Gemeinsame Krebsregister, das rechtlich als eine dem Berliner Landesrecht unterstehende Stelle ausgestaltet ist, uneingeschränkt verbindlich werden. Dazu gehört auch, daß Sachsen einen Anspruch auf Überlassung seiner Daten erhält, z. B. weil die "sächsischen Daten" besonders vollständig und damit besonders wertvoll für die (Fort-)Führung eines eigenständigen Registers sind, oder weil sie Gegenstand spezieller Forschungen werden sollen. Auf die vertragliche Absicherung eines solchen Anspruches zu dringen werde ich nicht nachlassen.

10.1.2 Klinische Krebsregister (Tumorzentren)

Ärzte und Zahnärzte können Klinikregister und Nachsorgeleitstellen damit beauftragen, die Pflichtmeldungen über Krebserkrankungen in das Krebsregister in Berlin in ihrem Auftrag durchzuführen. Diese Stellen werden also zwischen die Ärzte und das Krebsregister geschaltet. Sie dürfen grundsätzlich die Daten nur weiterleiten und nicht für eigene Zwecke verwenden, es sei denn, der Patient hat freiwillig und ausdrücklich in eine solche Datenverarbeitung in den Klinikregistern und Nachsorgeleitstellen eingewilligt. Da dort weder bestimmte beabsichtigte Maßnahmen der Qualitätssicherungen noch ein bestimmtes Forschungsvorhaben Voraussetzung für die Datensammlung ist, sondern tatsächlich eine Datensammlung auf Vorrat angelegt wird, können weder § 33 Abs. 4 Nr. 4 noch § 34 Abs. 3 Nr. 1 SächsKHG eine einwilligungsunabhängige Datenübermittlung dorthin begründen.

Die Klinikregister und Nachsorgeleitstellen sehen ihre Aufgabe nicht in der bloßen Mittler- und Weiterleitungsfunktion, sondern wollen selbst kleine epidemiologische Krebsregister anlegen und entsprechende Forschung betreiben. Sie müssen wissen, daß sie ausschließlich auf der Grundlage einer zivilrechtlich, strafrechtlich und öffentlich-rechtlich wirksamen Einwilligung arbeiten dürfen. Darauf habe ich die fünf Tumorzentren, die es in Sachsen gibt, nachdrücklich hingewiesen. Im Auftrag des Tumorzentrums Dresden hat das Institut für medizinische Informatik und Biometrie am Universitätsklinikum der TU Dresden die notwendigen einheitlichen Vordrucksätze für die Meldungen der Ärzte an die Tumorzentren auf der Grundlage wirksamer Einwilligungen des jeweiligen Patienten unter meiner Mitwirkung erarbeitet. Dabei wurde deutlich, daß das Sächsische Krebsregistergesetz mit seiner widerspruchsunabhängigen Meldepflicht die praktische Handhabung der Verfahren wesentlich erleichtert.

Über die Möglichkeit, mit ausdrücklicher Einwilligung des Patienten (nach sorgfältiger Belehrung über Art, Umfang und späteren Verwendungszweck der Daten) also auch kleine klinische Krebsregister zu unterhalten, bin ich nicht besonders glücklich: Ich stelle mir die Belehrungsgespräche zwischen Arzt und Patient als belastend und für den Patienten auch verwirrend vor. Natürlich stellen die Apologeten der Klinikregister das in Abrede.

Mit diesem Beispiel läßt sich wieder einmal begründen, daß eine naheliegende

fachwissenschaftliche Auswertung von Daten - mit Ausnahme etwa besonders wenig valider oder wirklich intimer Daten - bei strenger Zweckbindung und frühestmöglicher Anonymisierung ohne Einwilligung der Betroffenen möglich werden sollte. Entsprechende Vorschläge für eine Novellierung des Sächsischen Datenschutzgesetzes erarbeite ich. Der Wissenschaftsstandort Deutschland darf nicht unter bürokratischem Datenschutz leiden.

10.1.3 Dienstanweisungen für den Datenschutz in Krankenhäusern

Mit den Mindestanforderungen, die eine Dienstanweisung für den Datenschutz im Krankenhaus erfüllen sollte, habe ich mich in meinem 4. Tätigkeitsbericht (10.1.5) beschäftigt. Enthielt der damals von mir zu bewertende Entwurf kaum Hinweise für den Umgang mit Patientendaten, hatte ich diesmal einen Entwurf zu bewerten, der auf mehr als 50 Seiten den allgemeinen Datenschutz im Krankenhaus abhandelte. Ich habe angeregt, diesen sicher in bester Absicht erstellten Entwurf stark zu kürzen, weil zu umfangreiche, dazu in der Art eines Kommentars abgefaßte Dienstanweisungen für die Praxis ungeeignet sind. Hinzu kommt der Lesewiderstand, den Beschäftigte angesichts eines datenschutzrechtlichen "Gesamtwerks" zu überwinden haben.

Eine Dienstanweisung sollte nicht die Überlegungen, Begründungen oder sogar die Rechtsprechung wiedergeben, die zu den getroffenen Regelungen geführt haben. Sie sollte in einem allgemeinen Teil die datenschutzrechtliche Grundbegriffe erläutern (z. B. personenbezogene Daten, Patientendaten) und auf die zu beachtenden Gesetze, Rechtsverordnungen und Verwaltungsvorschriften hinweisen. Auch Kurzerläuterungen zu den zentralen Datenschutzvorschriften im Sächsischen Krankenhausgesetz (§§ 33, 34 SächsKHG) halte ich für sinnvoll. Darüber hinaus sollte eine Dienstanweisung so konkret wie möglich sein und vermeiden, daß den Beschäftigten das Wie der Umsetzung überlassen bleibt. So bleibt z. B. der Hinweis, daß "ärztliche Aufzeichnungen auf elektronischen Datenträgern oder anderen Speichermedien nur zulässig sind, wenn besondere Sicherungs- und Schutzmaßnahmen ergriffen werden, um Veränderungen, Vernichtung und unrechtmäßige Verwendung zu verhindern" nur eine Leerformel, solange die für den Datenschutz verantwortliche Krankenhausleitung nicht für Sicherungs- und Schutzmaßnahmen sorgt. Eine Dienstanweisung befaßt sich mit der organisatorischen Seite des Datenschutzes und der "Schwachstelle Mensch".

In einem Krankenhaus sollte per Dienstanweisung vor allem die Postbehandlung (s. 4. Tätigkeitsbericht unter 10.1.6) geregelt werden sowie die Patientenaufnahme, der Umgang mit archivierten Patientendaten, das Patientengespräch im Mehrbettzimmer (nachstehend 10.1.7), telefonische Auskünfte, Einsichtnahme von Patienten und durch Dritte in Krankenakten, Übermittlung von Patientendaten an die Krankenhausseelsorge usw.

Unter diesen Gesichtspunkten überarbeitet die Datenschutzbeauftragte des Krankenhauses derzeit den Entwurf. Ich werde die Arbeit begleiten. Mein Ziel ist es, aus der Endfassung eine Musterdienstanweisung zu erstellen.

10.1.4 Förmliche Verpflichtung des Krankenhauspersonals auf das Datengeheimnis und Belehrung über die ärztliche Schweigepflicht

Immer wieder baten Krankenhäuser, die sich in kommunaler Trägerschaft oder in der Trägerschaft des Freistaates Sachsen befinden, "Schweigepflichterklärungen" und "Merkblätter zur Verpflichtungserklärung" datenschutzrechtlich zu beurteilen. Keines der vorgelegten Formblätter entsprach den datenschutzrechtlichen Anforderungen.

Sinn einer Verpflichtung auf das Datengeheimnis ist es, den Beschäftigten nahezubringen, daß sie personenbezogene Daten nur im Rahmen ihrer Befugnisse *verarbeiten* dürfen und *Schweigen* allein nicht reicht. Es geht also darum, ob und in welcher Weise personenbezogene Daten überhaupt erhoben und weiterverarbeitet werden dürfen. Die Frage der Übermittlung der Daten an Dritte ist nur ein Detail, wenn auch ein wichtiges. Die Beschäftigten sind besonders auf die für ihre Tätigkeit einschlägigen Spezialgesetze hinzuweisen, für den Umgang mit Patientendaten im Krankenhausbereich also auf das Sächsische Krankenhausgesetz (z. Zt. prüfe ich, ob dieses Gesetz auch für Krankenhäuser im Straf- und Maßregelvollzug gilt). Darüber hinaus muß eine Unterrichtung über die sonstigen bei der Tätigkeit zu beachtenden Vorschriften über den Datenschutz erfolgen. Hierzu zählen außer den für das Krankenhaus auch die für den konkreten Arbeitsplatz geschaffenen Regelungen (z. B. Poststelle, Telefonzentrale, PC-Arbeitsplätze). All dies wurde nicht berücksichtigt. Ebensowenig wurde beachtet, daß es keine *Verpflichtung* auf die ärztliche Schweigepflicht nach § 203 Strafgesetzbuch, § 3 der Berufsordnung der Sächsischen Landesärztekammer sowie § 9 BAT-O gibt, sondern lediglich eine *Belehrung* über diese Vorschriften. Übersehen wurde auch, daß die Berufsordnung der Sächsischen Landesärztekammer nur für *Ärzte* gilt und daß sie für alle Beschäftigten, die keine Ärzte oder ärztliches Hilfspersonal sind, keine Pflicht zur Verschwiegenheit begründet.

Daher habe ich eine speziell auf die datenschutzrechtlichen Belange eines Krankenhauses in öffentlicher Trägerschaft abgestimmte "Schweigepflichterklärung" entworfen sowie ein Merkblatt mit den notwendigsten Erläuterungen und Auszügen aus den einschlägigen Rechtsvorschriften. Ich habe den Krankenhäusern die Verwendung empfohlen und darauf hingewiesen, daß das Merkblatt weder eine ausführliche Kommentierung ist noch eine Dienstanweisung für den Datenschutz ersetzt. Wie mir das SMS mitgeteilt hat, sind die Krankenhäuser in Landesträgerschaft angewiesen wurden, die von mir vorgeschlagenen und nachstehend abgedruckten Formblätter zu verwenden. Das Formblatt mit dem Wortlaut von § 6 SächsDSG (Datengeheimnis), § 32 SächsDSG (Ordnungswidrigkeiten), § 33 SächsDSG (Straftaten), § 33 SächsKHG (Datenschutz), § 203 StGB (Verletzung von Privatgeheimnissen), § 9 BAT-O (Schweigepflicht) ist hier nicht abgedruckt.

Name des Krankenhauses

Verpflichtung auf das Datengeheimnis
sowie
Belehrung über die Schweigepflicht, die Wahrung des Patientengeheimnisses und die Einhaltung datenschutzrechtlicher Vorschriften

Frau/Herr _____, dessen/deren Tätigkeit sie/ihn mit personenbezogenen Daten, insbesondere Patientendaten, regelmäßig in Verbindung bringt, wurde auf die Wahrung des Datengeheimnisses nach § 6 Sächsisches Datenschutzgesetz verpflichtet. Außerdem wurde sie/er über die arbeitsvertragliche Pflicht zur Verschwiegenheit (§ 9 BAT-O) und die Wahrung des Patientengeheimnisses (§ 203 Strafgesetzbuch) belehrt und darüber informiert, daß diese Pflichten auch nach Beendigung des Arbeitsverhältnisses fortbestehen.

Sie/Er wurde darauf hingewiesen, daß personenbezogene Daten nur im Rahmen der Befugnisse des Sächsischen Datenschutzgesetzes und der für die Tätigkeit einschlägigen Spezialgesetze verarbeitet oder verwendet werden dürfen und daß beim Umgang mit Patientendaten vorrangig das Sächsische Krankenhausgesetz zu beachten ist. Darüber hinaus hat er/sie die sonstigen bei der Tätigkeit zu beachtenden Vorschriften über den Datenschutz zu befolgen. Dazu zählen auch arbeitsplatzspezifische Regelungen (z. B. Dienstanweisung für den Datenschutz, Anweisungen für den Umgang mit Telefax-Geräten, Vernichtung von Akten und sonstigen Datenträgern, Zuständigkeitsregelungen, Einzelanweisungen von Vorgesetzten).

Er/Sie wurde ausdrücklich darauf hingewiesen, daß ein Verstoß gegen datenschutzrechtliche Vorschriften mit Geldbuße bzw. Geld- oder Freiheitsstrafe geahndet werden kann und dies arbeitsrechtliche Maßnahmen nicht ausschließt. Eine Verletzung des Datengeheimnisses wird in den meisten Fällen eine Verletzung der arbeitsvertraglichen Schweigepflicht darstellen; zugleich kann in ihr eine Verletzung des Patientengeheimnisses liegen.

Sie/Er erklärt hiermit, hinreichend über die Einhaltung des Datenschutzes unterrichtet zu sein, und bestätigt den Empfang einer Abschrift diese Protokolls sowie eines Merkblatts zu den einschlägigen Rechtsvorschriften.

_____ _____

(Unterschrift der/des Verpflichteten) (Unterschrift der/des Verpflichtenden)

_____

(Ort und Datum der Verpflichtung)

Merkblatt zur Verpflichtungserklärung

Wer ist "bei der Datenverarbeitung" beschäftigt?
"Bei der Datenverarbeitung" sind alle Personen beschäftigt, deren Aufgabengebiet sie regelmäßig mit personenbezogenen Daten, im Krankenhausbereich sind dies insbesondere die Patientendaten, in Verbindung bringt.

Der Schutz von Patientendaten

Was sind Patientendaten?
Patientendaten sind alle Einzelangaben über persönliche oder sachliche Verhältnisse eines bestimmten oder bestimmbaren Patienten. Patientendaten sind auch die personenbezogenen Daten von Angehörigen und anderen Bezugspersonen des Patienten sowie sonstiger Dritter, die dem Krankenhaus im Zusammenhang mit der Behandlung bekannt werden. Außer den in automatisierten Dateien gespeicherten oder in Karteien oder Krankenakten aufgezeichneten Daten gehören auch die auf andere Weise festgehaltenen Informationen über den Patienten dazu (z. B. Röntgenaufnahmen, graphische Aufzeichnungen wie EKG, Blut- und Gewebeproben usw.). Auch auf mündlichem Wege erlangte und nicht aufgezeichnete Kenntnisse über seine persönlichen oder sachlichen Verhältnisse sind Patientendaten.

Welche Datenschutzvorschriften sind beim Umgang mit Patientendaten zu beachten?
Im Krankenhaus dürfen Patientendaten nur erhoben (beschafft), verarbeitet (erfaßt, aufgenommen, aufbewahrt, verändert) oder sonst genutzt (auf eine sonstige Art und Weise verwendet) werden, soweit § 33 Abs. 2 Nr. 1 bis 3 des Sächsischen Krankenhausgesetzes (SächsKHG) dies erlaubt oder der Patient eingewilligt hat. Ohne Einwilligung des Patienten dürfen seine Daten nur in den Fällen des § 33 Abs. 3 Nr. 1 bis 8 SächsKHG an Personen oder Stellen außerhalb des Krankenhauses übermittelt (weitergegeben, mitgeteilt) werden.

Mit der Einwilligung dürfen die gesetzlichen Erlaubnisgründe für die Erhebung, Verarbeitung, sonstige Nutzung und Übermittlung von Patientendaten nicht beliebig erweitert werden. Die Einwilligung bedarf der Schriftform, wenn nicht wegen besonderer Umstände eine andere Form angemessen ist.

Datenschutz ist also mehr als nur Verschwiegenheit!

Eine besondere Form des "Datenschutzes" ist die Schweigepflicht der Ärzte und des medizinischen Personals. Sie schützt das Patientengeheimnis und gilt zusätzlich zu den übrigen Datenschutzvorschriften. Die unbefugte Offenbarung des Patientengeheimnis kann nach § 203 Strafgesetzbuch geahndet werden (s. u.).

Wann ist die Offenbarung des Patientengeheimnisses befugt, wann ist sie unbefugt?

Das Patientengeheimnis wird *unbefugt offenbart*, wenn es ohne Zustimmung des Pati-

enten oder ohne ein anderes Recht zur Mitteilung in irgendeiner Weise an einen anderen (Dritten) gelangt. Dabei ist es gleichgültig, ob der Dritte seinerseits schweigepflichtig ist oder ob es sich um einen Angehörigen des Patienten handelt. Dritte in diesem Sinne sind nicht die an der Behandlung eines Patienten im Krankenhaus beteiligten Ärzte und deren Hilfspersonal sowie die mit der Patientenverwaltung Beschäftigten, der sogenannte "zum Wissen berufene Personenkreis".

Das Patientengeheimnis wird *befugt offenbart*, wenn der Patient die betreffenden Personen von der Schweigepflicht entbunden hat. Dies hat in der Regel schriftlich zu erfolgen. Ohne eine Entbindung von der Schweigepflicht ist die Offenbarung nur befugt (und damit nicht strafbar), wenn in einem Gesetz die Mitteilung vorgeschrieben (z. B. Bundesseuchengesetz) oder unter bestimmten Voraussetzungen (z. B. nach dem Sächsischen Krankenhausgesetz) zugelassen ist. Auch eine Rechtsgüterabwägung kann die Befugnis zur Offenbarung schaffen.

Der Schutz von anderen personenbezogenen Daten

Was sind - ganz allgemein - personenbezogene Daten?
Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (z. B. Krankenhausbeschäftigte, Handwerker, Lieferanten, Mitarbeiter von Forschungseinrichtungen usw.).

Unter welchen Voraussetzungen dürfen personenbezogenen Daten verarbeitet werden?
Die Verarbeitung personenbezogener Daten ist nur zulässig, wenn das Sächsische Datenschutzgesetz oder eine besondere - "bereichsspezifische" - Rechtsvorschrift sie erlaubt. Dabei gehen bereichsspezifische Rechtsvorschriften dem Sächsischen Datenschutzgesetz vor. Bei der Verarbeitung von Beschäftigtendaten sind vorrangig § 31 SächsDSG und - soweit es sich um Beamte handelt - das Sächsische Beamtengesetz und die dazu ergangenen Rechtsverordnungen zu beachten.

Folgen datenschutzrechtlicher Verstöße

Ein Verstoß gegen datenschutzrechtliche Verarbeitungsvorschriften kann je nach Schwere eine Ordnungswidrigkeit gemäß § 32 Sächsisches Datenschutzgesetz - (Geldbuße bis zu 50.000 DM möglich) oder eine Straftat gemäß § 33 SächsDSG (Freiheitsstrafe bis zu zwei Jahren oder Geldbuße) sein. Meist wird es sich gleichzeitig um eine Verletzung der Verschwiegenheitspflicht nach § 9 BAT-O handeln, so daß auch arbeitsrechtliche Konsequenzen zu erwarten sind. Sofern der Tatbestand der unbefugten Offenbarung des Patientengeheimnisses im Sinne von § 203 Strafgesetzbuch erfüllt ist, kann ein Beschäftigter nach dieser Vorschrift bestraft werden.

10.1.5 Keine Vernichtung kopierter Therapieberichte nach Abschluß einer psychotherapeutischen Behandlung

Ein Petent teilte mir mit, daß im Zusammenhang mit seiner psychotherapeutischen

Behandlung in einem sächsischen Landeskrankenhaus der Therapiebericht eines anderen Krankenhauses in Kopie übermittelt worden sei. Dem habe er zugestimmt. Nach der nunmehr abgeschlossenen Behandlung wünsche er die Vernichtung der Kopie, weil sie ohne seine Zustimmung nicht in den Verfügungsbereich des Landeskrankenhauses gelangt wäre; das Krankenhaus weigere sich jedoch. Der Petent bat mich um Prüfung, ob er die Vernichtung verlangen könne.

Ich habe diesen Sachverhalt wie folgt beurteilt:

Für den Bereich der Krankenhäuser regelt § 33 Abs. 6 SächsKHG die Löschung von Patientenakten. Danach dürfte die Kopie des Therapieberichts erst nach Ablauf der Aufbewahrungsfrist vernichtet werden. Die Tatsache, daß sie ohne Zustimmung des Petenten nicht in den Besitz des Landeskrankenhauses gelangt wäre, rechtfertigt keine vorzeitige Vernichtung. Selbst wenn der Arzt dazu bereit wäre, stünde dem eine Rechtsvorschrift entgegen; denn die Berufsordnung der Sächsischen Landesärztekammer, die auf dem Sächsischen Heilberufekammergesetz basiert und für die Ärzte verbindlich ist, gibt eine Aufbewahrungsfrist vor. Nach § 15 dieser Vorschrift haben Ärzte "die in Ausübung ihres Berufs gemachten Feststellungen und getroffenen Maßnahmen" aufzuzeichnen und diese Aufzeichnungen *mindestens* zehn Jahre nach Abschluß der Behandlung aufzubewahren. Im Hinblick auf die Verjährungsfrist des § 852 BGB befürworte ich 30 Jahre.

Die geschlossene Dokumentation einer Behandlung und die dabei entstandenen Unterlagen bilden die "Patientenakten", die nicht nur im Interesse des Patienten, sondern auch des Arztes geführt und aufbewahrt werden. Es ist davon auszugehen, daß der behandelnde Arzt den Therapiebericht des anderen Krankenhauses für die Behandlung des Petenten benötigt und verwertet hat und die Kopie deshalb zum Bestandteil der ärztlichen Dokumentation, also der Patientenakte, geworden ist.

10.1.6 Verfilmung von Krankenunterlagen durch private Dienstleister

Mehrfach ist die Frage an mich herangetragen worden, ob und unter welchen Voraussetzungen Krankenhäuser private Dienstleister mit der Verfilmung von Patientenakten beauftragen dürfen. Dazu habe ich mich wie folgt geäußert:

Die Mikroverfilmung oder Erfassung von Patientenakten auf optischen Speichermedien ist eine Datenverarbeitung im Auftrag, der gemäß § 33 Abs. 10 i. V. m. § 36 Abs. 1 SächsKHG das Regierungspräsidium zustimmen muß. Die Zustimmung darf nur erteilt werden, wenn sichergestellt ist, daß beim Auftragnehmer die Datenschutzbestimmungen des Sächsischen Krankenhausgesetzes sowie (subsidiär) des Sächsischen Datenschutzgesetzes eingehalten werden. In Abhängigkeit von den Datensicherheitsmaßnahmen des Dienstleisters (Aktentransport, räumliche Bedingungen, Personal) kann möglicherweise nur eine Verfilmung in den Räumen des Krankenhauses unter Aufsicht von Mitarbeitern des Krankenhauses in Betracht kommen.

Beabsichtigt ein Krankenhaus die Erteilung eines solchen Auftrags, sollte es sich anhand der neueren Rechtsprechung vergewissern, ob die Originalunterlagen weiterhin aufbewahrt werden müssen. Soweit mir bekannt ist, haben die Gerichte in Streitfällen bisher nur Originalunterlagen Urkundenqualität zuerkannt. Außerdem sollte geklärt werden, wie unzutreffende Daten auf einem Mikrofiche oder optischem Speichermedium berichtigt werden können (§ 33 Abs. 1 Satz 1 SächsKHG i. V. m. § 18 SächsDSG). Nach meiner Kenntnis fehlen dazu bisher die technischen Möglichkeiten. Zu bedenken wäre auch die Haltbarkeit der neuartigen Datenträger, und daß das Sichtbarmachen der auf ihnen gespeicherten Daten bei der langfristigen Aufbewahrung (üblicherweise 30 Jahre nach Abschluß der Behandlung) gewährleistet sein muß.

§ 33 Abs. 10 SächsKHG fordert, daß die für Ärzte und ärztliches Hilfspersonal geltende Schweigepflicht beim Auftragnehmer entsprechend eingehalten wird. Da er und seine Mitarbeiter nicht zum ärztlichen Hilfspersonal gehören - auch nicht im weitesten Sinne -, findet § 203 StGB keine unmittelbare Anwendung. Für die Praxis bedeutet dies, daß die mit der Verfilmung beauftragten Personen nach § 2 Abs. 2 Nr. 2 Verpflichtungsgesetz zur Verschwiegenheit verpflichtet werden müssen. Nur in diesem Fall gehören sie als für den öffentlichen Dienst besonders Verpflichtete zu den in § 203 StGB genannten Personen und können wie Ärzte und ärztliches Hilfspersonal bei einem Bruch des Patientengeheimnisses bestraft werden.

10.1.7 Gespräche zwischen Arzt und Patient im Mehrbett-Zimmer

Beim SMS haben sich 1996 die Beschwerden von Patienten über das mangelnde datenschutzrechtliche Bewußtsein von Krankenhausärzten gehäuft. Die Patienten haben beklagt, daß in Mehrbettzimmern Anamnesedaten erhoben und bei Visiten Diagnosen besprochen werden, so daß Bettnachbarn zwangsläufig Kenntnis von Krankheitsdaten erhalten, die gemäß § 203 StGB der ärztlichen Schweigepflicht unterliegen. Das SMS hat sich durch diese Beschwerden veranlaßt gesehen, die sächsischen Krankenhäuser auf die Beachtung des Patientengeheimnisses hinzuweisen und mich zu diesem Zweck um eine datenschutzrechtliche Bewertung sowie um Vorschläge gebeten, durch welche praktischen Maßnahmen die Probleme vermieden werden können.

Ich habe das Vorhaben des SMS mit folgenden Überlegungen unterstützt:

Die zu treffenden Maßnahmen sind vor dem Hintergrund zu sehen, daß im Krankenhausbereich kein Patient vollkommen von seinen Mitpatienten abgeschottet werden kann. Ist er in einem Mehrbettzimmer untergebracht, muß er es hinnehmen, daß Mitpatienten von seinen Krankheitsdaten und den an ihm durchgeführten Behandlungen im gewissen Umfang Kenntnis erhalten. Das heißt jedoch nicht, daß er mit der Anmeldung stillschweigend in die Offenbarung des Patientengeheimnisses einwilligt und die ärztliche Schweigepflicht gegenüber den Mitpatienten nicht gilt.

Vor der ersten medizinischen Maßnahme führt - von Notfällen abgesehen - der Arzt mit dem Patienten ein Aufnahmegespräch, um Anamnesedaten zu erheben, die Diagnose des einweisenden Arztes bzw. den Verdacht auf eine bestimmte Erkrankung zu besprechen. Der Patient wird über Eingriff, Behandlung sowie mögliche Risiken umfassend aufgeklärt und unterschreibt den Behandlungsvertrag. Zu diesem Zeitpunkt ist er regelmäßig in der Lage, das Arztzimmer oder einen separaten Raum aufzusuchen, so daß es nur in seltenen Ausnahmefällen gerechtfertigt ist, ein solches Gespräch im Krankenzimmer vor Mitpatienten zu führen.

Bereits bei diesem Aufnahmegespräch kann der Arzt die Form der künftigen Kommunikation erörtern, um individuelle Wünsche und Empfindlichkeiten des Patienten zu erkennen und sie in Abhängigkeit von Erkrankung, Eingriff, Behandlung und örtlichen Besonderheiten später berücksichtigen zu können. Gegebenenfalls muß dem Patienten erklärt werden, welche unabweisbaren Gründe seinen Bedürfnissen entgegenstehen. Auf jeden Fall muß der Arzt vermeiden, den Patienten erst bei der Visite zu fragen, ob er mit einem Gespräch in Gegenwart von Mitpatienten einverstanden ist. Viele Patienten werden Hemmungen haben, die Frage in dieser Situation zu verneinen, vor allem, wenn sie sich in einem physisch bzw. psychisch angegriffenen Zustand befinden.

Dagegen hat der Patient *sozialadäquate, übliche und alltägliche Behandlungsmaßnahmen* zu dulden, auch in Anwesenheit von Mitpatienten. Insoweit ist die Offenbarung des Patientengeheimnisses wohl unvermeidbar. Problematisch ist jedoch, wo die Grenze liegt und welche datenschutzrechtlichen Maßnahmen dann greifen sollten.

Die Frage nach der Grenze hängt nach meiner Auffassung von der Art der Daten ab, nicht von einem "positiven" oder "negativen" Inhalt. So sind *Befund, Heilungschancen, bleibende oder vorübergehende Schädigungen, Anamnesedaten, Therapien, Angelegenheiten der Intimsphäre und alles, was dem Patienten peinlich oder unangenehm werden könnte*, generell vertraulich zu behandeln, d. h. nur in einem Vieraugengespräch zu erörtern. Dies muß nicht zwangsläufig im Arztzimmer stattfinden. Soweit zumutbar, könnten Mitpatienten gebeten werden, das Zimmer vorübergehend zu verlassen. Ist im Einzelfall kein Vieraugengespräch möglich oder hat der Patient im Vorfeld (nach ausdrücklicher Befragung) keine Vorbehalte geäußert, sollten diese Punkte gleichwohl *leise* besprochen werden. Alternativ oder zusätzlich könnte ein Fernseh- oder Rundfunkgerät ein- bzw. lautgeschaltet, ein Paravent aufgestellt oder auf schriftliche oder telefonische Kommunikation ausgewichen werden.

10.1.8 Einladung zu einer Spezialuntersuchung auf Postkarte

Eine Klinik und Poliklinik für Neurologie bat ihre Patienten mit vorgedruckten Postkarten zu Spezialuntersuchungen des Gehirns, und zwar mit folgendem Text:

Auf Veranlassung von Frau/Herrn Dr. ..... werden Sie gebeten, sich am ..... um ..... in der hiesigen Abteilung zur elektroenzephalographischen (hirnelektrischen) Untersuchung einzufinden. Treffen Sie bitte folgende Vorbereitungen:

1. *Notieren Sie den Namen der z. Zt. eingenommenen Arzneimittel bzw. bringen Sie je eine Packung mit.*
2. *Nehmen Sie bitte am Abend vor der EEG-Untersuchung eine gründliche Kopfwäsche vor, bitte danach Kopfhaut nicht einölen und keinen Haarspray benutzen.*
3. *Halten Sie in der Nacht vor der EEG-Untersuchung ausreichend Nachtruhe ein und meiden Sie Alkohol.*
4. *Übliche Mahlzeiten sollten eingehalten werden.*

.....

Techn. EEG-Assistentin

Bitte nehmen Sie an diesem Tag Ihre Medikamente zu Hause nicht ein, sondern erst hier nach erfolgter Spezialuntersuchung!

Dies halte ich für einen massiven Fehlgriff.

Ich habe dem Krankenhaus mitgeteilt, daß es weder mit der durch § 203 StGB geschützten ärztlichen Schweigepflicht noch mit den datenschutzrechtlichen Regelungen des § 33 SächsKHG zu vereinbaren ist, wenn für ein solches Schreiben, das Angaben über den Patienten enthält, statt eines Briefes eine Postkarte verwendet wird.

Der erst seit kurzem in der Klinik tätige Direktor teilte mir seine Betroffenheit über diese Praxis mit, von der er keine Kenntnis hatte. Per Dienstanweisung hat er unverzüglich dafür gesorgt, daß diese Postkarten das Haus nicht mehr verlassen, und auf einer Ärztekonferenz die Verwendung von Postkarten mit Patientendaten generell untersagt.

10.1.9 Abschlußbericht der Kommission zur Untersuchung von Mißbrauch der Psychiatrie im sächsischen Gebiet der ehemaligen DDR (Kommission Psychiatriemißbrauch)

Nach der Wende berichteten die Medien immer wieder von Zwangseinweisungen in psychiatrische Einrichtungen der DDR, die aus politischen Gründen erfolgt seien. Dabei wurde dem Krankenhaus für Psychiatrie Waldheim und dem Haftkrankenhaus Waldheim eine zentrale Rolle zugeschrieben. Die Initiativen von Betroffenen, Gruppen unterschiedlicher Richtungen und Politikern führten dazu, daß sich auch der Sächsische Landtag mit dieser Frage beschäftigte. Das Kabinett beschloß, beim SMS die Kommission Psychiatriemißbrauch durch den Sächsischen Staatsminister für Soziales, Gesundheit und Familie einzurichten.

Aufgabe der Kommission Psychiatriemißbrauch war es zu klären, ob es einen systematischen Mißbrauch der Psychiatrie in der DDR gegeben hat, ob Menschen z. B. durch Mittel der psychiatrischen Medizin in unzulässiger Weise seelisch und körperlich beeinträchtigt, rechtswidrig ihrer Freiheit beraubt oder beim Verdacht politisch motivierter Straftaten psychiatrisch begutachtet und durch Gerichtsbeschluß in psychiatrische Einrichtungen eingewiesen wurden. Die Kommission sollte damit einen Beitrag zur Aufarbeitung der DDR-Vergangenheit leisten. Darüber hinaus hat sie auch Einzelschicksale untersucht und über die Feststellungen Gutachten gefertigt, wenn Betroffene oder ihre Angehörigen dies gewünscht haben.

Zum Jahresende 1996 hat die Kommission Psychiatriemißbrauch über ihre Arbeit entsprechend dem Kabinettsbeschluß einen Abschlußbericht verfaßt, der mir im Entwurf übersandt worden ist. Ich hatte zu prüfen, ob die Veröffentlichung - beispielsweise im Zusammenhang mit der beabsichtigten Behandlung im Sächsischen Landtag - datenschutzrechtlich unbedenklich ist.

Der Bericht besteht aus einem allgemeinen Teil und der Darstellung von 126 Einzelfällen, die den allgemeinen Teil konkretisieren und die Antragsbearbeitung dokumentieren sollen.
Ich habe mich dazu wie folgt geäußert:

1. Im allgemeinen Teil sind die Namen von *Privatpersonen* zu löschen, die nicht in die Bekanntgabe ihres Namens im Abschlußbericht eingewilligt haben. Entsprechendes gilt für Angaben, die einen Personenbezug erlauben. *Personen des öffentlichen Lebens* (z. B. Abgeordnete, kommunale Mandatsträger, Staatssekretäre, Bürgermeister etc.) dürfen genannt werden. Zulässig ist es in diesem Fall auch, Daten von *Kommissions- und Arbeitsgruppenmitgliedern sowie von Mitarbeitern* bekanntzugeben, soweit sie ihre Eigenschaft als Amtsträger betreffen und erforderlich sind. Zwar habe ich im Gegensatz zur Kommission nicht alle Angaben für erforderlich gehalten (z. B. Wohnort, Grund des Ausscheidens), aber meine Bedenken zurückgestellt, weil - so wurde mir versichert - die Notwendigkeit im Vorfeld eingehend diskutiert worden sei. Schließlich habe ich auch das Argument akzeptiert, die Betroffenen hätten sämtlich am Bericht mitgewirkt und dabei die Daten über sich eingebracht, so daß ihr Persönlichkeitsrecht nicht verletzt werde. Eine formgerechte schriftliche Einwilligung wäre hier im Sinne von § 4 Abs. 2 SächsDSG sicher unangemessen gewesen.

2. Die 126 Einzelfälle enthalten keine Namen von Betroffenen, sondern Schlüsselnummern. Zwei Kommissionsmitglieder können diese Nummern über eine Liste den Betroffenen wieder zuordnen. Die übrigen Angaben sind stark schematisiert und lassen auch wegen des Systems zur Verschlüsselung der psychiatrischen Einrichtungen keinen Rückschluß auf bestimmte Personen zu. Auch wenn dies keine Anonymisierung im strengen Sinne von § 3 Abs. 2 Nr. 4 SächsDSG ist, habe ich sie als "faktische Anonymisierung" angesehen und keine Bedenken gegen die Bekanntgabe der Einzelfälle in der jetzigen Form geäußert. Ich hatte zuvor

angeregt, auf die Darstellung der Einzelfälle zu verzichten. Dem steht nach Auffassung der Kommission jedoch der Kabinettsbeschluß entgegen, den ich respektiere.

10.1.10 Recht Betroffener auf Einsicht in Akten der Kommission Psychiatriemißbrauch

Haben sich Betroffene an die Kommission Psychiatriemißbrauch beim SMS gewandt (Einzelheiten zur Aufgabe und Tätigkeit dieser Kommission im vorstehenden Abschnitt), um mit ihrer Hilfe Klarheit darüber zu erlangen, ob in ihrem persönlichen Fall oder dem eines Angehörigen ein Psychiatriemißbrauch vorlag, hat die Kommission diesen Einzelfall geprüft. Dabei ist sie den Umständen der Einweisung sowie der Art und Dauer der Behandlung nachgegangen und hat mit Einwilligung des Betroffen Akten anderer Behörden oder Fachkrankenhäuser beigezogen. Außerdem hat sie eine psychiatrische Untersuchung veranlaßt, über deren Ergebnisse der Facharzt ein Vorgutachten zu erstellen hatte. Sie waren die wesentlichen Grundlagen für das Endgutachten, das dem Betroffenen übersandt wurde.

Ein Betroffener verlangte, auch das Vorgutachten zu sehen. Ich hatte zu prüfen, ob ihm die Einsichtnahme gestattet werden muß. Nach der Geschäftsordnung der Kommission hätte das Vorgutachten nicht nach außen bekanntgegeben werden dürfen. Ich bin zu folgendem Ergebnis gekommen:

Die Aufgabe der Kommission Psychiatriemißbrauch ist bedauerlicherweise nicht durch Gesetz geregelt worden. Damit ist die verlangte Akteneinsicht ein Antrag außerhalb eines spezialgesetzlichen Verfahrens, so daß sich Auskunfts- und Einsichtsansprüche nicht nach bereichsspezifischen Rechtsvorschriften richten, sondern nach § 17 SächsDSG als Auffangvorschrift. Die Geschäftsordnung kann die darin festgeschriebenen Rechte der Betroffenen nicht einschränken, weil sie keine Rechtsnorm ist.

Gemäß § 17 Abs. 3 SächsDSG hat die speichernde Stelle einem Betroffen Einsicht in die zu seiner Person geführten Akten zu gewähren. Da § 3 Abs. 6 SächsDSG eine Akte als einen Träger personenbezogener Daten definiert - der datenschutzrechtliche Aktenbegriff also insoweit nicht mit dem umgangssprachlichen Aktenbegriff übereinstimmt - ist das Vorgutachten selbst eine Akte. Für die Akteneinsicht kommt es daher nicht darauf an, wo sich ein Schriftstück befindet - im Aktenhefter des Betroffenen oder z. B. bei den Arbeitsunterlagen der Kommission oder ihrer Arbeitsgruppen -, sondern darauf, ob es zur Person des Betroffenen gefertigt wurde. Das ist bei einem Vorgutachten über den Betroffenen der Fall.

Das Akteneinsichtsrecht ist grundsätzlich unbeschränkt, solange es *berechtigte* Interessen Dritter nicht beeinträchtigt (§ 17 Abs. 4 SächsDSG). Es gab keine Hinweise darauf, daß dies der Fall sein könnte. Auf keinen Fall sind die Mitglieder und Mitarbeiter der Kommission Psychiatriemißbrauch und ihrer Arbeitsgruppen solche

Dritten (§ 3 Abs. 4 SächsDSG), auch wenn sie wie hier zum Jahresende 1996 die Arbeit eingestellt haben und die Akten nun ein Referat im SMS verwaltet.
Folglich steht dem Betroffenen eine Einsicht in das Vorgutachten zu.

Ein anderer Betroffener vermutete in den bei der Kommission Psychiatriemißbrauch über ihn vorhandenen Unterlagen ein Schreiben, das er als "Denunziantenbrief" bezeichnete, und verlangte eine Kopie. Da die Kommission diese verweigerte, bat er mich um Unterstützung.

Wie sich herausstellte, war das Schreiben Bestandteil einer vor dem 3. Oktober 1990 über den Petenten geführten Strafakte, die sich bei der Kommission Psychiatriemißbrauch als vollständige Kopie befand. Fraglich war, ob die Strafaktenkopie damit Teil der Kommissionsakten geworden war. In diesem Fall hätte sich das Auskunfts- und Einsichtsrecht nach dem Sächsischen Datenschutzgesetz gerichtet, andernfalls - wie bei der Originalakte - nach der Strafprozeßordnung.

Bei Anwendung des Sächsischen Datenschutzgesetzes hätte die Kommission Psychiatriemißbrauch gemäß § 17 Abs. 4 SächsDSG eine Interessenabwägung vorzunehmen. Sie hätte also zu prüfen, ob das Interesse des Betroffenen an der Akteneinsicht das Interesse eines Dritten an der Geheimhaltung überwiegt. Sofern eine Entscheidung anhand der vorhandenen Unterlagen nicht möglich ist, müßte der Betroffene ggf. gebeten werden, sein Interesse an der Akteneinsicht zu konkretisieren; der Dritte hätte ggf. sein entgegenstehendes Interesse darzulegen.

Ich habe mich jedoch dafür ausgesprochen, die Kopie wie das Original zu behandeln. Die Kopie war von der Staatsanwaltschaft - wohl ohne hinreichende rechtliche Befugnis - übersandt worden, weil sie das Original nicht aus der Hand geben wollte. Dies darf nicht dazu führen, daß ein Betroffener "auf Umwegen" bei einer Behörde Einsicht in Akten nimmt, die dieser Behörde nicht gehören und sich dort nur vorübergehend befinden, weil sie - hier mit Einwilligung des Betroffenen - beigezogen worden sind. Der Betroffene darf also nicht mehr und nicht weniger Daten zur Kenntnis nehmen als bei Einsichtnahme in das Original. Die Entscheidung über den Antrag hat deshalb auch die Stelle zu treffen, die das Original verwaltet, hier die Staatsanwaltschaft.

Dies sowie Einzelheiten über Einsichts- und Auskunftsansprüche nach der Strafprozeßordnung bzw. der Richtlinien für das Straf- und Bußgeldverfahren habe ich dem Petenten mitgeteilt.

10.1.11 Datenschutz im Maßregelvollzug

Eine steigende Zahl von Patientenbeschwerden aus dem Maßregelvollzug über Datenschutzverstöße des Personals in den Sächsischen Fachkrankenhäusern für Psychiatrie und Neurologie (Fachkrankenhäuser) bestätigt die Ausführungen in meinem 4. Tätigkeitsbericht (1.1.10) über das unzureichende Datenschutzbewußtsein

der Beschäftigten. Zwar ist das gesamte Personal der Fachkrankenhäuser inzwischen nach einem von mir vorgeschlagenen Muster (oben 10.1.4) über das Datengeheimnis und die ärztliche Schweigepflicht belehrt worden. Ein effektiver Datenschutz ist damit noch nicht gewährleistet, solange Dienstanweisungen für den Datenschutz fehlen. Das SMS sieht deshalb die Notwendigkeit, bei den Fachkrankenhäusern die Erstellung von Dienstanweisungen zu veranlassen.

Im Hinblick auf eine einheitliche Handhabung und weil sich Fachliteratur und Rechtsprechung mit Datenschutzproblemen im Maßregelvollzug bisher kaum beschäftigt haben, hat das SMS eine Arbeitsgruppe gebildet, an der ich beteiligt bin und in der Problemlösungen erarbeitet und für die Übernahme in Dienstanweisungen aufbereitet werden sollen. Dies erfordert eine Auseinandersetzung mit besonders schwierigen Fragen wie
- Videoüberwachung im Maßregelvollzug,
- Öffnung eingehender und ausgehender Post bei Patienten im Maßregelvollzug,
- Telefonüberwachung im Maßregelvollzug,
- Umfang der Weitergabe von Patientenakten an die Gerichte,
- Zusammenarbeit mit externen Einrichtungen und Übermittlung von Krankheitsdaten an diese,
- Einwilligungsfähigkeit von Psychiatriepatienten,
- Einsicht von Patienten in ihre Krankenakten und Umgang mit den darin enthaltenen Daten des behandelnden Psychiaters, der sich mit seiner Person (eigenen Gefühlen, subjektiven Einschätzungen usw.) in die Behandlung einbringen muß.

Zum Ende des ersten Quartals 1997 soll ein fertiger Entwurf vorliegen.

10.1.12 Erweiterung der Meldepflicht für übertragbare Krankheiten

Das Bundes-Seuchengesetz gilt nicht nur für Krankheiten, die von Mensch zu Mensch übertragen werden, sondern auch für Krankheiten, die durch Tiere (z. B. Fuchs/Tollwut, Mücke/Malaria) oder Gegenstände (z. B. ärztliche Geräte/Hepatitis B) und Lebensmittel auf den Menschen übertragen werden können. Unabhängig vom Weg der Infektion und davon, ob von der infizierten Person eine Ansteckungsgefahr ausgeht, kommt es für die Meldungen allein auf einen für den Menschen besonders gefährlichen Krankheitserreger an. Diese sind in einem in § 3 BSeuchG enthaltenen Katalog aufgelistet, der von den Landesregierungen durch Rechtsverordnung erweitert werden kann (§ 7 Abs. 3 BSeuchG). Von dieser Ermächtigung hat die Sächsische Staatsregierung mit der *Verordnung des Sächsischen Staatsministeriums für Soziales, Gesundheit und Familie über die Erweiterung der Meldepflicht für übertragbare Krankheiten nach dem Bundes-Seuchengesetz (SeuchMeldVO) vom 11. November 1995* Gebrauch gemacht. Nunmehr sind auch die durch Zecken-Bisse verursachten Borreliose-Erkrankungen meldepflichtig.

Da das Bundes-Seuchengesetz den Inhalt der Meldungen nicht regelt, erfolgen sie mit Namen und Anschrift des Patienten. Im Hinblick auf Maßnahmen der

Gesundheitsämter zur Verhütung oder Bekämpfung übertragbarer Krankheiten ist dies sicher unerläßlich. Fragwürdig erschien einer Krankenhausärztin jedoch die namentliche Meldung im Fall der Borreliose, weil von der infizierten Person keine Gefahr für die Allgemeinheit ausgeht und sich insoweit ein Einschreiten der Gesundheitsämter erübrigt. Nach Auffassung der Ärztin haben solche Meldungen allenfalls statistischen Wert.

Ich habe das SMS um Stellungnahme zu der Frage gebeten, wie und unter welchen Aspekten namentliche Meldungen von an Borreliose erkrankten oder gestorbenen Personen ausgewertet werden, denn sie enthalten keine Angaben über den (vermuteten) Übertragungsmodus, so daß Erkenntnisse über Infektionswege oder infektionsepidemiologische Übersichten nur unter Schwierigkeiten erlangt werden können, nämlich nur durch (für jede Verwaltung aufwendige) Rückfragen bei den gemeldeten Personen. Wurde der Tod gemeldet, sind nachträgliche Erkenntnisse ohnehin kaum mehr möglich. Hier der die Borreliose betreffende Auszug aus der umfangreichen Stellungnahme:

Obwohl die Meldepflicht erst im November 1995 eingeführt wurde, sind in Sachsen 1995 bereits 31 Erkrankungen und 1 Sterbefall (gegenüber 16 Erkrankungen 1994) bekannt geworden. In ersten Studien 1995 haben wir in 70 von 275 (= 25,4 %) untersuchten Zecken aus dem Zeisigwald, einem Naherholungsgebiet bei Chemnitz, Borrelien nachgewiesen. 1996 wurde eine sachsenweite Studie begonnen (2.000 - 3.000 Zecken). Aus diesen ersten sächsischen Untersuchungsergebnissen abzuleiten, jeder Zeckenstich solle antibiotisch behandelt werden, wäre unwissenschaftlich und widerspräche dem Übermaßverbot. Es müssen zwingend das Erkrankungspotential (Erreger-Wirt-Beziehung) und noch vorhandene Unzulänglichkeiten der Diagnostik in die Betrachtung einbezogen werden. In naher Zukunft wird uns die Aufgabe erwachsen, die Indikation oder Nichtindikation einer Schutzimpfung wissenschaftlich (epidemiologisch, klinisch, ökonomisch, ethisch) zu begründen. Ohne Datenfundus ist dies nicht möglich."

Diesen Ausführungen ist nicht zu entnehmen, welche Rolle dabei den *namentlichen* Meldungen zukommt. Meine Fragen sind damit nach wie vor offen. Derzeit erscheint es mir sinnvoll, daß endlich Datenschutzbestimmungen in das Bundes-Seuchengesetz aufgenommen werden und der Inhalt der Meldungen an die Gesundheitsbehörden konkretisiert wird, so daß z. B. die Meldungen in Abhängigkeit von der Art des Erregers namentlich oder anonym erfolgen. Ich habe die Diskussion angestoßen.

10.1.13 Anforderung der Epikrise beim Krankenhaus durch den örtlichen Träger der Sozialhilfe

Ein Krankenhaus bat mich um Prüfung, ob der örtliche Träger der Sozialhilfe berechtigt sei, nach einer stationären Behandlung die vollständige Epikrise anzufordern. Hintergrund dieser Forderung waren Auseinandersetzungen zwischen örtlichem und überörtlichem Träger der Sozialhilfe um die Zuständigkeit bei der

Entgiftung eines Alkoholabhängigen in Fachkrankenhäusern für Suchtkranke oder in psychiatrischen Fachkrankenhäusern, Fachabteilungen und Spezialeinrichtungen (im einzelnen nachstehend unter 10.2.8). Es stellte sich heraus, daß die Übermittlung der vollständigen Epikrise weder für die Bestimmung der Zuständigkeit noch für einen anderen Zweck erforderlich war.

10.2 Sozialwesen

10.2.1 Dienstanweisung für den Datenschutz im Sozialbereich

Ein Sozialleistungsträger hat mich um Stellungnahme zu dem Entwurf seiner "Datenschutzordnung" gebeten. In folgenden Punkten habe ich einen Überarbeitungsbedarf gesehen:

- Sozialdaten, Personaldaten und sonstige personenbezogene Daten wurden in einem gemeinsamen Abschnitt "personenbezogene Daten" abgehandelt, ohne die Besonderheiten des Sozialdatenschutzes und des Personaldatenschutzes zu verdeutlichen und auf die einschlägigen Rechtsvorschriften hinzuweisen. Diese waren zwar in der Datenschutzordnung gesondert aufgelistet, ebenso die zu beachtenden Verwaltungsvorschriften sowie sonstigen Anweisungen und Empfehlungen zum Datenschutz (z. B. Bekanntmachungen des Sächsischen Datenschutzbeauftragten), jedoch ohne sachlichen Zusammenhang. Ich habe angeregt, einen konkreten Bezug zwischen Vorschriften und Inhalt herzustellen und den einzelnen Datenarten (Sozialdaten, Personaldaten, sonstige personenbezogene Daten) jeweils eigene Abschnitte zu widmen.

- Die Datenschutzordnung sah vor, daß jede Abteilung ein separates Dateien- und Geräteverzeichnis führt. In meiner Bekanntmachung vom 29. September 1993 (SächsABl. S. 1175) habe ich empfohlen, daß die funktionalen Stellen lediglich *Dateibeschreibungen* erstellen und dem behördlichen Datenschutzbeauftragten für das bei ihm geführte *zentrale Dateien- und Geräteverzeichnis* zuleiten. Da ich dies für übersichtlicher und aussagefähiger halte, habe ich angeregt, die beabsichtigte Regelung zu überdenken.

  Vorgesehen war auch, vorübergehend (bis zu drei Monaten) vorgehaltene Dateien nicht in das Verzeichnis aufzunehmen. Dies ist mit § 10 SächsDSG nicht zu vereinbaren. Alle Dateien mit "Echtdaten" gehören in das Verzeichnis. In der Praxis werden dies ohnehin nur solche sein, die länger als drei Monate benötigt werden. Werden sie (z. B. für einmalige Sonderläufe) innerhalb eines kürzeren Zeitraums verarbeitet, sehe ich keinen Grund, sie zu "unterschlagen". Da Verfahrensentwicklungen meist mit Testdaten, also erfundenen oder verfremdeten Daten, erfolgen und Testdateien daher keine personenbezogenen Daten enthalten, dürfte insoweit für die Praxis kein Problem entstehen.

- Es ist wenig sinnvoll, Zulässigkeitsvoraussetzungen, Beteiligungs- und Formvorschriften für automatisierte Abrufverfahren in einer Datenschutzordnung darzustellen. Für effektiver halte ich es, durch die Dienstanweisung organisatorisch sicherzustellen, daß eine kompetente Stelle in der Behörde (z. B. Organisationsreferat, ggf. in Zusammenarbeit mit dem Behördlichen Datenschutzbeauftragten) vor der Einrichtung automatisierter Abrufverfahren beteiligt wird, wobei diese Stelle die Aufgabe hätte, die Zulässigkeitsvoraussetzungen (z. B. nach § 8 SächsDSG oder § 79 SGB X) zu prüfen, auf die Einhaltung der Formerfordernisse zu achten und den Sächsischen Datenschutzbeauftragten zu unterrichten.

- Ich habe davon abgeraten, die Maßnahmen zur Gewährleistung der Datensicherheit in abstrakter Form darzustellen, weil es in der Praxis auf *wirksame* Maßnahmen ankommt. Und das sind konkrete Maßnahmen, z. B. Hausverfügungen zum Umgang mit Einzelplatz-PCs oder Telefax-Geräten, zur Vernichtung von Schriftgut, zur Schlüsselverwaltung und Reinigung von Dienstzimmern. Auch Anweisungen, was bei der Wartung von EDV-Anlagen durch Fremdfirmen zu beachten ist, gehören dazu. Sinnvoller wäre deshalb ein Datensicherheitskonzept, das alle Maßnahmen zur Gewährleistung der Datensicherheit konkret beschreibt.

- Gut gefallen hat mir, daß in einem Abschnitt das "Wie" und "Wann" der Zusammenarbeit mit dem behördlichen Datenschutzbeauftragten und seine Stellung innerhalb des Hauses klargestellt wurde. So hat danach z. B. der Schriftverkehr mit dem Sächsischen Datenschutzbeauftragten über den behördlichen Datenschutzbeauftragten zu erfolgen. Auch die Pflichten, die sich für die Beschäftigten gegenüber dem behördlichen Datenschutzbeauftragten aufgrund seiner Befugnisse ergeben, wurden erläutert.

Der überarbeitete Entwurf liegt mir noch nicht vor. Wie mir vorab mitgeteilt wurde, sind meine Anregungen fast vollständig aufgenommen worden.

10.2.2 Vordrucke im Verfahren nach § 4 SchwbG zur Feststellung einer Behinderung

Gemäß § 4 SchwbG stellt auf Antrag des Behinderten die für die Durchführung des Bundesversorgungsgesetzes zuständige Behörde das Vorliegen einer Behinderung und den Grad der Behinderung fest.

In guter Zusammenarbeit mit dem Sächsischen Landesamt für Familie und Soziales - in dessen Eigenschaft als Landesversorgungsamt - habe ich die bisher in diesem Verfahren verwendeten Vordrucke datenschutzrechtlich geprüft. Die Überarbeitung ist abgeschlossen.

Zu den gemäß § 67 a Abs. 1 SGB X im Antragsvordruck erforderlichen Hinweisen für den Antragsteller habe ich eine Formulierung angeregt, die sich weitgehend an den

Vorschlägen orientiert, die 1995 in den Gesprächen zwischen dem Bundesbeauftragten für den Datenschutz, dem Bundesministerium für Arbeit und Sozialordnung und den Spitzenverbänden der Sozialleistungsträger über Datenschutzklauseln in Vordrucken und Merkblättern der Leistungsträger erarbeitet worden waren. Sie lautet: *„Um sachgerecht über Ihren Antrag entscheiden zu können, werden auf der Grundlage der §§ 1 bis 4 des Schwerbe-hindertengesetzes von Ihnen Informationen und Unterlagen benötigt. Sie werden deshalb gebeten, den Antrag sorgfältig und vollständig - möglichst in Maschinen- oder Blockschrift - auszufüllen und uns die erbetenen Nachweise möglichst umgehend zu überlassen. Wir bitten Sie auch, die beigefügten Einwilligungserklärungen zu unterschreiben und zurückzuschicken. Wenn sich Unterlagen zu den festzustellenden Behinderungen (z. B. Befundberichte, ärztliche Gutachten, Kurschlußgutachten, EKG, Labor- und Röntgenbefunde) in Ihren Händen befinden, fügen Sie bitte alle diesem Antrag bei! Sie können dadurch zu einer beschleunigten Bearbeitung und Entscheidung beitragen. Ihre Mithilfe, die in den §§ 60 bis 65 des Allgemeinen Teils des Sozialgesetzbuches (SGB I) vorgeschrieben ist, erleichtert uns eine rasche Erledigung Ihrer Angelegenheit. Die Grenzen Ihrer Mitwirkungspflicht ergeben sich aus § 65 SGB I.*

Bitte beachten Sie, daß wir Ihnen, wenn Sie uns nicht unterstützen, die Leistung ganz oder teilweise versagen oder entziehen können (§ 66 SGB I).“

Auch bei der Einwilligungserklärung wurde weitgehende Übereinstimmung erzielt: *„Ich bin vorbehaltlich nachfolgender Erklärung damit einverstanden, daß das Amt für Familie und Soziales - Versorgungsamt - im Rahmen der Bearbeitung meines Antrags nach dem Schwerbehindertenrecht von den Krankenhäusern, Rehabilitationseinrichtungen und Trägern der Sozialversicherung, die ich im Antrag angegeben habe oder die aus den von mir überlassenen Unterlagen ersichtlich sind, Krankenpapiere, Aufzeichnungen, Krankengeschichten, Untersuchungsbefunde und Röntgenbilder einholt, die es für die Entscheidung über meinen Antrag benötigt. Ich bin damit einverstanden, daß das Amt für Familie und Soziales - Versorgungsamt - von Ärzten, die mich behandelt haben, Auskünfte einholt und Unterlagen beizieht. Das schließt die Unterlagen ein, die diese Ärzte und Einrichtungen von anderen Ärzten und Einrichtungen erhalten haben.*

Folgende Ärzte bzw. Einrichtungen schließe ich ausdrücklich von dieser Einwilligung aus:
...
Soweit sie durch diese Erklärung nicht ausdrücklich ausgeschlossen sind, entbinde ich die beteiligten Ärzte von ihrer Schweigepflicht und stimme der Verwertung der Auskünfte und Unterlagen im Verwaltungsverfahren zu.

Ärztliche Untersuchungen, die während des laufenden Verfahrens stattgefunden haben, werde ich dem Amt für Familie und Soziales - Versorgungsamt - umgehend mitteilen. Wenn ich bei dieser Mitteilung nichts Gegenteiliges erkläre, bin ich damit einverstanden, daß auch die Unterlagen über diese ärztlichen Untersuchungen

angefordert werden.

Datum.....
Unterschrift.....“

Nach dieser Erklärung darf das Versorgungsamt dann, wenn sich aus den von einem benannten Arzt überreichten Unterlagen ergibt, daß weitere Ärzte eingeschaltet werden müssen, von diesen ohne erneute Einwilligung Auskünfte einholen und Unterlagen anfordern. Nach meiner Auffassung wäre es der datenschutzfreundlichere Weg, dem Betroffenen eine erneute Einwilligungserklärung vorzulegen, um ihm die Möglichkeit zur Prüfung zu geben, ob diese Unterlagen an das Versorgungsamt gelangen sollen. Das Landesversorgungsamt fürchtet jedoch einen unangemessenen Verwaltungsmehraufwand und das Unverständnis des Antragstellers.

Bei dem gemäß § 76 Abs. 2 Nr. 1 SGB X erforderlichen Hinweis auf das Widerspruchsrecht hätte ich es begrüßt, wenn das Versorgungsamt dem Betroffenen vor der Herausgabe von Unterlagen an einen anderen Sozialleistungsträger den Zweck des Gutachtens und die Person des Gutachters mitteilt, um ihm Gelegenheit zu geben, der Übermittlung im konkreten Fall zu widersprechen. Ebenso wäre ein erneuter Hinweis auf die beabsichtigte Übermittlung und das Widerspruchsrecht zumindest dann sinnvoll, wenn seit dem Hinweis zu Beginn des Verwaltungsverfahrens eine längere Zeit vergangen ist. Dasselbe gilt für eine Information über das Widerspruchsrecht durch das Versorgungsamt, wenn der andere Sozialleistungsträger nicht selbst zu den Hinweisen nach § 76 SGB X verpflichtet ist (dieses Verfahren ist vorgesehen für den Träger der gesetzlichen Unfallversicherung in § 200 Abs. 1 SGB VII). Das Landesversorgungsamt sieht jedoch folgende Formulierung vor: *„Ich nehme zur Kenntnis, daß*

- *die Auskünfte und Unterlagen, die das Amt für Familie und Soziales - Versorgungsamt - im Zusammenhang mit dem Verfahren nach dem Schwerbehindertengesetz von einem Arzt erhalten hat, nach den geltenden datenschutzrechtlichen Bestimmungen an einen anderen Sozialleistungsträger übermittelt werden dürfen, soweit dies für die gesetzliche Aufgabenerfüllung des Amtes für Familie und Soziales - Versorgungsamt - oder des anderen Leistungsträgers erforderlich ist (§§ 69 Abs. 1, 76 Abs. 2 Nr. 1 des Zehnten Buches Sozialgesetzbuch - SGB X),*
- *ich dieser Datenübermittlung jederzeit widersprechen kann“.*

Bei der Anforderung von Unterlagen und der Erteilung von Auskünften muß die Erhebung personenbezogener Daten, die nicht für die Entscheidung über den Antrag erforderlich sind, vermieden werden. Andererseits ist jedoch darauf zu achten, daß nicht zu wenige Angaben verlangt werden und damit eine sachgerechte Entscheidung, unter Umständen zu Lasten des Antragstellers, nicht getroffen werden kann. Es ist aus fachlicher Sicht zu entscheiden, wie präzise eine Eingrenzung möglich ist. Falls erforderlich, muß eine weitergehende Formulierung gewählt werden. Unter diesem

Vorbehalt habe ich angeregt, die Frage nach den behandelnden Ärzten wie folgt zu erläutern: *„Anzugeben sind nur solche Ärzte, Kliniken, Krankenhäuser und Rehabilitationseinrichtungen, die Sie in den letzten fünf Jahren wegen einer Erkrankung behandelt haben, die im Zusammenhang mit den festzustellenden Behinderungen stehen können.“*

Die im Vordruck verlangten Angaben beschränken sich auf das Wesentliche. In den wenigen Punkten, in denen eine unterschiedliche Auffassung bestand, wurde Einigkeit erzielt.

10.2.3 Ausführung des Schwerbehindertengesetzes: Zuschüsse für den Arbeitgeber

Die Stadt Görlitz teilte mir mit, das Amt für Familie und Soziales Dresden (Zweigstelle der Hauptfürsorgestelle) fordere im Zusammenhang mit Zuwendungen zur Durchführung des Schwerbehindertengesetzes nunmehr die monatlichen Lohnscheine und Anwesenheitsnachweise sowohl des Behinderten als auch des Betreuers an. Bisher habe es genügt, eigens angefertigte Lohn- bzw. Gehaltsauszüge zu übersenden.

Die Arbeitgeber können Zuschüsse zur Abgeltung außergewöhnlicher Belastungen erhalten, die mit der Beschäftigung eines Schwerbehinderten verbunden sind, der nach Art oder Schwere seiner Behinderung im Arbeits- und Berufsleben besonders betroffen ist (§ 27 Abs. 1 SchwbAV). Art und Höhe der Zuwendung bestimmen sich nach den Umständen des Einzelfalls (§§ 27 Abs. 3, 26 Abs. 2 SchwbAV).

Grundlage des Zuschusses zu den außergewöhnlichen Aufwendungen im Sinne von § 6 Abs. 1 Nr. 1 Buchst. a, b und d SchwbG sind die tatsächlichen Personalkosten für den Behinderten und den Betreuer (Nr. 4.2 der " Richtlinie des Sächsischen Staatsministeriums für Soziales, Gesundheit und Familie für die Gewährung von Hilfen an Arbeitgeber zur Abgeltung außergewöhnlicher Belastungen bei der Beschäftigung Schwerbehinderter nach § 27 SchwbAV"). Für den Zuschuß zum Arbeitsentgelt für Schwerbehinderte im Sinne von § 6 Abs. 1 Nr. 1 Buchst. c SchwbG ist Bemessungsgrundlage das Bruttoarbeitsentgelt des Schwerbehinderten zuzüglich des Arbeitgeberanteils zur Sozialversicherung (Nr. 5.1 der Richtlinie).

In dem Zuwendungsbescheid wird, um die Personalkosten bzw. das Bruttoarbeitsentgelt feststellen zu können, als Anlage zum Auszahlungsantrag die Beifügung der Lohnscheine und Anwesenheitsnachweise des Schwerbehinderten und des Betreuers gefordert. Bei Abwesenheit des Behinderten ist der Grund anzugeben.

Bei den Daten des Behinderten handelt es sich gemäß § 67 Abs. 1 SGB X um Sozialdaten. Dies gilt auch für den Betreuer und seinen Vertreter, weil auch diese Daten vom Amt für Familie und Soziales im Hinblick auf seine Aufgaben nach dem Schwerbehindertengesetz erhoben, verarbeitet und genutzt werden.

Das Amt für Familie und Soziales darf die Daten nur erheben, wenn ihre Kenntnis zur Erfüllung seiner Aufgaben erforderlich ist (§ 67 a Abs. 1 SGB X).

Mit dem Sächsischen Landesamt für Familie und Soziales in dessen Eigenschaft als Hauptfürsorgestelle besteht Einigkeit darüber, daß die Vorlage der Lohnscheine nicht erforderlich ist. Es genügt ein Auszug, dessen Umfang noch im einzelnen festzulegen ist.
Weiterhin muß geklärt werden, welche Form des Anwesenheitsnachweises in Betracht kommt. Mit der Vorlage der "Stempelkarte" werden jedenfalls zu viele Daten übermittelt. Auch die Angabe des Grundes für die Abwesenheit ist nicht erforderlich.

Ich habe der Hauptfürsorgestelle ein gemeinsames Gepräch zur Klärung der Problematik angeboten.

Die Hauptfürsorgestelle teilte mir mit, der Schwerbehinderten-Ausschuß der Arbeitsgemeinschaft der Deutschen Hauptfürsorgestellen sei zu der Auffassung gelangt, die bisherige Förderpraxis nach § 27 SchwAV erfordere einen hohen Verwaltungsaufwand und führe zu datenschutzrechtlichen Problemen. Aus diesem Grund sei ein Unterausschuß zu § 27 SchwbAV gebildet worden, der eine neue Förderrichtlinie und verwaltungstechnische Festlegungen unter datenschutzrechtlichen Gesichtspunkten vorlegen solle.

Sobald sie erarbeitet ist, werde ich zu einem gemeinsamen Gespräch eingeladen.

10.2.4 Datenverarbeitung im Auftrag zur Wohngeldberechnung

In meinem 4. Tätigkeitsbericht habe ich mich unter 10.2.6 mit den Mängeln in den Verträgen befaßt, die zwischen den Zweckverbänden und den Gemeinden für Zwecke der Auftragsdatenverarbeitung abgeschlossen worden waren. Durch Zusatzvereinbarungen sind diese Mängel inzwischen beseitigt worden.

Die Zweckverbände haben sich verpflichtet, bei der automatisierten Wohngeldberechnung die technischen und organisatorischen Maßnahmen zur Gewährleistung der Datensicherheit so zu treffen, daß die in der Anlage zu § 78 a SGB X genannten Anforderungen erfüllt werden. Außerdem haben sie sich verpflichtet, nur Unterauftragnehmer einzusetzen, die diese Voraussetzungen ebenfalls erfüllen. Alle Unterauftragnehmer werden mit Namen und Anschrift in den Verträgen genannt.

Zum Vertragsbestandteil wurde eine IT-Sicherheitsrichtlinie, die den auftraggebenden Gemeinden einen bestimmten Sicherheitsstandard garantieren und ihnen einen Überblick über die Maßnahmen im einzelnen verschaffen soll. Denn gemäß § 80 Abs. 1 SGB X bleibt der Auftraggeber auch bei einer Datenverarbeitung im Auftrag für die Einhaltung des Datenschutzes verantwortlich. Zudem ist er gemäß § 80 Abs. 2 SGB X verpflichtet, gegebenenfalls Weisungen zur Ergänzung der vorhandenen technischen

und organisatorischen Datensicherheitsmaßnahmen und des Datenschutzes zu erteilen und getroffene Maßnahmen zu kontrollieren. Damit die Gemeinden dies durchsetzen können, haben sich die Zweckverbände vertraglich verpflichtet, diesbezüglichen Forderungen zu entsprechen.

Vereinbart wurde auch, daß die Zweckverbände für das Wohngeldverfahren ein Dateien- und Geräteverzeichnis erstellen, das die Voraussetzungen des § 10 SächsDSG erfüllt, es den Gemeinden zur Ergänzung des eigenen Dateien- und Geräteverzeichnisses zur Verfügung zu stellen und aktualisierte Fassungen unaufgefordert zu übersenden.

10.2.5 Fragebogen für Berufs- und Vereinsbetreuer zur Feststellung von Interessenkonflikten

Ist eine volljährige Person aufgrund einer psychischen Krankheit oder einer körperlichen oder geistigen Behinderung nicht in der Lage, die eigenen Angelegenheiten zu erledigen, bestellt das Vormundschaftsgericht einen Betreuer. Das Gericht wird bei dieser Aufgabe gemäß § 8 BtBG durch Betreuungsbehörden unterstützt, die eigenständig ermitteln, ob und in welchem Umfang eine Person Betreuung benötigt und welcher Betreuer geeignet sein könnte. Der festgestellte Sachverhalt sowie der in Betracht kommende Betreuer werden dem Gericht zur Entscheidungsfindung mitgeteilt. Da bei der Auswahl des Betreuers auf die Gefahr von Interessenkonflikten Rücksicht zu nehmen ist (§ 1897 Abs. 5 BGB), muß u. a. sichergestellt werden, daß ein Betreuer sein Wissen aus dem Betreuungsverhältnis nicht zum eigenen Vorteil ausnutzen kann, z. B. durch die Weitergabe von Informationen über freiwerdende Wohnungen an den im Immobilienbereich tätigen Ehepartner oder die Beauftragung des eigenen Pflegedienstes.

Eine Betreuungsbehörde hat mich um die Bewertung eines Fragebogens gebeten, der dazu dienen soll, bei bestellten und künftigen Betreuern Interessenkonflikte zwischen der Tätigkeit als Betreuer und eventuellen Nebentätigkeiten zu erkennen. Zu diesem Zweck wird nach direkten oder indirekten Beteiligungen an Immobilien-, Antiquitäten- und Räumungsfirmen sowie Pflegediensten gefragt wie auch nach Tätigkeiten in diesen Bereichen.

Ich bezweifele, ob mit dem Fragebogen das angestrebte Ziel erreicht werden kann, denn aus der speziellen Konstellation eines Einzelfalls können sich Interessenkonflikte ergeben, die der vorliegende Fragenkatalog nicht erfaßt (z. B., wenn ein guter Freund des Betreuers Immobilienmakler ist). Deshalb sollten Leerzeilen für frei zu formulierende Fragen vorgesehen werden. Noch besser wäre jedoch eine umfassende Belehrung des Betreuers in bezug auf den konkreten Betreuungsfall.

Gegen die einzelnen Fragen habe ich keine Bedenken erhoben, jedoch gegen eine generelle und schematische Verwendung des Fragebogens, und zwar aus folgenden Gründen:

Wenn § 1897 Abs. 5 BGB besagt, daß bei der Auswahl des Betreuers auf die Gefahr von Interessenkonflikten Rücksicht zu nehmen ist, heißt das nach Auffassung einschlägiger Kommentare, daß es sich um *konkrete Gefahren* oder *konkret gegebene Umstände* eines Interessenkonflikts handeln muß (Palandt Rdnr. 8 zu § 1897 BGB mit Hinweis auf BT-Drucks. 11/4528 S. 128; Knittel, Kommentar zum Betreuungsgesetz, Stand 10. Ergänzungslieferung, § 1897 BGB, S. 34). Eine solche Einschätzung ist jedoch nur anhand des Einzelfalls möglich, zu dem sowohl die Situation des Betreuten als auch die des Betreuers gehören. Ausgangspunkt für die Befragung des Betreuers muß die Situation des Hilfsbedürftigen sein, die der Betreuungsbehörde durch die Sachverhaltsermittlung hinreichend bekannt ist. Deshalb erübrigt sich eine Befragung des Betreuers, wenn die persönlichen und sachlichen Verhältnisse des Hilfsbedürftigen keine Ansatzpunkte für Interessenkonflikte aufgrund von Nebentätigkeiten bieten, z. B. weil der Hilfsbedürftige ohne Einkommen oder Vermögen in einem Heim lebt und es deshalb unerheblich ist, ob der Betreuer an einem Pflegedienst oder einem Räumungsunternehmen beteiligt ist. Entsprechendes gilt, wenn weder Immobilien noch Antiquitäten vorhanden sind oder erworben werden können, der Betreuer aber im Immobiliengeschäft oder Antiquitätenhandel tätig ist.

In formeller Hinsicht war der Fragebogen zu überarbeiten, weil der Zweck der Datenerhebung nicht angegeben war und der Hinweis fehlte, daß keine Rechtsvorschrift zur Auskunft verpflichtet, die Beantwortung der Fragen jedoch Voraussetzung für die Gewährung von Rechtsvorteilen ist (§ 11 Abs. 2 SächsDSG).

10.2.6 Einhaltung datenschutzrechtlicher Vorschriften bei der Bearbeitung von Wohngeldanträgen

In einer Eingabe beschwerte sich eine Wohngeldempfängerin darüber, daß die Wohngeldstelle im Rahmen der Antragsbearbeitung ihren Arbeitslosenbescheid, den Mietvertrag einschließlich Betriebskostenabrechnung sowie den Internatsmietvertrag, eine Studienbescheinigung, BAföG-Bescheide und Kostenbelege für die auswärtig studierende Tochter verlangte und Kopien dieser Unterlagen zur Wohngeldakte nahm.

Ich habe die Wohngeldakte der Petentin geprüft und festgestellt, daß die angeforderten Unterlagen erforderlich waren.

Arbeitslosenhilfebescheid
Die Höhe der im Arbeitslosenhilfebescheid ausgewiesenen Arbeitslosenhilfe ist Grundlage für die Berechnung des Familieneinkommens (§§ 8, 9 Nr. 3 i. V. m. Anlage 7 WoGSoG).

Mietvertrag - Betriebskostenabrechnung
Der Mietvertrag ist der Nachweis für die Antragsberechtigung, die gemäß § 3 Abs. 1 WoGSoG demjenigen zusteht, der die Miete vertragsgemäß zu entrichten hat. Außerdem ergibt sich aus ihm, ob Räume zur gewerblichen Nutzung gemietet wurden.

Für sie wird kein Wohngeld gewährt (§ 7 Abs. 2 WoGSoG). Der Mietvertrag belegt Wohnungsgröße und Heizungsart, von denen der Zuschlag für Wärme und Warmwasser abhängig ist (§ 21 WoGSoG). Allerdings darf dieser Zuschlag die zur Wärme- und Warmwasser*erzeugung* tatsächlich aufgewendeten Kosten (Brennstoffe, Betriebskosten) nicht übersteigen. Eine solche Prüfung ist nur anhand der Betriebskostenabrechnung möglich.

Internatsmietvertrag, Studienbescheinigung, BAföG-Bescheide
Ist ein zum Haushalt zu rechnendes Familienmitglied auswärtig untergebracht, werden bei der Ermittlung des Jahreseinkommens Aufwendungen zur Erfüllung gesetzlicher Unterhaltsverpflichtungen bis zu 200 DM monatlich abgesetzt (§ 11 Nr. 1 WoGSoG). Bei Kindern, die sich an einem anderen Ort aufhalten und dort einer Berufsausbildung nachgehen, gehen die Wohngeldstellen stets davon aus, daß sie weiterhin zum Haushalt des Antragstellers gehören. Deshalb verlangte die Wohngeldstelle den Nachweis, daß monatliche Aufwendungen in Höhe von 200 DM zur Erfüllung der gesetzlichen Unterhaltspflicht erbracht werden und das Kind tatsächlich - wie im Antrag angegeben - studiert.

Der Internatsmietvertrag belegt die auswärtige Unterbringung und die dafür aufzuwendenden Kosten. Die Studienbescheinigung belegt die Immatrikulation an einer Hochschule, nicht aber die Aufnahme oder Durchführung des Studiums, also die tatsächliche Berufsausbildung. Nach den Erfahrungen der Wohngeldstelle sind viele der immatrikulierten Studenten (vorübergehend) berufstätig oder werden von anderen Personen als dem Antragsteller maßgeblich unterstützt. Um dies festzustellen bzw. auszuschließen, hat die Wohngeldstelle BAföG-Bescheide angefordert, weil aus ihnen Nebeneinkünfte und Zahlungen Dritter ersichtlich sind.

Kostenbelege
Die Belege waren erforderlich, weil die Petentin nur regelmäßige Unterhaltszahlungen in Höhe von 100 DM glaubhaft machen konnte, für die Gewährung des vollen Freibetrags jedoch der Nachweis oder zumindest das Glaubhaftmachen darüber hinausgehender Aufwendungen Voraussetzung ist.

Ich kann nachvollziehen, daß ein ehrlicher Antragsteller die Vielzahl von Nachweisen als unverhältnismäßig empfindet. In Zeiten knapper öffentlicher Haushaltsmittel ist es jedoch genauso nachvollziehbar, daß sich die Verwaltung keine großzügige Handhabung leisten kann oder wegen des zunehmenden Leistungsmißbrauchs verstärkt auf Nachweisen besteht.

Aus meiner Sicht bestehen keine Bedenken, Kopien von Unterlagen zu den Akten zu nehmen, soweit sie die Verwaltungsentscheidung dokumentieren und im Hinblick auf Widerspruchs- oder Gerichtsverfahren und gegenüber Rechnungsprüfungsbehörden Bedeutung haben können.

10.2.7 Erforderlichkeit von Einkommensteuerbescheiden für die Gewährung von Erziehungsgeld nach dem Bundeserziehungsgeldgesetz

Regelmäßig fordern die Ämter für Familie und Soziales im Zusammenhang mit der Gewährung von Bundeserziehungsgeld die Antragsteller zur Vorlage des letzten Einkommensteuerbescheids auf. Ein Antragsteller hielt die Angaben über die Einkünfte seiner Ehefrau für nicht erforderlich und schwärzte sie daher. Als das Amt auf dem *vollständigen* Einkommensteuerbescheid bestand, bat er mich um eine Prüfung der Zulässigkeit. Ich bin zu dem Ergebnis gekommen, daß der vollständige Einkommensteuerbescheid aus folgenden Gründen erforderlich ist:

Das Bundeserziehungsgeld beträgt grundsätzlich 600,- DM monatlich und wird für zwei Jahre gewährt. Übersteigt das Einkommen nicht dauernd getrennt lebender Ehegatten eine bestimmte Einkommensgrenze, die nach Lebensalter des Kindes und Familiengröße variiert, mindert sich das Erziehungsgeld nach einem komplizierten Berechnungsmodus. Dieser knüpft unmittelbar an die Beträge an, um die das Einkommen die betreffende Einkommensgrenze übersteigt, wobei für die Minderung in den ersten zwölf Lebensmonaten des Kindes das Einkommen im Kalenderjahr der Geburt maßgebend ist.

Was als Einkommen gilt, regelt das Bundeserziehungsgeldgesetz, und es stellt dabei einen unmittelbaren Bezug zum Einkommensteuerrecht her. So sind z. B. nur Einkünfte aus Einkunftsarten anzusetzen, die auch bei der Einkommensteuer berücksichtigt werden. Ihre Höhe ist nach steuerrechtlichen Vorschriften zu ermitteln, die zu *negativen* Einkünften führen können. Für die Einkommensberechnung nach dem Bundeserziehungsgeldgesetz werden jedoch nur die *positiven* steuerlichen Einkünfte angesetzt, ebenso die im Ausland erzielten Einkünfte, die im Inland aufgrund eines Doppelbesteuerungsabkommens nicht versteuert werden. Für die Einkommensberechnung nach dem Bundeserziehungsgeldgesetz wird der Gesamtbetrag dieser Einkünfte um einen Vomhundertsatz vermindert, dessen Höhe davon abhängt, ob das Finanzamt Vorsorgeaufwendungen abgezogen hat. Außerdem vermindert es sich um Unterhaltsleistungen, die an geschiedene Ehegatten und sonstige Personen gezahlt werden, wenn diese Leistungen nach Einkommensteuerrecht abzugsfähig sind.

Nach § 67a Abs. 1 SGB X ist das Erheben von Sozialdaten nur zulässig, wenn ihre Kenntnis zur Aufgabenerfüllung der erhebenden Stelle erforderlich ist. Streng genommen sind dies die positiven Einkünfte einschließlich der Tatsache, ob sie einem Doppelbesteuerungsabkommen unterliegen, sowie die nach Einkommensteuerrecht als Sonderausgaben bzw. außergewöhnliche Belastungen abzugsfähigen Unterhaltsleistungen. Alle übrigen Angaben könnten - nach entsprechender Erläuterung - vom Antragsteller geschwärzt werden.

Da einem Steuerbescheid mit geschwärzten Einkünften nicht mehr zu entnehmen ist, ob ausschließlich negative Einkünfte unkenntlich gemacht wurden, ist die Vorlage

eines Steuerbescheids ohne Schwärzungen im Teil "Einkünfte" erforderlich. Nur so hat er überhaupt Nachweiswert. Erläuterungen im Antragsformular, welche Besteuerungsgrundlagen geschwärzt werden dürfen und welche nicht, dürften - abgesehen vom Umfang - auf das Unverständnis der meisten Antragsteller treffen, weil differenzierte steuerliche Erläuterungen ohne entsprechende Fachkenntnis leicht mißverstanden werden. Im übrigen schließt eine sachgerechte Entscheidung stets eine Prüfung zugunsten des Antragstellers ein. Unter dem Gesichtspunkt, daß komplizierte und umfangreiche Anträge oft unvollständig oder fehlerhaft ausgefüllt werden, ermöglicht ein Steuerbescheid eine wirksame Plausibilitätskontrolle des Antrags. Plausibilitätsmerkmale sind z. B. Kinderfreibeträge, Freibeträge aufgrund einer Körperbehinderung und die Erläuterungen zum Steuerbescheid. Auch deswegen ist der vollständige Einkommensteuerbescheid erforderlich.

Wie mir das Amt für Familie und Soziales mitgeteilt hat, wurden - nachdem der Petent den vollständigen Steuerbescheid vorgelegt hatte - sogar Tatsachen bekannt, die zu einer Erhöhung des Bundeserziehungsgeldes führten, weil auch hier der Antrag unvollständig ausgefüllt worden war.

Der Fall zeigt wie das vorstehend unter 10.2.6 erörterte Beispiel, daß bei der Prüfung, ob ein bestimmter Nachweis zu einem Antrag erforderlich ist oder nicht, eine "punktuelle Betrachtungsweise" unangebracht ist. Anders ausgedrückt: Nicht jeder von einer Behörde geforderte Nachweis darf für sich betrachtet werden. Innerhalb des einzelnen Nachweises darf nicht nur die Erforderlichkeit jeder einzelnen Angabe hinterfragt werden. Vielmehr muß der Plausibilitätszusammenhang im Auge behalten werden, der sich oft erst aus dem "Zusammenspiel" mehrerer Nachweise ergibt. Damit ist der Plausibilitätszusammenhang ein eigenständiges Kriterium für die Erforderlichkeit.

10.2.8 Anforderung der Epikrise beim Krankenhaus durch den örtlichen Träger der Sozialhilfe

Ein Krankenhaus teilte mir mit, das Sozialamt fordere nach einer stationären Behandlung zur Prüfung seiner Zuständigkeit die vollständige Epikrise, also einen Abschlußbericht über Anamnese, Diagnose und Behandlung des Patienten, an. Das Sozialamt begründete diese Anforderung damit, der Landeswohlfahrtsverband Sachsen verlange bei der Entgiftung eines Alkoholabhängigen in Fachkrankenhäusern für Suchtkranke oder in psychiatrischen Fachkrankenhäusern, Fachabteilungen und Spezialeinrichtungen die Epikrise, um zu überprüfen, ob diese Entgiftung in einer solchen Einrichtung hätte erfolgen müssen.

Gemäß § 3 Abs. 3 Satz 2 SächsAGBSHG ist der Landeswohlfahrtssverband als überörtlicher Träger der Sozialhilfe sachlich zuständig für die Krankenhilfe nach § 37 BSHG, wenn Hilfe in einer der oben erwähnten Einrichtung zu gewähren ist. Die Kosten für die Entwöhnungsbehandlung eines Alkoholkranken hat er daher zu tragen, weil sie in einer solchen Facheinrichtung erfolgen muß, die Kosten der Entgiftung

jedoch nur, wenn auch sie in der Facheinrichtung durchgeführt werden mußte. Aus der Formulierung „zu gewähren ist“ zieht er also die Schlußfolgerung, nicht entscheidend sei, ob die Entgiftung in der Einrichtung erfolgt ist, sondern ob dies medizinisch notwendig war.

Der Landeswohlfahrtsverband bestätigte jedoch nicht die Darstellung des Sozialamts, daß er für diese Prüfung die Vorlage der Epikrise verlange. Sie sei vielmehr weder für ihn noch für den örtlichen Träger der Sozialhilfe zur Prüfung seiner Zuständigkeit erforderlich. Daher begnüge er sich mit der Feststellung des Fachkrankenhauses bzw. der Fachabteilung, ob die Entgiftung dort hätte erfolgen müssen. Bisher sei dies in keinem Fall bejaht worden.

Diese Diskussion ist Teil eines bundesweiten Streits zwischen den örtlichen und den überörtlichen Trägern der Sozialhilfe über die sachliche Zuständigkeit (und damit die Pflicht zur Kostentragung) einer Entgiftung. In mehreren schiedsgerichtlichen Verfahren auf der Grundlage der Fürsorgerechtsvereinbarung, u. a. bei der Spruchstelle für Fürsorgestreitigkeiten Stuttgart, wird versucht, eine Lösung zu finden. Dieser Streit darf nicht auf dem Rücken der Betroffenen ausgetragen werden. Ein Grund, die für andere Ärzte, insbesondere nachbehandelnde, bestimmte und damit sehr ausführliche, u. U. sogar Angaben zum sozialen Umfeld enthaltene Epikrise anzufordern, besteht nicht.

Auch bei der Überprüfung auffällig hoher Rechnungen - ein weiterer Fall, in dem nach Angaben des Sozialamts die vollständige Epikrise verlangt wird - wird man andere Möglichkeiten haben, als deren Vorlage. Das Sozialamt wandte ein, aus der Beantragung der Kostenübernahme allein sei nicht erkennbar, ob es sich um eine sogenannte Gesamtmaßnahme handle, die sowohl Entgiftung als auch Entwöhnung beinhalte. Dennoch werde man künftig keine Epikrisen, sondern lediglich entsprechende Aussagen bezüglich einer Gesamtmaßnahme beim Krankenhaus anfordern.

Das Sozialamt hat zugesagt, nicht erforderliche Angaben in den in der Vergangenheit angeforderten Epikrisen § 84 Abs. 2 SGB X entsprechend zu schwärzen.

10.2.9 Unter welchen Voraussetzungen wird ein eingetragener Verein, der als Träger der freien Jugendhilfe anerkannt ist, zur öffentlichen Stelle?

Ein eingetragener Verein, der als Träger der freien Jugendhilfe anerkannt ist, bereitet geistig leicht behinderte Jugendliche auf einen Beruf vor. Förderung und Finanzierung erfolgen im Rahmen der Kinder- und Jugendhilfe (SGB VIII) und des Arbeitsförderungsgesetzes. Der Verein beabsichtigte, diese Mädchen und Jungen anhand eines Fragebogens um Auskunft über ihr soziales Umfeld und ihre Lebenssituation zu bitten. Die meisten von ihnen leben in ungeordneten Familienverhältnissen oder in Heimen.

Diese Befragung erschien einem Abgeordneten des Sächsischen Landtags nicht nur wegen ihres Inhalts problematisch (z. B., ob die Mutter einen Freund hat), sondern auch, weil sie den jungen Betroffenen als "Hausaufgabe" mitgegeben worden war und sie dies als Zwang zur Beantwortung der Fragen empfanden. Der Abgeordnete bat mich, tätig zu werden. Ich habe ihm mitteilen müssen, daß dies nicht möglich ist, weil es sich hier um eine nicht-öffentliche Stelle handelt, die aus dem Anwendungsbereich des Sächsischen Datenschutzgesetzes herausfällt, und zwar aus folgenden Gründen:

Ein eingetragener Verein ist eine juristische Person des privaten Rechts. Er gilt gemäß § 2 Abs. 2 SächsDSG nur dann und insoweit als öffentliche Stelle, als er Aufgaben der öffentlichen Verwaltung wahrnimmt. Die Frage war also, ob die von dem Verein im Rahmen der Kinder- und Jugendhilfe nach dem SGB VIII wahrgenommene Aufgabe eine Aufgabe der öffentlichen Verwaltung ist. Dies habe ich verneinen müssen.

Das SGB VIII unterscheidet zwischen der freien und der öffentlichen Jugendhilfe. Jugendhilfe ist gemäß § 3 Abs. 1 SGB VIII "durch die Vielfalt von Trägern unterschiedlicher Wertorientierungen und die Vielfalt von Inhalten, Methoden und Arbeitsformen" gekennzeichnet. Bestimmte Aufgaben weist das SGB VIII ausschließlich der öffentlichen Jugendhilfe zu. Träger der öffentlichen Jugendhilfe sind damit stets öffentliche Stellen.

Die Träger der öffentlichen Jugendhilfe können gemäß § 76 SGB VIII bestimmte Aufgaben auf anerkannte Träger der freien Jugendhilfe zur Ausführung übertragen. Ob dadurch eine private Stelle zwangsläufig zu einer öffentlichen Stelle wird und in meinen Zuständigkeitsbereich fällt, ist noch nicht ausdiskutiert. Auf keinen Fall wird eine private Stelle zu einer öffentlichen Stelle, wenn sie von sich aus eine Aufgabe wahrnimmt, die auch Aufgabe der öffentlichen Verwaltung ist. Das ist hier der Fall. Denn es haben Privatpersonen einen Verein zur Erreichung eines gemeinnützigen Zwecks gegründet und damit im Privatbereich auf privatrechtlicher Basis eine Einrichtung geschaffen, deren Zweck sich mit denen der Jugendhilfe deckt. Die für den Betrieb einer solchen Einrichtung gesetzlich vorgeschriebene Erlaubnis ist keine Aufgabenübertragung.

10.2.10 Vorlage des Sozialversicherungsausweises beim Sächsischen Gemeindeunfallversicherungsverband (SGUVV)

Der SGUVV bat im Zusammenhang mit einem aktuellen Feststellungsverfahren den Antragsteller um "Überlassung von Kopien der vollständigen Behandlungsnachweise aus dessen Sozialversicherungsausweis der ehemaligen DDR".

Bereits in einem früheren ähnlichen Fall hatte der SGUVV aufgrund einer datenschutzrechtlichen Prüfung zugesagt, in Zukunft Schreiben, mit denen Kopien des SV- Ausweises angefordert werden, zu präzisieren. Es sollte erläutert werden, wofür die Kopien erforderlich sind, und eine Beschränkung auf einen bestimmten Zeitraum erfolgen.

Der Vordruck, mit dem nunmehr die Vorlage des SV-Ausweises erbeten wurde, ist genauer als der früher verwendete. Entgegen der damaligen Absprache fehlt jedoch eine Beschränkung auf einen bestimmten Zeitraum. Auch die Unterrichtung der Betroffenen ist noch nicht ausreichend. So muß noch deutlicher formuliert werden, daß nicht der gesamte SV-Ausweis, sondern nur die medizinisch relevanten Teile vorzulegen sind. Ferner sind die Hinweispflichten des § 67 Abs. 3 SGB X nicht erfüllt.

Der SGUVV teilte mir mit, daß eine unserer Absprache entsprechende Begrenzung des Zeitraums, für den Kopien des Sozialversicherungsausweises vorgelegt werden sollen, in einer Dienstanweisung geregelt worden sei. Im hier vorliegenden Fall sei diese Einschränkung aus Versehen oder wegen seiner Besonderheiten jedoch nicht berücksichtigt worden.
Für den Fall, daß auch von anderen Versicherten nicht erforderliche Kopien verlangt worden sein sollten, habe ich den SGUVV gebeten, diese Unterlagen gemäß § 84 Abs. 2 Satz 1 SGB X zu vernichten.

Ergänzend habe ich den SGUVV gebeten, nicht den Versichertennamen für die Bildung des Aktenzeichens zu verwenden. Üblicherweise nutzt er die ersten drei Buchstaben, für kurze Namen sogar den vollständigen Namen. Zur Abgrenzung der Sachakten dürften auch eine Ziffer oder nicht namensbezogene Buchstaben ausreichen.

Bei der Neugestaltung des Vordrucks sind meine datenschutzrechtlichen Einwände weitestgehend berücksichtgt worden. So wird in Zukunft der Zeitraum genannt, für den Kopien aus dem Sozialversicherungsausweis vorgelegt werden müssen. Weiterhin erfolgt auch ein deutlicher Hinweis darauf, daß nur Kopien der Heilbehandlungsnachweise erforderlich sind.
Insgesamt konnte somit Übereinstimmung erzielt werden.

10.3 Lebensmittelüberwachung und Veterinärwesen

10.3.1 Befugnisse von Lebensmittelüberwachungs- und Veterinärämtern zur Erhebung von Daten über Tierhalter

Ein Lebensmittelüberwachungs- und Veterinäramt bat mich um Auskunft, wie es sich Daten über Tierhalter in seinem örtlichen Zuständigkeitsbereich, insbesondere über kleinere tierhaltende Betriebe (z. B. Bauern, Imker oder Hundezüchter), beschaffen könne. Als Behörde des öffentlichen Gesundheitsdienstes sei es auf die Kenntnis der entsprechenden Daten angewiesen, um aufgabengemäß auch bisher nicht erfaßte tierhaltende Betriebe beraten und kontrollieren zu können. Bei welchen anderen öffentlichen Stellen Daten über Tierhalter vorhanden seien und aufgrund welcher Rechtsvorschriften es sich diese Daten von dort besorgen dürfe, sei unklar.

Ich habe dem Lebensmittelüberwachungs- und Veterinäramt mitgeteilt, wo eine Datenerhebung in Betracht kommt und wo sie verboten ist:

a) Gegenüber den Betroffenen, hier den Tierhaltern, bestehen für die in § 1 SächsGDG genannten Zwecke und die in § 8 Abs. 2 Nr. 2, 3, 4, 6 und 7 SächsGDG genannten Aufgaben die Datenerhebungsbefugnisse gemäß § 9 Abs. 1 Satz 1 SächsGDG. Danach dürfen die LÜVÄ als Behörden des öffentlichen Gesundheitsdienstes insbesondere alle zur Aufgabenerfüllung *erforderlichen* Auskünfte von den Betroffenen verlangen. Erforderlich zur Aufgabenerfüllung sind Angaben, ohne deren Kenntnis die Aufgaben der erhebenden Stelle nicht erfüllt werden könnten. Nicht ausreichend ist, wenn die Information lediglich zur Aufgabenerfüllung *dienlich* ist.

   Als Problem bleibt aber, daß gerade die Betroffenen, also die Tierhalter, den LÜVÄ unbekannt sind.

b) Gegenüber privaten Dritten, etwa Nachbarn der Tierhalter, bestehen Datenerhebungsbefugnisse gemäß § 9 Abs. 2 SächsGDG.

c) Im Verhältnis zu anderen Behörden des öffentlichen Gesundheitsdienstes (§ 2 SächsGDG) bestehen Erhebungs- und Übermittlungsbefugnisse gemäß §§ 6, 7 SächsGDG.

d) Im Verhältnis zu anderen öffentlichen Stellen, die keine Behörden des öffentlichen Gesundheitsdienstes sind, sind je nach Rechtsgebiet unterschiedliche Erhebungs- und Übermittlungsregelungen zu beachten. Im einzelnen kommen in Betracht:

   - Finanzbehörden
     Der Ermittlung bisher unbekannter Tierhalter bei den Finanzbehörden steht das Steuergeheimnis, § 30 AO, entgegen. Ausnahmen hiervon sind nur nach Maßgabe von § 30 Abs. 4 AO zulässig. Eine Offenbarung etwa von Einkünften aus Land-

und Forstwirtschaft für Zwecke der Ermittlung bisher unbekannter Tierhalter im Zuständigkeitsbereich eines LÜVA ist danach ausgeschlossen, denn sie diente weder der Durchführung eines Verfahrens (der Steuerbehörde) im Sinne des § 30 Abs. 2 AO noch ist ein Gesetz ersichtlich, welches die Offenbarung ausdrücklich zuließe noch hat der Betroffene zugestimmt (der Betroffene ist vielmehr nicht bekannt) noch führt ein LÜVA Strafverfahren in Steuersachen durch. Die Voraussetzungen von § 30 Abs. 4 Nr. 5 AO können in einem Verfahren, in dem es um die Ermittlung bisher unbekannter Tierhalter geht, ebenfalls nicht erfüllt sein.

- Die Sächsische Tierseuchenkasse

  Die Tierseuchenkasse speichert Tierhalter-Daten zum Zwecke der Beitragserhebung, §§ 16, 17 SächsAGTierSG. Sie erhält diese Angaben auf zweierlei Wegen: Das Statistische Landesamt übermittelt ihr die "Ergebnisse der Viehzählung" gemäß § 16 Abs. 4 Satz 1 SächsAGTierSG. Von der jeweiligen "Gemeinde- oder Stadtverwaltung" erhält die Tierseuchenkasse "die für die Beitragserhebung erforderlichen Angaben aus der Viehzählung" gemäß § 16 Abs. 4 Satz 2 SächsAGTierSG.

  Der Ermittlung bisher unbekannter Tierhalter bei der Tierseuchenkasse steht § 16 Abs. 8 BStatG entgegen. Nach dieser Vorschrift dürfen die aufgrund einer besonderen Rechtsvorschrift, hier § 16 Abs. 4 Satz 1 SächsAGTierSG, übermittelten Einzelangaben nur für die Zwecke verwendet werden, für die sie übermittelt wurden. Zweck der Übermittlung der "Ergebnisse der Viehzählung" vom Statistischen Landesamt an die Tierseuchenkasse ist die Erhebung von Beiträgen von den Tierhaltern. Mit der Weiter-Übermittlung dieser Daten an ein LÜVA zum Zwecke der Ermittlung bisher unbekannter Tierhalter würde ein anderer Zweck verfolgt; dies gerade erlaubt § 16 Abs. 8 Satz 1 BStatG nicht.

- Der Träger der Landwirtschaftlichen Unfallversicherung

  Der Ermittlung bisher unbekannter Tierhalter bei der Landwirtschaftlichen Berufsgenossenschaft als Träger der gesetzlichen Unfallversicherung stehen die Vorschriften über den Schutz der Sozialdaten (§§ 67 ff. SGB X) in der Regel nicht entgegen. Gemäß § 68 Abs. 1 Satz 1 SGB X dürfen u. a. Name, Vorname sowie die derzeitige Anschrift des Betroffenen u. a. an Behörden der Gefahrenabwehr übermittelt werden, soweit kein Grund zur Annahme besteht, daß dadurch schutzwürdige Interessen des Betroffenen beeinträchtigt werden. Die Lebensmittelüberwachungs- und Veterinärämter der Städte und Kreise sind Behörden der Gefahrenabwehr, weil ihre Aufgabe allgemein und im Einzelfall die Abwehr drohender Schäden für die Gesundheit von Mensch und Tier (§ 8 Abs. 2, insbesondere etwa Nr. 4 SächsGDG) ist. Die Erhebung von Tierhalter-Daten bei der Landwirtschaftlichen Berufsgenossenschaft halte ich daher im Einzelfall für zulässig: Unter Voraussetzungen von § 11 Abs. 4 Nr. 8 SächsDSG als Datenerhebung bei einem Dritten gemäß § 13 Abs. 1 i. V. m. § 12 Abs. 2 Nr. 1 SächsDSG.

- Gewerbeämter

Die Gewerbeämter speichern Daten über Tierhalter, soweit diese im Einzelfall ein anzeigepflichtiges Gewerbe gemäß § 14 Abs. 1 und 2 GewO betreiben. In Einzelfällen können somit Gewerbeämter über Informationen z. B. über die Betreiber von Privatzoos, Zirkussen oder Bewachungsunternehmen verfügen.
Der Ermittlung einer Vielzahl bisher unbekannter Tierhalter oder dem regelmäßigen Abgleich der Tierhalter-Daten eines LÜVA mit den Angaben aus den Gewerbeanzeigen steht jedoch die abschließende Regelung von § 14 Abs. 5 GewO entgegen. Danach dürfen die Daten der Gewerbeanzeigen regelmäßig nur an die dort enumerativ bestimmten Behörden übermittelt werden. Lebensmittelüberwachungs- und Veterinärämter zählen nicht zu den dort aufgeführten Behörden. Daher dürfen sie zumindest keine regelmäßigen oder vollständigen Abgleiche ihrer Datenbestände mit denen der Gewerbeämter durchführen.
Demgegenüber dürfen im Einzelfall ("fallweise") gemäß § 14 Abs. 6 GewO die dort genannten Daten über Tierhalter, nämlich "Name", "betriebliche Anschrift" sowie "angezeigte Tätigkeit", von einem Gewerbeamt an ein LÜVA übermittelt werden, soweit dies zur Erfüllung der in die Zuständigkeit des LÜVA fallenden Aufgaben erforderlich ist. Weitere Daten aus der Gewerbeanzeige dürfen nur nach der strengen Maßgabe von § 14 Abs. 6 Satz 2 GewO übermittelt werden.

- Andere Stellen
  Die Ermittlung bisher unbekannter Tierhalter bei anderen kommunalen oder staatlichen Stellen kann, falls keine speziellen Rechtsvorschriften vorhanden sind, im Einzelfall unter den Voraussetzungen von § 11 Abs. 4 Nr. 8 SächsDSG als Datenerhebung bei einem Dritten gemäß § 13 Abs. 1 i. V. m. § 12 Abs. 2 Nr. 1 SächsDSG zulässig sein.

10.3.2 Datenerhebung der Lebensmittelüberwachungsbehörden über Milchhemmstoffe beim Landeskontrollverband e. V.

Das SMS hat sich mit der Frage an mich gewandt, unter welchen Voraussetzungen Lebensmittelüberwachungsbehörden Daten über sog. Hemmstoffe (z. B. Penizilline) in der von den Milcherzeugern bei Molkereien angelieferten Milch beim "Sächsischen Landeskontrollverband e. V." (mit Sitz in Chemnitz) erheben dürfen. Der Landeskontrollverband habe sich bisher unter Hinweis auf den Datenschutz der Milcherzeuger, also der anliefernden Landwirte, geweigert, den Lebensmittelüberwachungsbehörden "positive Hemmstoffbefunde" - also die Feststellung des Vorhandenseins von Hemmstoffen in der Milch - mitzuteilen.

Der Hintergrund der Anfrage ist folgender: Die sog. Landeskontrollverbände sind private Untersuchungsstellen, die im Auftrag der Molkereien die Untersuchungen vornehmen, welche die sog. Milch-Güteverordnung vorschreibt. Der ausführliche Name dieser Verordnung, nämlich "Verordnung über die Güteprüfung und Bezahlung der Anlieferungsmilch" (vom 9. Juli 1980, BGBl. I S. 878, zuletzt geändert durch die Fünfte Verordnung zur Änderung der Milch-Güteverordnung vom 27. Dezember 1993,

BGBl. I S. 2481) macht deutlicher, worum es geht: Die von jedem Milcherzeuger bei Molkereien oder ähnlichen milchsammelnden und verarbeitenden Stellen angelieferte Milch ist auf ihren Gehalt an Nährstoffen zu untersuchen, aber auch darauf, inwieweit sie schädliche Stoffe wie Bakterien oder eben Hemmstoffe enthält. Der Grundkonzeption nach handelt es sich bei dieser Vorschrift um eine ausschließlich wirtschaftsverwaltungsrechtliche Regelung: Es wird ein Qualitätsprüfungs- und Sicherungsverfahren vorgeschrieben, welches dafür sorgen soll, daß diejenigen Bauern, die bessere Milch anbieten, einen Preiszuschlag erhalten, während diejenigen, die schlechtere Milch anliefern, einen Preisabschlag hinnehmen müssen.
Daneben gibt es lebensmittelrechtliche, also dem Schutz des Verbrauchers von Milcherzeugnissen dienende Vorschriften: Das Lebensmittelüberwachungsrecht und die zu seiner Ausführung berufenen Behörden haben dafür zu sorgen, daß gesundheitlich schädliche Milcherzeugnisse nicht in Verkehr gebracht werden. Für Hemmstoffe ist die einschlägige Vorschrift § 15 LMBG, der es in Absatz 1 und 2 verbietet, vom Tier gewonnene Lebensmittel gewerbsmäßig in den Verkehr zu bringen, wenn in oder auf ihnen Stoffe mit pharmakologischer Wirkung vorhanden sind, die entweder nicht angewendet werden dürfen oder nach deren Anwendung Wartezeiten vorgeschrieben sind, die unterschritten wurden.
Es kann nicht überraschen, daß es zwischen diesen beiden Regelungsbereichen Überschneidungen gibt: Milch, die eine lebensmittelrechtlich unzulässige Beschaffenheit hat, ist von minderer Güte, sie hat einen geringeren Marktwert, wenn sie denn für den milchverarbeitenden Betrieb überhaupt verwertbar ist, weil in der Molkerei die Milch sehr vieler Hersteller vermischt wird, so daß die Eigenschaften einzelnen angelieferter Milchmengen durch Verdünnung lebensmittelrechtlich unschädlich werden können.

Die Prüfung der Zulässigkeit der vom Ministerium für wünschenswert gehaltenen Datenbeschaffung durch die LÜVÄ beim Landeskontrollverband ergab folgendes:
Die Befugnisse der LÜVÄ als Lebensmittelüberwachungsbehörden (§ 1 Abs. 2 SächsAGLMBG) - nicht als Veterinärbehörden - personenbezogene Daten zu verarbeiten, insbesondere zu erheben, ist in § 41 LMBG i. V. m. § 12 SächsAGLMBG nur recht allgemein geregelt. Ergänzend gilt das Sächsische Datenschutzgesetz. Diesem sind auch die Voraussetzungen zu entnehmen, unter denen ausnahmsweise Daten statt beim Betroffenen selbst bei einem Dritten erhoben werden dürfen. Um eine solche Datenerhebung bei einem Dritten handelte es sich nämlich. Denn soweit es um die Überwachung der Milcherzeugung und Milchverarbeitung geht, stellt die Feststellung von Hemmstoffen in der von einzelnen Milcherzeugern angelieferten Milch eine Einzelangabe über deren sachliche Verhältnisse dar. Werden diese Daten nicht beim milcherzeugenden Bauern, sondern beim Sächsischen Landeskontrollverband e. V. erhoben, so werden sie gemäß § 3 Abs. 1 und 4 SächsDSG bei einem "Dritten" erhoben. Hieraus folgt, daß eine Datenerhebung der LÜVÄ beim Landeskontrollverband nur unter den Voraussetzungen zulässig ist, unter denen § 11 Abs. 4 SächsDSG eine Datenerhebung bei Dritten erlaubt. In Betracht kommen insofern § 11 Abs. 4 Nr. 2 (Einwilligung des Milcherzeugers), Nr. 4 (nach Verletzung einer Auskunftspflicht und entsprechender Vorwarnung), Nr. 5

(tatsächliche Anhaltspunkte für unrichtig gemachte Angaben des Milcherzeugers), Nr. 6 (erforderlich zur Abwehr erheblicher Nachteile für das Gemeinwohl oder einer unmittelbar drohender Gefahr für die öffentliche Sicherheit, also in diesem Fall für die Gesundheit der Verbraucher) und Nr. 8 (Ersparung unverhältnismäßigen Aufwandes ohne Beeinträchtigung schutzwürdiger Interessen des Milcherzeugers).
Wenn im Einzelfall die Voraussetzungen einer dieser Sonderregelungen erfüllt sind, darf also das LÜVA sich Daten beim Landeskontrollverband beschaffen, aber eben nicht, wie das Ministerium sich gewünscht hätte, so, daß von sich aus der Landeskontrollverband in jedem Falle eines positiven Hemmstoffbefundes das zuständige LÜVA unterrichtet.

Anders wäre es, wenn die Milch-Güteverordnung für den Fall positiver Hemmstoffbefunde in der angelieferten Milch eine Erhebungsbefugnis der Lebensmittelüberwachungsbehörde beim Landeskontrollverband oder eine Übermittlungspflicht des Verbandes gegenüber den Lebensmittelüberwachungsbehörden vorsähe. Dies ist jedoch nicht der Fall. Vielmehr beschränkt sich die Milch-Güteverordnung in § 2 Abs. 8 Satz 2 auf eine Meldepflicht des Verbandes gegenüber den Lebensmittelüberwachungsbehörden, die dann eintritt, wenn ein bestimmter Gehalt an Keimen oder an sog. somatischen Zellen überschritten wird. Im Umkehrschluß ergibt sich, daß der in Satz 1 derselben Vorschrift erwähnte positive Hemmstoffbefund eine Übermittlungspflicht gegenüber den zuständigen (Lebensmittelüberwachungs-)Behörden nicht auslöst.
Immerhin ist aber die Feststellung von Hemmstoffen, unabhängig von deren Konzentration, von dem Untersuchungsverband als Untersuchungsstelle dem Milcherzeuger, also dem Landwirt, mitzuteilen (§ 2 Abs. 8 Satz 1 Milch-Güteverordnung). Außerdem sind die Ergebnisse der Untersuchungen, also auch die Feststellung von Hemmstoffen, gemäß § 5 Abs. 3 der Verordnung drei Jahre bei der Molkerei (oder für diese beim Landeskontrollverband) aufzubewahren und der nach Landesrecht zuständigen Stelle auf Verlangen vorzulegen.

Sollte es sich tatsächlich herausstellen, daß die Selbstkontrolle der Milchwirtschaft hinsichtlich der Hemmstoffbelastung der in den Molkereien angelieferten Milch nicht ausreichend funktioniert, müßte der Gesetz- bzw. Verordnungsgeber in dem erforderlichen Umfang eine Übermittlungspflicht des Landeskontrollverbandes einführen.

11 Landwirtschaft, Ernährung und Forsten

11.1 Dürfen Informationen, die bei einer Prüfung nach § 70 Abs. 3 Landwirtschaftsanpassungsgesetz gesammelt worden sind, den beteiligten ehemaligen LPG-Mitgliedern oder deren Rechtsnachfolgern zugänglich gemacht werden?

Bei der Umstellung von LPGen auf die neuen marktwirtschaftlichen Verhältnisse hat es bekanntlich den in vielen Fällen begründeten Verdacht gegeben, daß Genossenschaftsmitglieder geschädigt worden sind. Das hat dazu geführt, daß der Bundesgesetzgeber 1991 in das LwAnpG eine Vorschrift aufgenommen hat, die den Landwirtschaftsministerien der neuen Bundesländer die Befugnis gibt, Geschäftsführungsvorgänge im Zusammenhang mit der Umwandlung oder Abwicklung einer LPG zu prüfen, sofern Anhaltspunkte dafür vorliegen, daß nicht alles mit rechten Dingen zugegangen ist. Nach der auch heute noch geltenden Vorschrift des § 70 Abs. 3 LwAnpG hat das Ministerium das Recht, mündliche und schriftliche Berichte zu verlangen, Geschäftsakten und andere Unterlagen anzufordern sowie an Ort und Stelle Prüfungen und Besichtigungen vorzunehmen, wozu es sich auch geeigneter Prüfer - in der Regel Wirtschaftsprüfer - bedienen kann.
So wurde eine Vielzahl von Gutachten erstellt. Das SML hat diese Gutachten unter Verschluß genommen und sich auf Anfrage geweigert, den betroffenen Geschädigten bzw. den LPG-Mitgliedern diese Gutachten und ihre Ergebnisse mitzuteilen. Das SML meinte intern offenbar, es sei aus datenschutzrechtlichen Gründen daran gehindert.

Erst nach vielen Monaten - der zuständige Beamte hatte gewechselt - wurde mir die Frage gestellt, ob das so richtig sei. Das Ministerium war und ist befugt, die betreffenden Datenübermittlungen vorzunehmen. Dies folgt aus § 15 Abs. 1 Nr. 1 i. V. m. § 12 Abs. 1 SächsDSG. Die Übermittlung an Beteiligte ist zur Erfüllung einer Aufgabe des Ministeriums erforderlich und erfolgt für dieselben Zwecke, denen die Erhebung der Daten gedient hat.

Dies folgt aus der Auslegung von § 70 Abs. 3 LwAnpG. Danach darf das Püfungsverfahren nur eingeleitet werden, wenn der Behörde Anhaltspunkte für ein gesetzwidriges Verhalten bei der Geschäftsführung der LPG bzw. deren Nachfolgerin vorliegen. Die somit stattfindende Anlaßkontrolle hat ihren einzigen Zweck darin, die Grundlagen zu schaffen für Anzeigen bei der Staatsanwaltschaft (so in wenigen Fällen geschehen) sowie für Verfahren nach dem LwAnpG, in denen es auf eine gesetzgemäße Geschäftsführung der LPG ankommt. Da sie nur auf Antrag eines Beteiligten beginnen können, gehören die Gutachten in deren Hände.
Das Handeln der nach § 70 Abs. 3 LwAnpG tätigen Behörde im Einzelfall kann daher nur in Mitteilungen gegenüber Beteiligten bestehen, durch die diese darüber unterrichtet werden, wie die Behörde die Rechtslage einschätzt, womöglich versehen mit expliziten Empfehlungen. Diese Mitteilungen müssen als Darstellungen der Rechtslage personenbezogene Tatsachenangaben enthalten. Zweck des Prüfverfahrens nach § 70 Abs. 3 LwAnpG ist daher eine mehr oder weniger umfangreiche, jedenfalls

für eine Rechtsverfolgung hinreichend aussagekräftige und damit nützliche Bekanntgabe der gewonnenen - weitgehend personenbezogenen - Informationen an die Beteiligten.

Dieses aus der Auslegung des Wortlautes der Vorschrift folgende Ergebnis wird durch die Gesetzesmaterialien wie auch durch die einschlägige Literatur bestätigt (vgl. Dieter Schweizer, Das Recht der landwirtschaftlichen Betriebe nach dem Landwirtschafts-Anpassungsgesetz, 2. Aufl., Rdnr. 767; ferner Nies in RVI Band III B 500, Rdnr. 3 zu § 70 LwAnpG). Eine davon abweichende Praxis in den neuen Bundesländern war im BML nicht bekannt.

Es kommt daher datenschutzrechtlich nichts anderes in Frage, als die Ergebnisse einer Überprüfung nach § 70 Abs. 3 LwAnpG allen ehemaligen LPG-Mitgliedern bekannt zu machen, und zwar unabhängig davon, ob sie die Mitgliedschaft gekündigt haben oder nicht, damit sie ihre Ansprüche prüfen (lassen) und ggf. durchsetzen können.

11.2 Namentliche Kennzeichnung von Fischereifahrzeugen

Ein Petent wandte sich an mich, weil er sich durch die gemäß § 8 Fisch-VO bestehende Pflicht, an Fischereifahrzeugen, z. B. auch Angelkähnen, Namen und Anschrift des Eigentümers anzubringen, unnötig belastet fühlte. In keinem anderen Land bestehe eine solche Pflicht, dort beschränke man sich auf eine Kennzeichnung der Fischereifahrzeuge mittels Buchstaben und Zahlen, die dann, ähnlich wie bei Kraftfahrzeugen, behördlich registriert seien.

Der Petent hatte recht. Die jedermann zugängliche Kennzeichnung mit Klarnamen samt Anschrift ist zur Überwachung von Fischereifahrzeugen und Fangeräten nicht erforderlich.

Das hat das SML auch sofort eingesehen. Es hat zunächst durch Erlaß vom 10. September 1996 angeordnet, daß anstelle von Namen und Anschrift des Eigentümers ein Kennzeichen anzubringen ist, mittels dessen die Person des Eigentümers festgestellt werden kann. Die Art der Kennzeichnung solle durch „Vorschrift“ der jeweils örtlich zuständigen unteren Fischereibehörde bestimmt werden.

Dies ist nur eine vorläufige Lösung. Nötig ist eine förmliche Änderung der Fisch-VO.

12 Umwelt und Landesentwicklung

12.1 Ermittlung der Namen von Grundstückseigentümern und Mietern zum Zwecke der Abfallgebührenerhebung

Ein Petent bat mich zu prüfen, ob Datenschutzgründe der Ermittlung von Namen und Anschriften ortsfremder, jedoch namentlich bekannter Grundstückseigentümer und -nutzer von im Gemeindegebiet gelegenen Datschen-Grundstücken entgegenstünden. Die Abfallgebühren seien auch deswegen so hoch, weil insbesondere die auswärtigen Nutzer von Wochenendhausgrundstücken nicht zur Zahlung herangezogen würden.

Dem Petenten, der zuständigen Gemeindeverwaltung sowie dem zuständigen Abfallwirtschaftsamt des Landkreises habe ich folgendes mitgeteilt:

Der Ermittlung der Anschriften und ggf. auch der Namen von Eigentümern von im Gemeindegebiet gelegenen Grundstücken zum Zwecke der Abfallgebührenerhebung können Datenschutzgründe in der Regel nicht entgegenstehen. Die Untere Abfallbehörde, d. h. das Abfallwirtschaftsamt des Landkreises, darf zum Zwecke der Abfallgebührenerhebung Namen und Anschriften von Grundstückseigentümern bei den kreisangehörigen Gemeinden in deren Eigenschaft als Grundsteuerbehörden (gemeindliche Steuerämter) erheben. Das Steuergeheimnis (§ 30 AO) steht dem nicht entgegen, denn § 31 Abs. 3 AO erlaubt es den für die Verwaltung der Grundsteuer zuständigen Behörden, die nach § 30 AO geschützten Namen und Anschriften von Grundstückseigentümern zur Verwaltung anderer Abgaben, hier der Abfallgebühren, an andere Behörden, hier das zuständige Abfallwirtschaftsamt, auf dessen Ersuchen hin mitzuteilen.

Rechtliche Gründe, die einer Ermittlung der Anschriften und ggf. der Namen von Nutzungsberechtigten, in der Regel der Mieter, entgegenstehen könnten, sind ebenfalls nicht ersichtlich. Eine untere Abfallbehörde kann, wenn nach der Abfallwirtschafts- und Gebührensatzung des Landkreises neben den Grundstückseigentümern auch die Nutzungsberechtigten Gebührenschuldner sind, deren Anschriften und Namen entweder aufgrund besonderer Erhebungsvorschriften in der jeweiligen Abfallgebührensatzung oder unter den Voraussetzungen von § 11 Abs. 4 Nr. 8 (Vermeidung eines unverhältnismäßigen Aufwandes und Fehlen überwiegender schutzwürdiger Interessen der Mieter, als Gebührenschuldner) SächsDSG bei Dritten, nämlich den Grundstückseigentümern, erheben.

12.2 Datenübermittlungen bei der Ausführung des Bundesimmissionsschutzgesetzes

Der Inhaber eines Betonmischwerkes beschwerte sich bei mir, weil seine Anlage betreffende Daten vom Staatlichen Umweltfachamt an das Landratsamt weitergegeben und von diesem dann auch noch Grundstücksnachbarn zugänglich gemacht worden seien, die mit ihren Klagen über Belästigungen die Existenz seines Betriebes

bedrohten.

Was den Sachverhalt betrifft, bestätigten sich die Angaben des Petenten, die Informationsvorgänge, gegen die er sich wehrte, erwiesen sich jedoch als rechtlich einwandfrei. Im einzelnen:

Die Eigentümer eines benachbarten Wohngrundstückes hatten beim Amt für Umwelt- und Naturschutz des betreffenden Landkreises den Antrag gestellt, Lärmschutzauflagen anzuordnen. Das Landratsamt war sachlich zuständig; das ergibt sich aus dem komplizierten Regelwerk des BImSchG samt 4. BImSchV i. V. m. der Anlage zur Zuständigkeitsverordnung Immissionsschutz (ImSchZuV) vom 5. Juli 1995 (GVBl. S. 1282).
Das Landratsamt hatte nun in der Tat dem örtlich zuständigen Staatlichen Umweltfachamt mitgeteilt, daß es Beschwerden über die von der Anlage auf die Nachbarschaft ausgehenden Lärmbelästigungen gebe, woraufhin das zuständige StUFA vom Petenten auf der Grundlage des § 26 Abs. 1 BImSchG verlangt hatte, daß er *Art und Ausmaß der von seiner Anlage ausgehenden Emissionen sowie die Immissionen im Einwirkungsbereich der Anlage* durch eine vom SMU dazu ermächtigte Gutachterstelle ermitteln lasse.

Man muß wohl davon ausgehen, daß das LRA und das Staatliche Umweltfachamt bei der Durchführung des Bundesimmissionsschutzgesetzes zwei verschiedene Stellen nicht nur im organisatorischen, sondern auch im funktionellen Sinne sind, mit der Folge, daß die genannte Mitteilung des Landratsamtes an das Staatliche Umweltfachamt im Rechtssinne als Übermittlung (eines personenbezogenen Datums) anzusehen war. Dennoch kann nicht vernünftig bezweifelt werden, daß es sich um eine Übermittlung ohne Zweckänderung gehandelt hat (§ 13 Abs. 1 Nr. 1 i. V. m. § 12 Abs. 1 Nr. 1 SächsDSG), nämlich zum einheitlichen Zweck der Durchführung des Bundesimmissionsschutzgesetzes, so daß eine solche Mitteilung des LRA, die dann die Anordnung des StUFA gemäß § 26 BImSchG ausgelöst hat, rechtmäßig war.

Das vom Petenten wie verlangt beigebrachte Gutachten hatte sodann das StUFA dem Landratsamt als unterer Immissionsschutzbehörde bekanntgegeben. Auch dies war rechtmäßig nach § 13 Abs. 1 i. V. m. § 12 Abs. 1 SächsDSG: Im Rahmen der fachlichen Unterstützung des LRA als unterer Verwaltungsbehörde bei deren Aufgabenerfüllung (vgl. § 1 Satz 2 Nr. 1 der Aufgabenübertragungsverordnung des SMU vom 14. November 1994, GVBl. S. 1638) und im Hinblick auf die Zuständigkeit des LRA für eine nachträgliche Anordnung gemäß § 17 BImSchG i. V. m. der bereits genannten ImSchZuV durfte diese Datenübermittlung stattfinden.

Gegenstand dieser - wie gesagt erlaubten - Datenübermittlung war auch die fachamtliche Stellungnahme des StUFA gewesen, das es auf der Grundlage des schalltechnischen Gutachtens ausgearbeitet hatte und das die im Gutachten ermittelten Meßwerte in etwas allgemeinerer Form enthielt. Diese fachamtliche Stellungnahme des StUFA hatte dann das LRA den Grundstücksnachbarn, die sich bei ihm beschwert

hatten, inhaltlich zugänglich gemacht. Rechtsgrundlage für diese Datenübermittlung war das Akteneinsichtsrecht der an einem Verwaltungsverfahren Beteiligten gemäß § 29 Abs. 1 i. V. m. § 13 Abs. 1 VwVfG. Es war nicht erkennbar, aus welchem Grunde ausnahmsweise wegen berechtigter Interessen des Petenten die Akteneinsicht gemäß § 29 Abs. 2 VwVfG hätte verweigert werden können. Betriebs- und Geschäftsgeheimnisse, die gemäß § 30 VwVfG, § 10 Abs. 2 BImSchG zu schützen gewesen wären, waren nicht ersichtlich.

Man kann das Ergebnis wohl verallgemeinern: Das allgemeine Datenschutzrecht sichert die datenschutzrechtliche Flanke der Aufsplitterung der Zuständigkeiten bei der Ausführung des Immissionsschutzrechtes in ausreichendem Maße. Mit bereichsspezifischen Übermittlungsnormen wäre auf diesem Feld wohl wenig zu gewinnen.

13 Wissenschaft und Kunst

Übersendung eines Bescheids über Fördermittelgewährung für einen eingetragenen Verein auch an Dritte

Zur Pflege der regionalen Kultur sind in Sachsen sog. Kulturräume gebildet worden, deren vorrangige Aufgabe es ist, Mittel zur Unterstützung kultureller Einrichtungen zu vergeben. Ein solcher Kulturraum ist nach dem Kulturraumgesetz ein Zweckverband, dessen Mitglieder aus Landkreisen und Kreisfreien Städten bestehen. Damit ist er eine sonstige öffentliche Stelle im Sinne des § 2 Abs. 1 SächsDSG.

Ein eingetragener Verein beantragte bei dem für die Region zuständigen Kulturraum einen Zuschuß für Musikveranstaltungen während der Landesgartenschau und legte dazu Kosten- und Finanzierungspläne vor. Der Kulturraum lehnte den Antrag kurzerhand mit der Begründung ab, die Kostenaufstellung sei eine bewußte Täuschung, mit der sich der Verein ungerechtfertigt Fördergelder verschaffen wolle. Dabei berief sich der Kulturraum als "Beweis" auf ein Gespräch mit der Trägergesellschaft der Landesgartenschau über die Angaben im Antrag. Diesen Bescheid einschließlich Begründung sandte der Kulturraum nicht nur an den antragstellenden Verein, sondern per "Verteiler" auch an die Trägergesellschaft für die Landesgartenschau, das Regierungspräsidium sowie die Stadt, die Schauplatz der Landesgartenschau war.

Ich habe diesen Sachverhalt wie folgt beurteilt:

Der Antragsteller ist als eingetragener Verein eine juristische Person des privaten Rechts. Da das Sächsische Datenschutzgesetz nur dann Anwendung findet, wenn eine öffentliche Stelle Daten einer bestimmten oder bestimmbaren *natürlichen Person* verarbeitet, war insbesondere zu klären, ob und inwieweit die im Bescheid enthaltenen Vorwürfe natürliche Personen betreffen und ob diese bestimmbar sind.

Angaben über eine juristische Person des privaten Rechts können unter bestimmten Voraussetzungen zu Angaben über eine natürliche Person werden. Dies hat der Bundesgerichtshof mit Urteil vom 17. Dezember 1985 - VI ZR 244/84, NJW 1986, 2505, 2506 lSp., festgestellt. So stellt die Äußerung über die finanzielle Situation einer "Ein-Mann-GmbH" im Zusammenhang mit Angaben über den geschäftsführenden Gesellschafter zugleich eine auf diesen bezogene kreditrelevante Aussage dar. Ähnliche Auffassungen werden in der Literatur vertreten. Danach erfaßt der Schutzbereich der Datenschutzgesetze auch einzelne Mitglieder juristischer Personen bzw. eine oder mehrere hinter der juristischen Personen stehende natürliche Personen, wenn sich Angaben über die juristische Person auch auf sie beziehen - sozusagen auf sie "durchschlagen" (Ordemann/Schomerus/Gola, Anm. 2.9 zu § 3 BDSG) - bzw. Angaben über die juristische Person zugleich Angaben über eine natürliche Person sind (Dammann in Simitis/Dammann/Geiger/Mallmann/Walz, Rdnr. 19 zu § 3 BDSG).

Im vorliegenden Fall habe ich die Auffassung vertreten, daß die Betrugs- bzw. Täuschungsvorwürfe nur natürliche Personen treffen können. Denn juristische Personen können keine Täuschungshandlungen vornehmen, sondern nur die für sie verantwortlich handelnden Personen. Dies ist bei einem eingetragenen Verein der Vorstand, der über das öffentlich zugängliche Vereinsregister namentlich bestimmbar ist. Damit handelt es sich bei den Vorwürfen um personenbezogene Daten im Sinne des § 3 Abs. 1 SächsDSG mit der Folge, daß die Weitergabe von Mehrfertigungen des Bescheids als Übermittlung personenbezogener Daten anzusehen ist. Ohne Einwilligung der Betroffenen ist sie in diesem Fall nur zulässig, wenn das Verwaltungsverfahrensgesetz sie erlaubt.

§ 41 VwVfG sieht die Bekanntgabe eines schriftlichen Verwaltungsakts ausschließlich an die Beteiligten vor, wobei allein § 13 Abs. 1 VwVfG bestimmt, wer Beteiligter ist. Zu ihnen gehören nach dem bekannten Sachverhalt weder die Trägergesellschaft noch das Regierungspräsidium noch die Stadt. Ich habe den Kulturraum zur Stellungnahme aufgefordert. Eine sachgerechte Äußerung habe ich bisher nicht erhalten, so daß ich von einem Datenschutzverstoß ausgehe, der auf die Nichtbeachtung von Vorschriften des Verwaltungsverfahrensgesetzes zurückzuführen ist.

14 Technischer und organisatorischer Datenschutz

14.1 Neue Entwicklungen im Telekommunikationsrecht

Weil das Monopol der Telekom wegfällt, bedarf es neuer Rechtsvorschriften: Am 1.August 1996 trat das Telekommunikationsgesetz (TKG) in Kraft. Seit dem 19. Juli 1996 gilt die Telekommunikationsdienstunternehmen-Datenschutzverordung (TDSV), die noch auf der Grundlage des mittlerweile durch das TKG abgelösten Gesetzes über die Regulierung der Telekommunikation und des Postwesens (PTRegG) erlassen wurde. Dies hat unterschiedliche Anwendungsbereiche zur Folge. Gelten die datenschutzrechtlichen Regelungen des TKG nach § 89 für alle Unternehmen, die geschäftsmäßig Telekommunikationsdienste anbieten bzw. erbringen oder an der Erbringung solcher Dienste mitwirken, so sind bei der TDSV nur solche Unternehmen im Blick, die der Öffentlichkeit angebotene Telekommunikations- und Informationsdienstleistungen erbringen oder an der Übermittlung solcher Dienstleistungen mitwirken (§ 10 PTRegG). Diese Telekommunikationsdienstleistungen umfassen nach § 2 Nr. 6 TDSV nur das gewerbliche Angebot von Telekommunikation. Damit fallen Corporate Networks, firmen- und behördeninterne Telekommunikationsanlagen und -netzwerke aus dem Geltungsbereich der TDSV heraus. Also gelten zwar für alle Anbieter die datenschutzrechtlichen Bestimmungen des § 89 TKG, nicht jedoch die der TDSV. Allerdings ist auch in § 89 Abs. 1 TKG eine Verordnungsermächtigung enthalten, von der die Bundesregierung jedoch wegen der notwendigen Abstimmung erst Gebrauch machen will, wenn die ISDN-Richtlinie der Europäischen Union in Kraft getreten ist. Die von der Konferenz der Datenschutzbeauftragten des Bundes und der Länder formulierten Wünsche (Entschließung zum Datenschutz bei der Neuordnung der Telekommunikation vom 9./10. November 1995 in Bremen, 4. Tätigkeitsbericht unter 16.1.5) sind größtenteils umgesetzt worden. Bedenklich ist jedoch die Einführung eines besonderen automatisierten Abrufverfahrens in § 90 TKG, mit dem die Sicherheitsbehörden bestimmte Kundendaten (Name, Anschrift, Telefonnummer) von den Dienstanbietern erhalten, ohne daß dies die Diensteanbieter erfahren können. Da dies durch technische Maßnahmen sichergestellt werden soll, besteht hier die Möglichkeit eines unkontrollierten Zugangs zu solchen Dateien. Darüber hinaus ist diese Regelung wohl als Auftakt auch für weitergehende Forderungen gedacht. Eine ähnliche Regelung soll auch für Teledienste in das neue Informations- und Kommunikationsdienstegesetz (IuKDG) aufgenommen werden (nachstehend unter 14.2).

Erstmals werden auch technische Sicherheitsbestimmungen für alle Betreiber von Telekommunikationsanlagen verbindlich gemacht (§ 87 TKG). Ich erhoffe mir davon, daß endlich in diesem sensiblen Bereich die Anlagenhersteller gezwungen werden, Sicherheitsmaßnahmen nach dem Stand der Technik umzusetzen und dies auch für die Betreiber ausreichend zu dokumentieren.

14.2 Neue Medien

Nicht nur im Bereich der Telekommunikation, sondern auch bei der Nutzung von Computern und beim Fernsehen gibt es Entwicklungen und Angebote, die mit den vorhandenen rechtlichen Instrumentarien nicht mehr zu erfassen sind. Dabei tun sich zwei grundsätzliche Problembereiche auf.

Zum einen nähern sich die Angebote im Bereich der Nutzung von Computern Online-Dienste wie T-Online, Compuserve, Microsoft Network und American Online immer mehr den neuen Diensten im Fernsehen an. So wollen einerseits Online-Anbieter bewegte Bilder, also z. B. Videofilme, abrufbar einspeisen, anderseits wird im Pay-TV ebenfalls, zwar mit anderer Technik, das gleiche Angebot gemacht. Zwei bisher klar abgrenzbare Bereiche, die auch unterschiedlich geregelt waren, überschneiden sich immer mehr.
Der andere Problemkreis ergibt sich aus einem Kompetenzstreit zwischen Bund und Ländern: Während die Länder die Online-Dienste mit einem erweiterten Rundfunkbegriff zu erfassen suchen, beruft sich der Bund auf seine Zuständigkeit für Telekommunikation und Multimedia.

Bei den sich rasant entwickelnden Online-Diensten sind mehrere Tendenzen erkennbar.
- Die Träger-Anbieter-Funktionen fallen immer mehr zusammen.
- Der bisherige Gegensatz Individualkommunikation (Telefonieren) und Massenkommunikation (Fernsehen) löst sich auf. Exemplarische Zwischenformen sind Interaktives Fernsehen und das von den Online-Diensten angebotene electronic chatting (die "elektronische Kneipe"), in das man zu jeder Zeit einsteigen kann, um sich dort mit anderen Teilnehmern zu unterhalten.
- Der technische Wechsel ist rasant; eine längerfristige Vorhersage ist nicht möglich.
- Als Anbieter von Leistungen treten private Mailboxbetreiber auf, von kleineren Unternehmen mit einzelnen Angeboten bis hin zu großen kommerziellen Anbietern. Der Gesetzgeber wird berücksichtigen müssen, daß wohl ein kommerzieller Online-Dienst hohe Datenschutzanforderungen erfüllen kann, nicht aber der Student, der mit seinem PC eine Mailbox betreibt.

Wer hat aber die Gesetzgebungszuständigkeit? Wie können bestimmte Angebote noch klar begrifflich zugeordnet werden? Was ist bei inhaltlich auseinanderlaufenden Regelungen für bestimmte Dienste, die in der Praxis vom gleichen Anbieter und für den Nutzer schwer unterscheidbar angeboten werden? Mittlerweile haben sich Bund und Länder geeinigt, jeder für sich gesetzliche Regelungen mit gleichem Inhalt zu schaffen. Für Mediendienste, die per definitionem an die Allgemeinheit gerichtet sind, haben die Länder einen Staatsvertrag geschlossen, der sich derzeit im Ratifizierungsverfahren befindet.
Der Bund hat daneben einen Entwurf für ein Informations- und Kommunikationsdienstegesetz (IuKDG) vorgelegt, das nach einer Stellungnahme des Bundesrates derzeit im Bundestag behandelt wird. Beide Regelungen sind miteinander

gekoppelt und treten gleichzeitig in Kraft.
Die Datenschutzbeauftragten des Bundes und der Länder haben intensiv an den Datenschutzregelungen mitgewirkt. Ihre 1996 formulierten datenschutzrechtlichen Eckpunkte (4. Tätigkeitsbericht unter 16.3) sind im Multimediastaatsvertrag adäquat umgesetzt worden.

Leider zeichnet sich beim IuKDG eine bedenkliche Entwicklung ab: Nach dem Vorbild der Regelung in § 90 TKG will die Bundesregierung ein automatisiertes Abrufverfahren für die Sicherheitsbehörden einrichten. Die Datenschutzkonferenz hat sich dazu geäußert und dieses strikt abgelehnt (unten Abschnitt 16.3.3).

14.3 Kryptokontroverse

Nationales Medienrecht - auch das neu entstandene deutsche - bezieht sich in der Regel auf die Struktur des Netzes, hat aber den Endbenutzer weitgehend nicht im Blick. Angesichts der internationalen Entwicklungen wird sich bei den neuen Mediendiensten immer mehr die Frage stellen, inwieweit solches nationale Recht noch Wirkmöglichkeiten hat. Vor einigen Jahren konnte sich niemand den heutigen Verbreitungsgrad des Internet und die dadurch entstandenen Probleme vorstellen. Ich bezweifle, daß hier noch einheitliche internationale Regelungen entstehen und greifen können. Zu groß sind die unterschiedlichen nationalen Interessen; zu schnell ist der technische Fortschritt. Wir werden uns der Tatsache stellen müssen, daß sich die Verantwortung für die Durchsetzung des gebotenen Datenschutzes immer mehr auf den Endbenutzer verlagern wird. Das bedeutet allerdings, daß ihm Instrumente, wie z. B. die Verschlüsselung, nicht aus der Hand genommen werden dürfen.

Dies schafft allerdings für Sicherheitsbehörden neue Probleme. Ihr Hauptargument in der Debatte um die gesetzliche Regelung der Verschlüsselung ist, daß digitale abhörsichere terrestrische Kommunikationsnetze, Mailboxsysteme und satellitengestütztes Telefonieren durch die organisierte Kriminalität und den politischen Extremismus immer stärker benutzt werden. Konnten die Sicherheitsbehörden bisher mit richterlicher Genehmigung Nachrichteninhalte abhören, so wird dies jetzt massiv erschwert. Sichere Verschlüsselungsprogramme wie PGP (pretty good privacy) sind leicht zu erhalten. Der technische Aufwand, der nötig ist, um solche Schlüssel zu knacken, ist enorm und von den Behörden in der Regel nicht mehr zu leisten. Deshalb gehen die Überlegungen, den Zugriff auf die Kommunikation auch unter den neuen technischen Bedingungen zu ermöglichen, in mehrere Richtungen. Schärfste Variante ist das Verbot der Verschlüsselung privater Kommunikation. Dies ist weder praktikabel (gerade im Bereich der Wirtschaft) noch im Hinblick auf die Verfassungslage rechtlich durchsetzbar. Weitere Möglichkeiten werden in einer Antwort der Sächsischen Staatsregierung vom 5. November 1996 auf die Große Anfrage der SPD-Fraktion (Drs. 2/3556) zum Thema "Chancen und Risiken der Informationsgesellschaft" beschrieben, die ich in ihrer Tendenz teile:

Auf die Frage "Befürwortet die Staatsregierung ein generelles Verbot des Einsatzes

von Verschlüsselungssoftware (wie in Frankreich)? Wenn ja, warum? Wenn nein, welche Alternativen sieht die Staatsregierung, Polizei und Strafverfolgungsbehörden das Abhören digitaler Kommunikation im Bereich der neuen Medien zu ermöglichen?" hat die Staatsregierung geantwortet:

Ein generelles Verbot des Einsatzes von Verschlüsselungs-Software wird als nicht sachgerecht angesehen.
Die an der digitalen Telekommunikation teilnehmenden Personen haben ein schützenswertes Interesse, ihre Daten und Nachrichten zu verschlüsseln und damit einem allgemeinen Zugriff zu entziehen.
Faktisch würde ein Verbot von Verschlüsselungsverfahren bewirken, daß flächendeckend allen Grundrechtsträgern verboten werden würde, ihr Fernmeldegeheimnis mit technischen Hilfsmitteln autonom gegen den Zugriff Dritter zu sichern, um in wenigen Einzelfällen das staatliche Abhören zu ermöglichen. Darüber hinaus würde ein Verbot von Verschlüsselungsverfahren lediglich das öffentliche Angebot von Verschlüsselungsdienstleistungen verhindern können.
Es muß davon ausgegangen werden, daß die gerade für die staatliche Überwachung interessanten und im Sinne der Gefahrenabwehr- und Strafverfolgungsbehörden gefährlichen oder verdächtigen Personen über die erforderlichen Mittel verfügen, um ihre Telekommunikation ausreichend gegen staatlichen Zugriff zu schützen.
Als Alternative zum Verbot des In-Verkehr-Bringens von Verschlüsselungssoftware kommen Lizenzierungsverfahren in Betracht. Sinn und Zweck solcher Genehmigungsvorbehalte ist es, im Interesse der Gefahrenabwehr und der Strafverfolgung, die Teilnehmer nur solche Verschlüsselungsverfahren verwenden zu lassen, die den betreffenden Behörden Zugriff auf die Schlüssel zum Dechiffrieren der Nachrichten ermöglichen.
Als weitere Alternative könnte ein Hardware-Teil eingeführt werden, das nicht nur die Verschlüsselung beim Teilnehmer für diesen übernimmt, sondern auch im Falle einer richterlichen Entscheidung den Zugriff der Ermittlungsbehörden ermöglicht. Diese sogenannten 'Clipper-Chips' würden als Verschlüsselungszusatz im Teilnehmerendgerät eingebaut.
Ferner könnte durch eine freiwillige Normierung von Sprache, Faksimile und Datenkommunikation durch die Wirtschaft und die Errichtung von unabhängigen Trustzentren ein nationaler oder europäischer Defacto-Standard für öffentliche und private Netzwerke geschaffen werden. Während andere Verschlüsselungsprodukte dann immer noch gebaut werden könnten, würden sie wenig Absatzmöglichkeiten finden, aus Gründen der fehlenden Interoperatibilität.

Ich halte rechtliche Regelungen für nötig, damit staatliche Stellen ihrem gesetzlichen Auftrag zur Gefahrenabwehr und Strafverfolgung in dem Umfang wie bisher nachkommen können. Auf der anderen Seite ist dabei der Grundrechtsschutz der Bürger zu beachten. Es ist eine schwierige rechtliche und technische Aufgabe, solche Lösungen zu finden, die nicht doch relativ leicht unterlaufen werden können.

14.4 Internetbenutzung durch Behörden

Immer mehr sächsische Behörden bedienen sich des Internet. Zu den datenschutztechnischen Problemen, insbesondere der Verhinderung unberechtigter Zugriffsversuche, hat sich der Arbeitskreis Technik der Datenschutzbeauftragten des Bundes und der Länder ausführlich geäußert (4. Tätigkeitsbericht unter 14.1). Daneben stellt sich jedoch auch die Frage, was mit den personenbezogenen Daten geschieht, die bei der "normalen" Benutzung im Internet anfallen. Die Verwendung des Internet für Verwaltungsarbeit (z. B. Meldewesen, Kfz-Zulassungswesen u. ä.) wird hier nicht behandelt, da für diesen Bereich die Internet-Nutzung wegen des Sicherheitsrisikos generell abzulehnen ist. Ansonsten muß zwischen zwei Benutzungsformen unterschieden werden: der aktiven Nutzung (als "User") und der passiven Nutzung (in der Regel Öffentlichkeitsdarstellung durch Angebote auf einem WWW-Server).
Meist werden bei beiden Arten externe Dienstleister (Provider) herangezogen, die zum einen den örtlichen Zugang ins Internet bereitstellen, zum anderen die Präsentation des Auftraggebers auf einem Server erstellen und pflegen.

Aktive Nutzung

Für die aktive Nutzung des Internet durch Behörden bestehen mehrere Möglichkeiten. Man kann Kunde bei einem Online-Dienst sein, dessen Leistungspaket einen Internet-Zugang umfaßt. Man kann einen (z. B. mittelständischen) Internetprovider beauftragen, der einen Internet-Zugang vermittelt. Für die Adressierung gibt es in diesem Fall zwei Varianten: Jeder Nutzer erhält seine eigene Internet-Adresse, oder der Provider hat einen Pool von IP-Adressen, die er dann während der Sitzung dynamisch an die Teilnehmer vergibt (analog dem Internet-Zugang bei Online-Diensten). Schließlich kann die öffentliche Stelle (z. B. eine Universität) selbst einen Internet-Zugang schaffen.

Bei einer Session im Internet, also bei jeder Nutzung, entstehen Verbindungsdaten. Sowohl die Nutzerkennung als auch das Paßwort werden bei den gängigen Diensten über das Internet übertragen. Jeder WWW-Server speichert die Adressen der Nutzer, die seine Angebote abrufen. Und der Betreiber des Servers verwendet diese Daten dann auch, insbesondere bei kommerziellen Angeboten.

Dies ist bei einer dynamischen IP-Adresse des Nutzers (z. B. T-Online-Nutzer) wirkungslos, da der wahre Nutzer durch den Betreiber des angesprochenen WWW-Servers nicht ermittelt werden kann. Allerdings erhält der Service-Provider ein Bild der abgerufenen Dienste. Bei einer statischen Adresse jedoch ergibt sich das oben beschriebene Risiko.

Zu empfehlen ist deshalb:
- ein Hinweis an die Mitarbeiter, daß ihre Verbindungsdaten gespeichert werden (Dies kann auch in bezug auf Kostenersparnis hilfreiche Wirkung haben),
- eine vertragliche Regelung mit dem Service-Provider, daß die Verbindungsdaten über

die Dauer der Verbindung hinaus bei ihm nicht gespeichert werden.

Will ein Vorgesetzter die Verbindungsdaten auswerten, so muß er die Regelungen über die automatisierte Verarbeitung von Beschäftigtendaten beachten.

Präsentation im Internet

Bei einer Präsentation im Internet können drei Arten von personenbezogenen Daten eine Rolle spielen:
- die in der Präsentation auftauchenden Daten (z. B. der Professoren in elektronischen Vorlesungsverzeichnissen)
- Verbindungsdaten derjenigen, die das Angebot aufrufen
- Interaktionsdaten derjenigen, die das Angebot aufrufen (falls z. B. im Angebot die Möglichkeit existiert, eine Nachricht oder die Adresse zur Übersendung von Informationsmaterial zu hinterlassen).

Personenbezogene Daten in der Präsentation
Eine Verwendung personenbezogener Daten in einer Internetpräsentation ist grundsätzlich nur mit Einwilligung der Betroffenen gestattet. Da eine Information im Internet weltweit zugänglich ist, wäre ansonsten der Verhältnismäßigkeitsgrundsatz verletzt. Dies gilt auch für Daten, die bereits öffentlich zugänglich sind (z. B. Vorlesungsverzeichnisse, Abgeordnetenhandbücher).

Verbindungsdaten
Verbindungsdaten sind zu löschen, sobald sie nicht mehr benötigt werden. Im Falle der Beauftragung eines Service-Providers ist dieser darauf zu verpflichten (§ 7 SächsDSG - Datenverarbeitung im Auftrag). Dies ist auch nach den neuen Regelungen im Medienrecht (IuKDG, Mediendienste-Staatsvertrag) zu erwarten.

Interaktionsdaten
Bei Interaktionen muß deutlich sichtbar werden, welche Daten in welchen Phasen erhoben werden und was mit ihnen geschieht. Der Teilnehmer muß über den Zweck der Verarbeitung informiert (§ 4 Abs. 2 SächsDSG) und auf die Freiwilligkeit seiner Angaben hingewiesen werden (§ 11 Abs.2 SächsDSG). Bei einem Abbruch der Verbindung müssen die Daten gelöscht werden. Die Weiterverarbeitung der Daten bemißt sich nach den geltenden datenschutzrechtlichen Regelungen.

Datenverarbeitung im Auftrag

In der Regel werden Behörden bei der Internet-Anbindung auf externe Auftragnehmer zurückgreifen. Da personenbezogene Daten verarbeitet werden, sind die Regelungen einer Datenverarbeitung im Auftrag zu beachten. Der Auftraggeber (die Behörde) hat vertraglich zu sichern, daß der Auftragnehmer (Service-Provider) die - für den Auftraggeber! - geltenden datenschutzrechtlichen Bestimmungen einhält. Dies ist zur Zeit das Sächsische Datenschutzgesetz. Nach ihrem Inkraftreten sind in erster Linie

das IuKDG und der Mediendienste-Staatsvertrag einzuhalten.

Ein entsprechendes Muster für vertragliche Regelungen wird im folgenden vorgestellt:

- Der Auftragnehmer verpflichtet sich, die für ihn und den Auftraggeber (im folgenden "Vertragspartner") geltenden Anforderungen des Datenschutzrechtes, insbesondere des Sächsischen Datenschutzgesetzes (SächsDSG), zu beachten und die bei der Abwicklung des Vertrages entstehenden personenbezogenen Daten nur entsprechend den Weisungen des Vertragspartners zu verarbeiten.
- Der Auftragnehmer ist verpflichtet, bei der Verarbeitung personenbezogener Daten ausschließlich Personal einzusetzen, das auf das Datengeheimnis nach § 6 SächsDSG verpflichtet ist.
- Der Auftragnehmer erklärt, die nach § 9 SächsDSG erforderlichen personellen, technischen und organisatorischen Maßnahmen getroffen zu haben. Der Auftragnehmer legt hierzu ein Datensicherungskonzept vor und erklärt, daß das mit der Vertragserfüllung beauftragte Personal fachlich und persönlich geeignet ist.
- Der Auftragnehmer verpflichtet sich, die bei der Vertragserfüllung entstehenden personenbezogenen Daten auf keinen Fall für eigene Zwecke zu verarbeiten, an Dritte über die zur Erfüllung des Vertrages notwendigen Zwecke hinaus zu übermitteln oder einer sonstigen Nutzung zuzuführen.
- Bei Beendigung des Vertragsverhältnisses ist der Auftragnehmer verpflichtet, die durch die Erfüllung des Vertragsverhältnisses zu diesem Zeitpunkt noch bei dem Auftragnehmer gespeicherten personenbezogenen Daten an den Vertragspartner auf Weisung des Vertragspartners zu übermitteln und zu löschen.
- Werden von dem Auftragnehmer zur Erfüllung des Vertrages Dritte beauftragt, so sind die vertraglichen Leistungen durch den Auftragnehmer so zu gestalten, daß sie den Datenschutzbestimmungen im Vertragsverhältnis zwischen dem Auftragnehmer und dem Vertragspartner entsprechen.
- Der Vertragspartner seinerseits ist nicht berechtigt, sich oder Dritten mittels der Dienste des Auftragnehmers nicht für ihn oder den Dritten bestimmte Daten und Informationen zu verschaffen.
- Bei Verletzung von Datenschutzvorschriften mit Schadensfolge für den Vertragspartner ist eine Vertragsstrafe in Höhe des vereinbarten monatlichen Fix-Entgeltes zu zahlen. Weitergehende Schadensersatzansprüche bleiben durch diese Regelung unberührt.
- Die Verletzung von Datenschutzvorschriften durch den Auftragnehmer bzw. durch vom Auftragnehmer beauftragte Dritte berechtigt den Vertragspartner zur fristlosen Kündigung.

14.5 Computerviren

Fachzeitschriften unterrichten regelmäßig über neue Computerviren sowie über vorbeugende Maßnahmen gegen einen Virenbefall. Sogar Tageszeitungen berichten häufig über das Auftreten neuer Computerviren und über die damit verbundenen Gefahren. Dennoch werden diese Hinweise von öffentlichen Verwaltungen nicht genügend beachtet, werden vor allem keine ausreichenden Vorsichtsmaßnahmen getroffen. Ein Virenbefall von PCs - so geschehen auch in einem sächsischen Landratsamt - ist die Folge.

Computerviren sind gezielt hervorgerufene Softwareanomalien, die eine Datenveränderung oder Datenzerstörung ohne Wissen und Zutun des Anwenders bewirken. Sie verhalten sich wie echte Viren, sie pflanzen sich fort und bleiben oft lange Zeit unbemerkt, bis ihre schädigende Wirkung einsetzt.

Neben den herkömmlichen Computerviren werden in der Fachliteratur noch andere Softwareanomalien unter folgenden Namen aufgeführt: "Trojanische Pferde", "Logische Bomben", "Falltüren", "Würmer" und "Spoofing-Programme". Sie unterscheiden sich in ihrer Wirkweise, jedoch nicht im Resultat - der unbefugten Datenveränderung oder -zerstörung. Deshalb wird im folgenden "Computerviren" als Oberbegriff für alle unerwünschten Softwareanomalien verwandt.

Computerviren können über Standleitungen, Wählleitungen/Modem und Glasfaserleitungen übertragen oder auch auf einem Datenträger weitergegeben werden. Sie befallen nicht nur Einzelplatz-PCs mit dem am meisten verbreiteten Betriebssystem MS-DOS, sondern auch die Systeme OS/2, UNIX, Windows 95, Windows NT oder Novell Netzwerke etc. Für jedes dieser Betriebssysteme existieren spezielle Viren und Virenschutzprodukte.

Neben den häufigsten Computerviren, die ausführbare Programme (*.COM, *.EXE) befallen, gibt es noch sogenannte Makroviren. Sie nisten sich als Makros getarnt in Word- und EXCEL-Makros ein und können sich so - systemunabhängig - besonders schnell verbreiten.

Die Gefahr, die von Computerviren ausgeht, ist deshalb besonders groß, weil ihre schädigende Wirkung häufig erst mit Zeitverzögerung einsetzt und die Viren sich inzwischen bereits weit verbreitet haben. Dabei gefährden Computerviren häufig nicht nur die Daten und Programme auf einem einzelnen Computer, sondern wegen der zunehmenden Vernetzung auf einer Vielzahl von EDV-Anlagen.

Die Nichtverfügbarkeit eines Datenverarbeitungssystems oder die Verletzung der Integrität (Unversehrtheit) der Daten und Programme nach Virenbefall bewirkt in der öffentlichen Verwaltung einen erheblichen wirtschaftlichen Schaden. Der Schaden für das Gemeinwohl ist oft noch höher einzustufen.

Vorbeugende Sicherheitsmaßnahmen gegen Virenbefall

Die Gewährleistung der Sicherheit ihrer Informationssysteme ist eine wichtige Aufgabe der öffentlichen Verwaltung. Dazu gehört der Schutz vor einer "Infektion" mit Computerviren.

Der PC-Benutzer bemerkt einen Virenbefall meist erst, wenn Unregelmäßigkeiten bei der Bedienung auftreten, Daten verändert oder zerstört sind, also erst während der sogenannten Schadensphase. Es ist jedoch möglich, Computerviren bereits während der Ausbreitungsphase zu entdecken und zu beseitigen. Geeignet sind dazu vor allem Prüfsummenprogramme und Virenscanner. Der Einsatz dieser Prüfsoftware setzt voraus, daß sie schon vor dem Virenbefall auf dem PC installiert worden ist.

Prüfsummenprogramme berechnen bei der Installation eines Programmes für jede ausführbare Datei eine Prüfsumme, die versteckt abgespeichert wird. Diese Berechnung kann jederzeit erneut durchgeführt werden und mit dem zuletzt abgespeicherten Ergebnis verglichen werden. Stimmen beide Ergebnisse überein, ist die Programmdatei unverändert. Ist das Ergebnis nicht identisch, wurde die Programmdatei inzwischen verändert. Als mögliche Ursache dafür ist eine Infektion mit Computerviren in Betracht zu ziehen.

Mit einem Virenscanner läßt sich die Programmdatei nach den bislang bekannten Viren durchsuchen und diese entfernen. Jedes Virus hat einen charakteristischen Aufbau, eine bestimmte Kombination von Bytes. Beim Prüfen mit einem Virenscanner werden die Programmdateien mit dem in einer Tabelle gespeicherten Aufbau bekannter Viren verglichen. Ein Nachteil besteht darin, daß nur nach bereits bekannten Viren gesucht werden kann. Deshalb müssen die Virensuchprogramme regelmäßig durch ein Update etwa vierteljährlich aktualisiert werden.

Auf weitere vorbeugende Maßnahmen sei ohne nähere Erläuterung hingewiesen:
- Vor Installation eines neuen Programmes Programmdisketten auf Viren prüfen,
- nur schreibgeschützte Programmdisketten nutzen,
- Programme versiegeln,
- PCs und Datenträger mit Prüfsummen- und aktuellem Virensuchprogramm überprüfen,
- PC durch zusätzliche Hardware (Steckkarte zur Abwehr von Viren) schützen,
- PCs und Datenträger vor unbefugter Benutzung (Zugangs- und Zugriffskontrolle) schützen,
- Nutzung privater Disketten (auch Fremd-, Test- und Demo-Disketten) auf Dienst-PC verbieten,
- Nutzung dienstlicher Disketten auf privaten PCs verbieten,
- Notfall-Diskette (Startprogramm für Betriebssystem) für Haveriefall erstellen,
- Boot-Reihenfolge vom Diskettenlaufwerk (i. d. R. Laufwerk A:) auf Festplattenlaufwerk (i. d. R. C:) ändern,
- Disketten vor dem Versand auf Virenbefall überprüfen und mit Schreibschutz

versehen,
- möglichst PCs ohne Diskettenlaufwerke einsetzen oder Diskettenlaufwerksschlösser anbringen,
- Schutz vor Makroviren:
    - Keine fremden/unbekannten Dokumente mit MS-Word oder MS-EXCEL laden, ohne vorher eine Virenprüfung durchgeführt zu haben,
    - Schreibschützen der NORMAL.DOT für Word bzw. GLOBAL.XLS für EXCEL,
    - Drücken der Shift-Taste beim Hochfahren von Winword bzw. beim Öffnen von Dokumenten.
- Regelmäßige Datensicherungen (vor allem nach größeren Veränderungen der Daten) durchführen,
- Mitarbeiter über Computerviren informieren,
- Verfahrensweise bei Virenbefall schriftlich festlegen.

Verhalten bei Befall eines PC mit Viren

Hinweise auf Virenbefall können beispielsweise folgende Phänomene sein: unbekannte Fehlermeldungen, vermehrte Festplatten- und Diskettenzugriffe, unerklärliches Verschwinden von Dateien, Nachlassen der Rechnerleistung, vorher nicht aufgetretene Programmabstürze. Bei diesen Symptomen wird folgendes Verhalten empfohlen:
- Bei Verdacht, Anwendung unverzüglich (wie gewohnt) beenden und PC ausschalten,
- Fachmann zu Rate ziehen,
- PC von virenfreier, schreibgeschützten Systemdiskette (Notfall-Diskette) neu starten,
- PC mit aktuellem Virensuchprogramm prüfen (evtl. Datensicherung durchführen),
- Viren (File- und Bootviren von Festplatte) entfernen, infizierte Disketten vernichten (z. B. Schreddern) oder mit „FORMAT A: /U“ formatieren,
- PC erneut mit Virensuchprogramm (Kontrolle) überprüfen,
- mögliche Quelle der Infektion ermitteln und andere Anwender warnen,
- Anwendersoftware und Datendateien wiederherstellen.

Werden die oben aufgeführten Sicherheitsmaßnahmen zukünftig beachtet, können die Schäden begrenzt und Infektionen weitestgehend vermieden werden. Es gibt allerdings keinen absoluten Schutz vor Computerviren.

14.6 "Datensammlungen im Büro" durch automatisierte Textverarbeitung

Jeder Brief, jedes Protokoll, jeder Vermerk - sofern mittels PC erstellt - wird in eine Datei oder ein Dateisystem abgelegt und verbleibt dort in vielen Fällen so lange, wie dies im Hinblick auf die einwandfreie (weitere) Nutzung des Textverarbeitungssystems nicht als störend empfunden wird - etwa solange genügend Speicherplatz verfügbar ist. Dies kann durchaus der Fall sein, bis der PC insgesamt aus dem Verkehr gezogen wird. Auf diese Weise kann das Schreibsystem früher oder später zu einer Datensammlung "entarten", deren jederzeitige Verfügbarkeit im Widerspruch zu den vorgeschriebenen Aufbewahrungsfristen einschlägiger schriftlicher Dokumente steht. Dabei fallen wohl

nur in verschwindend geringem Maße solche "elektronischen Dokumente" an, die keine personenbezogenen oder -beziehbaren Daten enthalten (mindestens Namen- bzw. Adressenangaben sind im allgemeinen immer darin enthalten); d. h. das Recht auf informationelle Selbstbestimmung ist berührt.

Leider verführt die Unsichtbarkeit solcher Datensammlungen im Gegensatz zu greif- und sichtbaren Aktenbergen oder großräumigen Registraturen dazu, die elektronisch gespeicherten verborgenen Daten bezüglich ihrer durchaus eben so hohen Schutzwürdigkeit kaum zu beachten. Das heißt, die für Dateien vorgeschriebenen Löschungen gemäß § 19 Abs. 1 Nr.2 SächsDSG bzw. gemäß einschlägigen datenschutzrechtlichen Spezialregelungen finden nicht statt. Textverarbeitungssysteme sind diesbezüglich eine Grauzone (obwohl sie hinsichtlich Recherchemöglichkeiten mit Datenbanken bzw. Dateisystemen vergleichbar sind und die Speicherkapazität einer Festplatte durchaus dem Aktenaufnahmevermögen eines Registraturraumes entspricht).

Es liegt auf der Hand, daß die enormen Vorzüge moderner Textverarbeitungssysteme gegenüber der Benutzung herkömmlicher Schreibtechnik nicht durch restriktive Datenschutzvorschriften gemindert oder gar weitgehend zurückgedrängt werden sollen. Wegen des heterogenen Inhalts des Datenbestandes eines Schreibsystems verbieten sich ohnehin pauschale Löschungsfristen (man weiß meistens nie, wann welcher Text noch einmal gebraucht werden könnte) und normierte Sicherheitsstandards (diese müßten zwangsläufig auf das "sensibelste" Dokument abstellen). Andererseits ist es auch nicht praktikabel, das Dateisystem etwa nach derartigen Kriterien aufzugliedern, weil dann jedes zu erstellende Dokument entsprechend kategorisiert werden müßte.

Es bleiben also lediglich gewisse Empfehlungen für den Umgang mit dem Speicherinhalt von Textverarbeitungssystemen, auf die der Blick der Verantwortlichen gelenkt werden soll, um wenigstens etwas zur Datenschutz-Risikominderung beizutragen.
Jeder Nutzer muß je nach Schutzwürdigkeit der Daten zwei Prinzipien beachten:

1. Dokumente hochgradig sensiblen Inhaltes sollten gar nicht auf der Festplatte gespeichert bleiben, sondern unverzüglich nach dem Ausdruck gelöscht werden. Ggf. kann in Ausnahmefällen wegen abzusehender Änderungen eine Kopie auf Diskette abgelegt werden. Diese sollte dann allerdings z. B. getrennt vom Dokument aufbewahrt bzw. gesichert werden, aber mindestens den gleichen Schutzmaßnahmen wie das Schriftstück selbst unterliegen (einschließlich Löschung bzw. - besser - Überschreiben).

2. Alle sonstigen Dokumente sollten zweckmäßigerweise dann von der Festplatte entfernt werden, wenn sie innerhalb eines angemessenen Zeitraumes nicht mehr "bewegt" worden sind; beispielsweise könnte (mittels Dateimanager) halbjährlich der Bestand nach Dokumenten "durchforstet" werden, die mindestens ein Jahr lang

keine Veränderung mehr erfahren haben, um sie auf der Festplatte zu löschen und ggf. - wiederum für einen angemessenen Zeitraum - auf externe Datenträger zu archivieren.

Weitere bürospezifische Maßnahmen sind denkbar, wobei es nie darum gehen sollte, jegliches Datenschutzrisiko auszuschließen zu wollen, wohl aber ein angemessenes Schutzniveau anzustreben (§ 9 Abs.1 Satz 2 SächsDSG).

14.7 Anforderungen zur informationstechnischen Sicherheit bei Chipkarten, erstellt vom Arbeitskreis "Technik" der Konferenz der Datenschutzbeauftragten des Bundes und der Länder[26]

I. Einleitung

Chipkarten sind miniaturisierte IT-Komponenten, meist in der genormten Größe einer Kreditkarte. Sie haben Eingang ins tägliche Leben gefunden, gewinnen zunehmend an gesellschaftlicher Bedeutung und bedürfen aus der Sicht des Datenschutzes zur Wahrung der informationellen Selbstbestimmung und der informationstechnischen Sicherheit größter Aufmerksamkeit.

Die derzeit bekannteste Chipkarten-Anwendung ist die Telefonkarte, die ein Guthaben enthält, das beim Gebrauch der Chipkarte in einem Kartentelefon reduziert wird, bis das Konto erschöpft ist und die Chipkarte unbrauchbar wird. Ebenfalls allgemein bekannt ist die Krankenversichertenkarte (KVK), die lediglich einen gesetzlich vorgegebenen Inhalt hat und zur Identifizierung des Patienten sowie zur Abrechnung ärztlicher Leistungen verwendet wird. Sie ist ein Beispiel für eine Chipkarte, die lediglich die dem Versicherten erkennbare Oberfläche einer umfassenden IT-Infrastruktur ist. Was unterhalb dieser Oberfläche geschieht, ist für die Betroffenen nicht transparent.

Weitere neue Anwendungsbereiche von Chipkarten sind derzeit in der Diskussion bzw. in der Erprobung, z. B.:
- die Chipkarte im bargeldlosen Zahlungsverkehr,
- Gesundheits- oder Patientenchipkarten zur Speicherung und Übermittlung medizinischer Daten.

Von der Technik her sind reine Speicherchipkarten zur Aufnahme von Daten (meist in Halbleiter-Technologie oder optischer Speichertechnik) von solchen Karten zu

[26] Die hiermit vorgelegte Ausarbeitung entspricht dem Wissensstand von Dezember 1996. Der schnelle Fortschritt bei der Entwicklung der Chipkartentechnologien macht im Prinzip eine ständige Anpassung erforderlich. Die Arbeitsgruppe hat jedoch beschlossen, zunächst ein fertiges Papier mit festgelegtem Aktualitätsstand vorzulegen, da sonst die Gefahr besteht, nie zu einem Abschluß zu kommen. Jedoch ist es geeignet, in weiteren Arbeitsschritten fortgeschrieben zu werden.
Zur besseren Lesbarkeit der Ausarbeitung wird sie durch ein *Abkürzungsverzeichnis* ergänzt.

unterscheiden, in die Mikroprozessoren und speichernde Bauteile integriert sind. Solche Prozessorchipkarten sind als Kleinstcomputer ohne Mensch-Maschine-Schnittstelle anzusehen. Ihre Verwendung bedarf also zusätzlicher technischer Systeme zum Lesen der gespeicherten Daten, zum Aktivieren der Funktionen der Mikroprozessoren und zum Beschreiben der Speicher.

Systeme zur Erschließung der Funktionen von Chipkarten werden im folgenden Chipkartenbasierte Dienstleistungssysteme (CDLS) genannt. Beispiele für solche Systeme sind:

- Öffentliches Telefon-Kartenterminal,
- Funktelefon (Handy),
- PC mit externem Kartenterminal oder integriertem Kartenleser,
- Laptop mit PCMCIA-Kartenleser,
- Geldausgabeautomat,
- Point-of-Sale-Kartenterminal (POS-Kartenterminal),
- Versicherten-Kartenterminal in seiner Stand-alone-Ausführung (ohne PC-Anschluß),
- Kontoauszugsdrucker,
- Airline-Checkin-Terminal,
- Customer-Service-Terminal,
- Fahrschein-/Parkticket-Terminal.

Sicherheitsbetrachtungen zum Einsatz von Chipkarten müssen deshalb auch die Sicherheit dieser Infrastrukturen einbeziehen.

Wichtige Funktionalitäten der Chipkarten sind:

- Chipkarten als Speicher von Daten, die hinsichtlich ihrer Vertraulichkeit und/oder Integrität hohen Schutzbedarf aufweisen (z. B. Kontodaten, medizinische Individualdaten, Personalausweisdaten, Führerscheindaten),
- Chipkarten als Mittel zur Authentisierung ihres Trägers für die Gewährung des Zugriffs auf sicherheitsrelevante Daten und Funktionen (Kontoverfügungen, Änderung medizinischer Individualdaten),
- Chipkarten als Mittel zur Signatur von Dokumenten (Verträge, Willenserklärungen, Befunde etc.),
- Chipkarten als Träger elektronischer Geldbörsen.

Die weiteren Ausführungen dieses Papiers beschränken sich auf die für die Sicherheit der Informationstechnik relevanten Merkmale und Anforderungen an Chipkarten, sowohl in ihrer Funktion als Instrumente zur Herstellung von Sicherheit als auch als sicherheitsbedürftige IT-Komponenten.

Obwohl - wie die Krankenversichertenkarte zeigt - auch Speicherchipkarten datenschutzrechtlich relevant sind, beschränken sich die weiteren Ausführungen auf Prozessorchipkarten. Diese haben in Zukunft sowohl hinsichtlich ihrer Verbreitung

und Anwendung als auch in Hinblick auf datenschutzrechtliche Chancen und Risiken eine größere datenschutzrechtliche Bedeutung.

II. Empfehlungen zum Einsatz von Chipkarten

Für den datenschutzgerechten Einsatz von Chipkarten ist eine konsequente und überzeugende Sicherungstechnologie erforderlich. Datensicherungsmaßnahmen müssen in ihrer Gesamtheit einen hinreichenden Schutz der Daten vor Mißbrauch gewährleisten. Dabei ist von folgenden Gefahren auszugehen:

- unbefugte Preisgabe von Informationen (Verlust der *Vertraulichkeit*),
- unbefugte Veränderung von Informationen (Verlust der *Integrität*),
- unbefugte Vorenthaltung von Informationen oder Betriebsmitteln (Verlust der *Verfügbarkeit*),
- unbefugte Änderung identifizierender Angaben (Verlust der *Authentität*).

Diese Gefahren sind sowohl dann zu betrachten, wenn die Daten auf der Chipkarte gespeichert werden, als auch dann, wenn sie in einer externen Datenbank gespeichert werden, die durch Chipkarten erschlossen wird.

Vor der Entscheidung über den sicherheitsrelevanten Einsatz von Chipkarten-Anwendungen sollte eine projektbezogene Technikfolgenabschätzung durchgeführt werden, so wie dies Art. 20 der EU-Datenschutzrichtlinie als Vorabkontrolle fordert. Zur Auswahl geeigneter und angemessener Sicherungsmaßnahmen ist eine systematische Einschätzung der Gefahren für das informationelle Selbstbestimmungsrecht und das Recht auf kommunikative Selbstbestimmung vorzunehmen und sind Lösungsvorschläge für eine Sicherungstechnologie zu erarbeiten.

Die Auseinandersetzung mit dem Phänomen "Chipkarte" zwingt zur Differenzierung zwischen den technischen Systemen und den Applikationen, die sich dieser Systeme bedienen, und der Chipkarte selbst. Genausowenig wie es "die" Chipkarte gibt, genausowenig kann man von "der" Chipkartenanwendung sprechen. Würde man datenschutzrechtliche und sicherheitstechnische Schlußfolgerungen ausschließlich aus einer der vielen Kombinationsmöglichkeiten ziehen, wäre eine Allgemeinverbindlichkeit der Aussagen bzw. Anforderungen nicht zu erreichen. Konkrete Rechtsprobleme und Risiken lassen sich nur mit einem Bezug zu bestimmten inhaltlichen und technischen Rahmenbedingungen aufzeigen. Die geplanten Gesundheits- und Patientenchipkartensysteme sind insoweit geeignete Beispiele.

Notwendig erscheint auch eine dauernde Bereitschaft, die schnell fortschreitende technologische Weiterentwicklung aufmerksam zu begleiten und bei Bedarf steuernd einzugreifen, denn die datenschutztechnischen Fragestellungen werden um so komplexer, je weiter sich die Chipkartentechnologie entwickelt.

Künftige neue Anwendungen werden sich tendenziell der Prozessorchipkartentechnologie bedienen. Prozessorchipkarten sind miniaturisierte Computer, die allerdings nicht über eigene Mensch-Maschine-Schnittstellen verfügen. Diese werden über CDLS realisiert. Datenschutzrechtliche Anforderungen erstrecken sich hier neben den CDLS auch auf die Rahmenbedingungen bei der Herstellung, bei der Initialisierung, beim Versand und bei der Ersatzbeschaffung von Chipkarten in Fällen des Verlustes oder der Zerstörung einschließlich des "Ungültigkeitsmanagements". Die Hersteller bieten Chipkarten an, deren Leistungsfähigkeit und Funktionsweise diesbezüglich zum Teil sehr unterschiedlich ist. Eine Standardisierung wäre auch aus datenschutzrechtlicher Sicht in diesem Bereich dringend zu empfehlen.

Das Sicherungskonzept für Chipkarten sollte folgende Mindestanforderungen erfüllen, wenn Schutzbedarf besteht:

1. Grundschutzmaßnahmen
- Ausstattung des Kartenkörpers mit fälschungssicheren Authentisierungsmerkmalen, wie z. B. Unterschrift, Foto, Hologramme
- Steuerung der Zugriffs- und Nutzungsberechtigungen durch die Chipkarte selbst
- Realisierung aktiver und passiver Sicherheitsmechanismen gegen eine unbefugte Analyse der Chip-Inhalte sowie der chipintegrierten Sicherheitsfunktionen
- Benutzung allgemein anerkannter, veröffentlichter Algorithmen für Verschlüsselungs- und Signaturfunktionen sowie zur Generierung von Zufallszahlen
- Sicherung der Kommunikation zwischen der Chipkarte, dem CDLS und dem ggf. im Hintergrund wirkenden System durch kryptographische Maßnahmen
- Sicherung unterschiedlicher Chipkartenanwendungen auf einer Chipkarte durch gegenseitige Abschottung
- Durchführung einer gegenseitigen Authentisierung von Chipkarte und CDLS mit dem Challenge-Response-Verfahren

2. Erweiterte Sicherungsmaßnahmen
- Realisierung weiterer "aktiver" Sicherheitsfunktionen des Betriebssystems, wie "Secure Messaging", I/O-Kontrolle aller Schnittstellen, Interferenzfreiheit der einzelnen Anwendungen, Verzicht auf Trace- und Debug-Funktionen und dergleichen. Zur Sicherung von Transaktionen oder zur Rekonstruktion nicht korrekt abgelaufener Transaktionen kann ein Logging vorhanden sein.
- Auslagerung von Teilen der Sicherheitsfunktionen des Betriebssystems in dynamisch bei der Initialisierung bzw. Personalisierung zuladbare Tabellen, damit der Chipkartenhersteller nicht über ein "Gesamtwissen" verfügt.

3. Grundsätzlich sollte zunächst die Möglichkeit in Betracht gezogen werden, daß bei der Chipkartenbenutzung Anonymität gewahrt bleiben kann. Ist dies nicht möglich, sollten Wahlmöglichkeiten anonymer Alternativen geschaffen werden.

4. Der Chipkarteninhaber bzw. die Betroffenen sollten die Möglichkeit erhalten, auf

neutralen, zertifizierten Systemumgebungen die Dateninhalte und Funktionalitäten ihrer Chipkarten einzusehen (Gebot der Transparenz).

5. Die gesamte Infrastruktur ist zu dokumentieren und die Produktion, die Initialisierung und der Versand der Chipkarten zu überwachen.

6. Für die gesamte Infrastruktur ist ein Mindestschutzniveau vorzuschreiben, das bei unbefugten Handlungen das Strafrecht anwendbar macht.

7. Alle Systemkomponenten datenschutzrelevanter Chipkartenanwendungen sind auf der Basis der Grundsätze ordnungsgemäßer Datenverarbeitung zu evaluieren.

8. Für die Informationsstrukturen sind zu Echtheits- und Gültigkeitsüberprüfungen (z. B. Abgleich gegen Sperr- und Gültigkeitsdateien) Kontrollmöglichkeiten zu schaffen.

9. Sicherheitsrelevante Karten (z. B. Bankkarten) sollten über den gesamten Lebenszyklus der Karte kryptographisch gesichert sein.

III. Technische Grundlagen

III.1 Hardware der Chipkarten

Chipkarten gibt es in vielfältigen Bauformen, Funktionsweisen und Funktionsspektren. Man unterscheidet Chipkarten hinsichtlich der

- Art der Datenübertragung bei der Interaktion mit der Außenwelt:
  ⇒kontaktbehaftet oder
  ⇒kontaktlos über elektromagnetische Felder (bestimmte kontaktlose Karten können auch über eine Entfernung von mehreren Metern von einem CDLS gelesen werden).
- Art der in der Karte bereitgestellten IT-Ressourcen:
  ⇒reine Speicherchipkarten mit nicht flüchtigem Speicher (z. B. Identifikationskarten),
  ⇒intelligente Speicherchipkarten mit EPROM (z. B.Telefonkarte) oder EEPROM (z. B. Krankenversichertenkarten),
  ⇒Prozessorchipkarten mit EEPROM, RAM, ROM und CPU,
  ⇒Prozessorchipkarten mit Coprozessor für die Abwicklung kryptografischer Verfahren (Krypto-Coprozessor).
- Art der Anwendung:
  ⇒elektronischer Zahlungsverkehr (Elektronische Geldbörse),
  ⇒Wegwerfkarten (Telefonkarte),
  ⇒wiederaufladbare Karten (z. B. Chipkarten im öffentlichen Personennahverkehr),
  ⇒multifunktionale wiederaufladbare Chipkarten (z. B. unterschiedliche

"Geldbörsen" auf einer Chipkarte),
⇒Berechtigungskarten (z. B. Mobiltelefone, Betriebsausweise).

Der Mikroprozessor einer Chipkarte leistet derzeit ca. 1 Million Befehle pro Sekunde. Direktzugriffsspeicher (RAM) erreichen eine Kapazität von 512 Byte, Festwertspeicher (ROM) für das Betriebssystem erreichen derzeit eine Kapazität von 16 KB, der elektrisch löschbare, programmierbare Festwertspeicher (EEPROM) mit der Kapazität von 16 KB erlaubt die Installation einer kleinen Datenbank. Im Vergleich dazu leisten Mikroprozessoren heute üblicherweise eingesetzter PC ca. 100 - 150 Millionen Befehle pro Sekunde und arbeiten mit RAM-Speichern von 8 - 32 MB.

III.2 Chipkarten-Betriebssysteme

Prozessorchipkarten verfügen über einen nicht überschreibbaren Speicherbereich, der keine Änderungen und somit auch keine Manipulationen ermöglicht.

In diesem "Read-Only-Memory" (ROM) befindet sich das Betriebssystem einer Chipkarte. Für Chipkarten-Betriebssysteme existieren u. a. die Normen aus der Serie ISO/IEC 7816, in der die Befehle solcher Systeme beschrieben werden. Die Chipkarten-Betriebssysteme nutzen diese Befehle in unterschiedlicher Weise, d. h., nicht jedes Betriebssystem unterstützt jedes Kommando oder jede Option eines Kommandos. Auch weisen fast alle Chipkarten-Betriebssysteme zusätzliche herstellerspezifische Kommandos auf. Die Chipkarten-Betriebssysteme ermöglichen die multifunktionale Nutzung von Chipkarten, können also mehrere unterschiedliche Anwendungen unterstützen.

Die folgende Darstellung wird an den internationalen Standard angelehnt:

III.2.1 Filesystem

Die Dateien des Betriebssystems sind hierarchisch organisiert. Den Ursprung des Dateisystems bildet das Master File (MF). Auf der MF-Ebene können Daten vorhanden sein, die von allen Anwendungen der Chipkarte gemeinsam genutzt werden (z. B. Daten über den Karteninhaber, Seriennummer, Schlüssel). Sie sind in der Regel in Elementary Files (EF) abgelegt.

Daneben gibt es auch sog. Dedicated Files (DF), die mit ihren untergeordneten EFs und ihren Funktionen die Anwendungen in einer Karte repräsentieren. Für jedes DF können separate Sicherheitsfunktionen definiert werden. Die DFs einer Chipkarte sind physikalisch und logisch voneinander getrennt, können aber auf die Daten auf der MF-Ebene zugreifen.

EFs können dem Betriebssystem zugeordnet sein und damit Daten enthalten, die das

Betriebssystem nutzt, z. B. anwendungsbezogene Paßwörter, Schlüssel und andere Zugriffsattribute zu Nutzdaten. Ein direkter Zugriff mittels des CDLS ist nicht möglich.

Sie können aber auch die Nutzdaten einer Anwendung enthalten, die ggfs. erst nach einer Authentisierung unter Berücksichtigung von Sicherheitsattributen gelesen und/oder verändert werden. Es gibt unterschiedliche Dateistrukturen für EFs: Sie können Records mit fester (linear fixed) oder variabler (linear variable) Länge enthalten, können eine Ringstruktur mit fester Länge (cyclic) haben, können jedoch auch eine amorphe, d. h. vom Benutzer frei wählbare Struktur (transparent) aufweisen, auf denen auf Daten byte- oder blockweise zugegriffen werden kann.

III.2.2 Authentisierung

Die Authentisierungstechniken zwischen Chipkarte und einer externen Einheit werden in der Norm ISO/IEC 9798-2 beschrieben. Es wird dabei zwischen interner Authentisierung, bei der sich die Chipkarte gegenüber der externen Einheit authentisiert, und externer Authentisierung, bei der sich die externe Einheit gegenüber der Chipkarte authentisiert, unterschieden. Die gegenseitige Authentisierung ist in Vorbereitung.

Neben diversen Befehlen zum Lesen, Schreiben und Löschen (jeweils nach der Authentisierung) von Files sowie zur Auswahl von zu bearbeitenden Files definiert ISO 7816-4 einige Kommandos, die für die Implementation von Sicherheitsfunktionalitäten bedeutsam sind:

- VERIFY zur Benutzerauthentisierung mit einer PIN. Dies kann eine auf MF-Ebene gespeicherte globale PIN oder eine DF-spezifische anwendungsbezogene PIN sein. Der Befehl überträgt die vom Nutzer eingegebene PIN und - falls erforderlich - die Nummer der zu überprüfenden PIN an die Karte. Diese vergleicht die eingegebene PIN mit dem gespeicherten Referenzwert. Ein Erfolg wird durch Senden des Status "OK" angezeigt, ansonsten ein interner Fehlversuchszähler dekrementiert und als Status "nicht OK" übertragen. Bei Zählerstand 0 wird die Anwendung der Applikation, die die PIN benutzt, blockiert. Bei einigen Betriebssystemen kann die Blockierung durch Eingabe eines Personal Unblocking Key (PUK) aufgehoben werden, der ebenfalls durch einen Fehlerzähler geschützt ist.

- INTERNAL AUTHENTICATE löst eine interne Authentisierung aus. Dazu erhält die Chipkarte den Schlüsselbezeichner des ausgewählten EF und Authentisierungsdaten (Zufallszahl). Die Chipkarte verschlüsselt dann die Zufallszahlen mit dem Schlüssel des ausgewählten EF und sendet das Chiffrat zurück. Die prüfende Einheit (z. B. das CDLS oder eine Patientenkarte) entschlüsselt und prüft die Übereinstimmung der Zufallszahlen.

– EXTERNAL AUTHENTICATE löst die externe Authentisierung aus. Dazu wird mit dem Befehl GET CHALLENGE eine Zufallszahl von der Chipkarte gefordert, die an die zu authentisierende Instanz übergeben wird. Diese verschlüsselt sie und sendet das Ergebnis zusammen mit der Nummer des zu verwendenden Schlüssels an die Karte zurück. Dann entschlüsselt die Karte die Zufallszahl mit dem Schlüssel der angegebenen Schlüsselnummer. Bei Übereinstimmung wird die zu authentisierende Instanz als authentisch anerkannt.

Weitere Sicherheitsfunktionen werden derzeit in ISO 7816-8 spezifiziert. Von besonderer Bedeutung ist hierbei das Kommando PERFORM SECURITY OPERATION, mit dem folgende Sicherheitsoperationen ausgeführt werden können:
– COMPUTE DIGITAL SIGNATURE,
– VERIFY DIGITAL SIGNATURE,
– VERIFY CERTIFICATE,
– HASH,
– COMPUTE CRYPTOGRAPHIC CHECKSUM,
– VERIFY CRYPTOGRAPHIC CHECKSUM,
– ENCIPHER,
– DECIPHER.

In ISO 7816-7 sind außerdem spezielle Sicherheitsfunktionen beschrieben, die sich auf Chipkarten mit einer sog. SCQL-Datenbank (Structured Card Query Language) beziehen.

III.3 Chipkartenbasierte Dienstleistungssysteme (CDLS)

Wie in der Einleitung kurz dargestellt, sind Chipkarten nicht als isolierte Träger von Risiken zu betrachten, wenn es um Fragen ihrer IT-Sicherheit geht. Aufwendige sicherheitstechnische Maßnahmen an und in der Chipkarte können durch unsichere Systemumgebungen bei der weiteren Verwendung der Daten konterkariert werden.

Wenn zum Beispiel das System eines zugriffsberechtigten Arztes nicht den erforderlichen Schutz bietet, können die Schutzmaßnahmen der Karte umgangen werden. Der Schutz der Chipkarte gegen unbefugte Manipulationen ist weitgehend wertlos, wenn beim elektronischen Zahlungsverkehr das POS-Terminal leicht manipuliert werden kann. Jedoch sieht ISO/IEC 7816 Schutzmechanismen vor, die bei richtiger Anwendung mit vertretbarem Aufwand nicht umgangen werden können.

Hier sollen jedoch nur für solche Komponenten Sicherheitsbetrachtungen angestellt werden, die chipkartenspezifisch sind. Solange die Chipkarten keine eigenen Mensch-Maschine-Schnittstellen enthalten, sind für die Erschließung der Chipkarteninhalte und -funktionen Systeme notwendig, mit denen die Chipkarten gelesen und beschrieben werden können. Auch wenn es einmal möglich sein wird, direkt mit der Chipkarte zu kommunizieren, z. B. über Sensorfelder, werden CDLS kaum entbehrlich sein, denn

sie stellen zumindest die Schnittstelle zu jenen Nutzern dar, die mit dem Inhaber der Karte nicht identisch sind. CDLS können eigene Verarbeitungskapazitäten bieten und auch die Verbindung zu anderen Systemteilen herstellen.

Bisher sind für alle Chipkarten-Anwendungen (Telefonkarten, Krankenversichertenkarten, Sicherungskarten für Mobiltelefone usw.) spezielle CDLS entwickelt und eingesetzt worden. Soweit erkennbar, werden universell einsetzbare CDLS bisher nicht auf dem Markt angeboten. Im Gesundheitswesen werden derzeit CDLS eingesetzt, deren Verwendung auf die Kommunikation mit der Krankenversicherungskarte eingeschränkt wurde. Da sich weitergehende Anwendungen abzeichnen, wurde eine Spezifikation für multifunktionale CDLS angefertigt, die von einem Arbeitskreis der Arbeitsgemeinschaft "Karten im Gesundheitswesen" und der Gesellschaft für Mathematik und Datenverarbeitung (GMD) herausgegeben worden ist.

Dieser Spezifikation liegt folgende Konzeption zugrunde:

- Die CDLS sind transparent für jeden Dialog zwischen einem Anwendungsprogramm und einer Chipkarte, sofern dieser Dialog über eine genormte Schnittstelle geführt wird. Damit ist ihre Anwendung auch außerhalb des Gesundheitswesens möglich.
- Allerdings ist die Option, ein universell einsetzbares CDLS zu schaffen, aus pragmatischen Erwägungen heraus relativiert worden. Von den nach ISO 7816-3 zulässigen Optionen für die Übertragungsparameter wird nur ein Teil als obligatorisch gefordert. Dies entspricht der Politik des Kreditkartensektors, die zulässigen Lösungen enger zu fassen als das Spektrum der Optionen. Der Spezifikation entsprechende CDLS können sowohl mit synchronen Chipkarten wie die Krankenversicherungskarte als auch mit Prozessor-Chipkarten kommunizieren, die ein standardisiertes Übertragungsprotokoll unterstützen.
- Es können anwendungsspezifische Funktionen im CDLS realisiert werden, die dann nicht dem Anwendungsprogramm überlassen werden, solange nicht andere Vorkehrungen zum Schutz der Karte vor unbefugten oder durch Fehlfunktionen ausgelösten schreibenden Zugriffen getroffen sind. So ist z. B. ein Modul zur Verarbeitung der Versichertenkarte gem. § 291 SGB V für Gesundheitskarten-Terminal spezifiziert worden.
- Es können je nach Anwendung weitere anwendungsspezifische Module definiert werden, die periphere Geräte steuern. So wurde für die Gesundheitschipkarten ein Modul definiert, das einen Drucker steuert, damit Ärzte ohne IT-Einsatz die Kartensysteme zumindest für die Übertragung des Inhalts der Versichertenkarte auf die Belege der vertragsärztlichen Versorgung nutzen können. Das Druckmodul mit der parallelen Schnittstelle ist optional zu realisieren.
- Eine Download-Funktion erlaubt die Behebung von Softwarefehlern und ggf. im gewissen Umfang einen Upgrade von Leistungen.
- Die Spezifikation gilt für kontaktbehaftete Chipkarten nach ISO 7816 in 5-Volt-Technologie. Kontaktlose Chipkarten und kontaktbehaftete Chipkarten in 3-Volt-Technologie sollen einbezogen werden, wenn die Normung Klarheit geschaffen hat.

Das gleiche gilt für eine Erweiterung von Standards für die Nutzung der Kontakte und für höhere als derzeit spezifizierte Übertragungsraten.
- Das Anwendungssystem in einem PC wird auf eine anwendungsunabhängige Schnittstelle für die Integration der Chipkartentechnik aufgesetzt.
- CDLS als separate Endgeräte können zusätzlich mit folgenden Optionen ausgestattet sein:
  - Display und/oder Tastatur,
  - mehrere Kontaktiereinheiten für eine Chipkarte im Normalformat gem. ISO-IEC 7816-2 oder
  - im Plug-in-Format.

IV. Sicherheitstechnische Gestaltungsspielräume

Für die Entwicklung sicherer Chipkartenanwendungen gibt es eine Vielzahl von Ansatzpunkten, die je nach den in einer anwendungsspezifischen Sicherheitspolitik definierten Anforderungen zur Verbesserung der Sicherheit mit gewissen Spielräumen ausgenutzt werden können. In diesem abschließenden Kapitel geht es einerseits darum, diese sicherheitstechnischen Gestaltungsspielräume darzustellen und andererseits die Empfehlungen der Datenschutzbeauftragten zur Ausschöpfung dieser Spielräume hervorzuheben.

IV.1 Allgemeine Anforderungen

Wie bereits einleitend dargestellt, sind Chipkarten als miniaturisierte Computer anzusehen, die (noch) nicht über eigene Mensch-Maschine-Schnittstellen verfügen. Daraus ergeben sich folgende Konsequenzen:
- Chipkarten sind leicht transportable Rechner. Die besonderen Bedrohungen der IT-Sicherheit, die z. B. bei anderen transportablen Rechnern (Laptops, Notebooks,...) berücksichtigten werden müssen, existieren in ähnlicher Weise auch für Chipkarten.
- Die Interaktion zwischen Mensch und Chipkarte bedarf zwischengeschalteter technischer Systeme (CDLS), die ebenfalls besonders zu sichern sind. Eine Chipkarte bildet zusammen mit dem CDLS ein vollständiges Rechnersystem mit Ein- und Ausgabekomponente. Die Evaluation der richtigen Funktionsweise setzt voraus, daß dabei alle Systemkomponenten einbezogen sind.
- Speicher- und Prozessorkapazitäten bilden Schranken für Sicherheitsfunktionen. Die technische Entwicklung dürfte diese Engpässe bald beseitigen. Heutige Betrachtungen müssen sie jedoch noch berücksichtigen.

Allgemein sind an die Sicherheitsfunktionen folgende Anforderungen zu stellen:
- Zugriffs- und Nutzungsberechtigungen sollten soweit möglich von der Chipkarte selbst geprüft und gesteuert werden.
- In Anwendungen sollten sich alle beteiligten Rechner (incl. Chipkarten) gegenseitig authentifizieren. Die Authentifizierung des Benutzers hat gegenüber der Chipkarte

zu erfolgen, wobei für die Zukunft angestrebt werden sollte, daß dies in sicherer Umgebung oder ohne zwischengeschaltete Systeme erfolgen kann. Dies würde eine autonome Stromversorgung der Chipkarte und geeignete Mensch-Maschine-Schnittstellen voraussetzen (z. B. Sensorfelder für biometrische Merkmale).
- Es muß grundsätzlich ein Mindestschutz vorhanden sein, mit dem die in § 202a Abs. 1 StGB geforderte "besondere Sicherung gegen unberechtigten Zugang" realisiert wird, um bei unbefugter Nutzung einer Chipkarte das Strafrecht anwendbar zu machen.

IV.2 Hardwarebezogene Maßnahmen zur IT-Sicherheit bei Chipkarten

IV.2.1 Herstellung, Initialisierung und Versand von Chipkarten

Sicherheitserwägungen greifen bereits bei der Herstellung, Initialisierung und dem Versand von Chipkarten. Dabei müssen
- die Produktion der Prozessoren und Chipkarten,
- die Produktion und das Laden von Software,
- das Erzeugen der Schlüssel,
- das Laden der Schlüssel in die Sicherheitsmodule (Internal Elemetary Files),
- das Laden von Hersteller- und Transportschlüssel für die spätere Initialisierung und
- der Versand der Chipkarten und Transportschlüssel an den Empfänger

durch entsprechende technische und organisatorische Maßnahmen abgesichert werden.

IV.2.2 Sicherheitsmerkmale des Kartenkörpers

Zur Unterstützung der Authentifizierung des Karteninhabers gegenüber der Chipkarte und damit des Nachweises, daß die Chipkarte
- zur jeweiligen Anwendung gehört und
- die die Karte vorlegende Person die Karte rechtmäßig nutzt,

sollte der Kartenkörper mit Sicherheitsmerkmalen ausgestattet sein, die der Sensibilität angemessen sind:
- Aufdruck,
- Hologramm,
- Unterschrift des Besitzers (nur bei nicht anonymen Anwendungen),
- Foto des Besitzers (nur bei nicht anonymen Anwendungen),
- aufgebrachtes Echtheitsmerkmal,
- Multiple Laser Image (durch Lasergravur auf der Chipkarte aufgebrachte hologrammähnliches Kippbild mit kartenindividuellen Informationen).

Dabei ist allerdings zu berücksichtigen, daß es Sicherheitsmerkmale gibt, die z. B. bei anonymen Chipkartenanwendungen (z. B. anonyme Zahlungsverfahren) die Anonymität aufheben würden und daher dabei nicht verwendet werden können.

IV.2.3 Sicherheitsmechanismen der Chip-Hardware

Sicherheitsmechanismen der Chip-Hardware richten sich vor allem gegen die Analyse der Chip-Inhalte und -Sicherheitssysteme mit Hilfe von Spezialgeräten, z. B. durch Abtragen dünner Chipschichten. Dabei kann unterschieden werden zwischen passiven Mechanismen, bei denen eine bestimmte Bauweise des Chips die Schutzfunktionen ergibt, und aktiven Mechanismen, die auf äußere Eingriffe passend reagieren und ggfs. den Chip zerstören.

Passive Mechanismen:
- Es gibt von außen keine direkte Verbindung zu den Funktionseinheiten. Ein Testmodus, der eventuell später nicht mehr erlaubte Zugriffe auf den Speicher ermöglicht, muß irreversibel auf den Benutzermodus geschaltet werden können.
- Interne Busse werden nicht nach außen geführt.
- Der Datenfluß auf den Bussen wird mit Scrambling geschützt.
- Der ROM befindet sich in den unteren Halbleiterschichten, um eine optische Analyse zu verhindern.
- Gegen das Abtasten von Ladungspotentialen erfolgt eine Metallisierung des gesamten Chips.
- Die Chipnummern werden eindeutig vergeben (werden u. U. von den Anwendungen benötigt).

Aktive Mechanismen:
- Es wird eine Passivierungsschicht aufgebracht, deren Entfernen einen Interrupt auslöst, der die Ausführung der Software unterbindet, sowie Schlüssel und andere sicherheitsrelevante Daten löscht.
- Es erfolgt eine Spannungsüberwachung. Wenn der Spannungswert den zulässigen Bereich über- oder unterschreitet, wird die weitere Ausführung von Prozessorbefehlen unterbunden.
- Den gleichen Zweck verfolgt die Taktüberwachung. Es werden damit Angriffe erschwert, mit denen die Abarbeitung einzelner Befehle analysiert werden soll.
- Es erfolgt eine Power-On-Erkennung, um bei Reset einen definierten Zustand herzustellen.

IV.3 Softwarebezogene Maßnahmen zur IT-Sicherheit bei Chipkarten

IV.3.1 Basisalgorithmen für Schutzfunktionen der Software

Die Schutzfunktionen der Chipkarten-Software basieren auf den bekannten und teilweise standardisierten Algorithmen zur Verschlüsselung, Signatur und Generierung von Zufallszahlen.

Dazu gehören symmetrische Verschlüsselungsalgorithmen wie DES, Triple-DES, IDEA und SC85 und asymmetrische Verfahren wie RSA, Signieralgorithmen wie DSS und RSA mit RipeMD160, Einwegfunktionen zur Berechnung des MAC und für das Hashing wie SHA und RipeMD160 sowie Zufallszahlengeneratoren.

IV.3.2 Schutzfunktionalitäten und -mechanismen des Betriebssystems

Zunächst sollte sichergestellt sein, daß sich nicht alle Teile des Betriebssystems im ROM befinden, damit der Chiphersteller nicht über das ganze Wissen über die Sicherung der Chipkarte verfügt. Wesentliche Teile des Betriebssystems können bei der späteren Initialisierung über entsprechend authentisierte CDLS dynamisch aus Tabellen geladen werden.

Darüber hinaus sollte das Betriebssystem in folgender Weise Sicherheit "erzeugen":

a) Die Identifizierung und Authentifizierung des Benutzers erfolgt mittels PIN oder mit biometrischen Verfahren.

Üblicherweise erfolgt die Prüfung einer PIN. Zwar können die normale Forderungen zur Paßwortverwaltung bei Rechnern nicht voll auf Chipkarten übertragen werden, jedoch sollte die PIN-Länge je nach Sensibilität mindestens 4 oder mehr Stellen betragen, die Anzahl der Fehlversuche begrenzt sein, die Möglichkeit bestehen, die PIN zu ändern und eine Freischaltung der Karte auch mittels Personal Unblocking Key (PUK) in Abhängigkeit von der Anwendung ermöglicht werden.

Biometrische Verfahren erfassen Fingerabdrücke, Augenhintergründe, Handgeometrien, Sprachmerkmale oder Unterschriftsdynamiken, verformeln sie und übertragen das Ergebnis zur Überprüfung auf die Chipkarte.

b) Es erfolgt eine Zugriffskontrolle mit einer Rechteverwaltung, wobei die Zugriffsrechte an die einzelnen Dateien geknüpft werden. Den Dateien sind Sicherheitsattribute zugeordnet, mit denen festgelegt wird, ob die Dateien (Daten) gelesen, kopiert, beschrieben, gelöscht, gesperrt oder freigegeben werden dürfen.

c) Wenn anderen Personen als dem Karteninhaber Zugriffsmöglichkeiten auf die Chipkarte gewährt werden sollen, erfolgt dies im Rahmen einer Programm-Programm-Kommunikation mit einem anderen Rechner oder einer anderen Karte (z. B. mit einer Professional Card). Der Rechner bzw. die andere Karte muß authentifiziert werden.

Die Rechnerauthentifizierung wird meist nach einem auf DES basierenden Challenge-Response-Verfahren vorgenommen.

Nach dem gleichen Schema verläuft die gegenseitige Authentifizierung von Chipkarte und Professional Card. Beide Benutzer müssen ihre Chipkarte aktivieren. Dann erfolgt die Authentifizierung zwischen den beiden Karten, wobei das CDLS die Daten transparent weiterleitet.

d) Zum Schutz gegen Ausforschung und Manipulation erfolgt eine sichere Datenübertragung zwischen Chipkarte und CDLS ("Secure Messaging").

e) Auf Opto-Hybridkarten können die Daten auf der optischen Fläche verschlüsselt

abgelegt werden. Die Entschlüsselung kann mit Hilfe des Prozessors erfolgen, der die Schlüssel verwaltet.

f) Das Betriebssystem führt eine I/O-Kontrolle aller Schnittstellen gegen unerlaubte Zugriffe durch.
g) Die Interferenzfreiheit der einzelnen Anwendungen wird gewährleistet, d. h., eine gegenseitige unerwünschte Beeinflussung der Anwendungen wird ausgeschlossen.
h) Trace- und Debugfunktionen sind nicht verfügbar.
i) Beim Initialisieren des Betriebssystems werden RAM und EEPROM geprüft.
j) Fehleingaben werden abgefangen.
k) Der Befehlsumfang wird auf die notwendigen Befehle reduziert. Funktionalitäten, die nicht zugelassen werden sollen, werden vom Betriebssystem unterbunden.
l) Die Dateiorganisation, Header und Speicherbereiche im EEPROM werden durch Prüfsummen abgesichert.
m) Das Betriebssystem sieht die Möglichkeit vor, die Chipkarte durch Löschung zu deaktivieren (etwa nach Ablauf einer Gültigkeitsdauer), jedoch verhindert es die mißbräuchliche Deaktivierung.

IV.3.3 Die Sicherheit der Anwendung

Die Betrachtung der Sicherheit bei der Anwendung von Chipkarten setzt die ganzheitliche Betrachtung der Kommunikation zwischen Chipkarten, CDLS und im Hintergrund wirkenden Systemen voraus. Die Kommunikation zwischen den einzelnen Systemen und Systembestandteilen ist ebenfalls mit kryptographischen Methoden zu sichern:

- Zur Unterstützung der Sicherheit der Kommunikation dienen Funktionen des Chipkarten-Betriebssystems zur gegenseitigen Authentifizierung von Chipkarten und Rechnern, zur sicheren Datenübertragung und zum Signieren und Verschlüsseln (siehe IV.3.2. c), d)).
- Gegen die unberechtigte Nutzung der Daten auf der Chipkarte muß eine Zugriffskontrolle erfolgen, die auf einer sicheren Identifikation und Authentifizierung der Benutzer beruht (siehe IV.3.2 a, b).

Darüber hinaus sind die folgenden für die Sicherheit der Anwendung bedeutsamen Maßnahmen zu berücksichtigen:

- Den Dateien auf der Chipkarte sind Befehle zuzuordnen, die mit ihnen ausgeführt werden können. Die Ausführung anderer Befehle ist zu unterbinden.
- Zugriffe auf geschützte Datenbereiche und Veränderungen der Daten sollten protokolliert werden - vorzugsweise auf der Chipkarte. Die Anwendung muß die Auswertung der Protokolldaten unterstützen.
- Bedarfsweise sollten Überprüfungen durch Abgleich mit Hintergrundsystemen erfolgen, z. B. die Erkennung gesperrter Karten durch Abgleich mit Sperrdateien, Feststellung von Betragslimits im chipkartengestützten Zahlungsverkehr.
- Die eindeutige Nummer des Chips schützt vor der Erstellung von Dubletten.

Bei den letzten beiden Spiegelstrichen muß allerdings berücksichtigt werden, daß mit solchen Maßnahmen bei anonymen Systemen unter Umständen die Anonymität gefährdet sein kann. Es kann nicht immer ausgeschlossen werden, daß anonyme Chipkarten einzelnen Nutzern zugeordnet werden, wenn die Identifizierung der Karte möglich ist.

IV.4 Risiken und Anforderungen bei chipkartenbasierten Dienstleistungssystemen (CDLS)

Zwar bilden - wie oben festgestellt - Chipkarten und CDLS erst zusammen ein vollwertiges Rechensystem, jedoch befinden sich beide Komponenten in der Regel in unterschiedlicher Verfügungsgewalt, die Karte in der des Inhabers und das CDLS in der von Anwendern. Denkbar ist auch, daß bei Inhabern und Anwendern unterschiedliche Vorstellungen und Interessen mit der Nutzung verbunden werden. Wesentliche Teile der unabdingbaren Sicherheitsmechanismen der Karte können daher konterkariert werden, indem die Steuerungssoftware des CDLS verändert oder die Hardware des CDLS manipuliert wird. Eine Zertifizierung von CDLS kann sich daher nur auf unveränderliche Teile beziehen.

Wenn eine Chipkarte in ein CDLS eingeführt wird, gibt der Inhaber die Verfügungsgewalt über die Software auf der Karte und die ihn betreffenden Datenbestände auf. Eine unbefugte Veränderung der Software muß daher technisch verhindert werden.

Allerdings sind die Datenbestände grundsätzlich variabel. Sie können daher benutzt werden, über das CDLS Daten abzulegen, die für den Karteninhaber verdeckt sind und nur mit bestimmten Codes gelesen werden können (verdeckte Kanäle). Dies eröffnet Möglichkeiten für unbefugtes oder gar kriminelles Handeln.

Der Karteninhaber sollte daher nicht nur die Möglichkeit haben, sich den Inhalt der gespeicherten Daten anzeigen zu lassen, sondern die tatsächlichen Funktionen z. B. auf neutralen CDLS testen zu können. Wegen der u. U. unterschiedlichen Interessenlagen (z. B. in wirtschaftlichen Beziehungen) ist die Prüfung der korrekten Funktion der Software sowie umgekehrt des Ausschlusses ungewollter Funktionen im realisierbaren Rahmen zu ermöglichen.

Manipulationen an der Hardware und der Eingabesteuerungssoftware der CDLS können auch dazu führen, daß die geheimen oder unverfälschbaren Authentifizierungsmerkmale (PIN, biometrische Merkmale) bei der Authentifizierung des Kartenbesitzers in das CDLS übertragen und so Dritten bekannt werden.

Es sind daher folgende Sicherheitsanforderungen an CDLS zu stellen:

– Die CDLS müssen über mechanisch gesicherte Gehäuse verfügen, damit eine

Hardware-Manipulation verhindert oder erschwert bzw. erkennbar wird.

- Sicherheitsmodule, die die für die vertrauliche Kommunikation mit Chipkarten und die gegenseitigen Authentifizierungen erforderlichen Hauptschlüssel enthalten, sind mechanisch (zum Beispiel durch Vergießung in Epoxidharz) und elektrisch gegen vielfältige Angriffsformen besonders abzusichern. Jeder Angriff auf das Sicherheitsmodul muß zum Löschen aller Schlüssel im Sicherheitsmodul führen. Dies setzt auch voraus, daß das Sicherheitsmodul weitgehend von der Stromversorgung des CDLS autark sein muß.
- Die CDLS müssen alle automatisch prüfbaren Sicherheitsmerkmale des Kartenkörpers prüfen können, müssen demzufolge also über die entsprechenden Sensoren verfügen (siehe IV.2.2).
- Sofern die Kommunikation zwischen Chipkarte und CDLS nicht durch kryptographische Verfahren gegen Abhören und Manipulation gesichert wird, ist das Abhören der Kommunikation durch mechanische Maßnahmen (sog. Shutter zum Abschneiden aller manipulativ mit der Karte in das CDLS eingebrachten Drähte) zu verhindern.

Als besonders angriffsgefährdet sind CDLS vom Typ "PC mit Kartenterminal" anzusehen, sofern sie nicht in manipulationsgeschützten Umgebungen eingesetzt werden. Erhöhte Schutzfunktionen werden hier als notwendig angesehen. Die bisherigen Spezifikationen für die CDLS lassen nicht erkennen, daß Maßnahmen gegen Penetrationsversuche aus der IT-Umgebung der Chipkartenanwendung im CDLS ergriffen werden können. Es fehlt daher an einem schlüssigen Sicherheitskonzept für das Zusammenspiel zwischen dem Betriebssystem und den Applikationen der (übergeordneten) IT-Umgebung und dem Betriebssystem und den Applikationen des Systems Chipkarte/CDLS.

Abkürzungsverzeichnis

CDLS	Chipkartenbasiertes-Dienstleistungssystem
CPU	Central Processing Unit (Zentraleinheit)
DES	Symmetrischer Verschlüsselungsalgorithmus (Data Encryption Standard)
DF	Dedicated File
DSS	Signieralgorithmus (Digital Signature Standard)
EEPROM	Electrically Erasable.Programmable Read Only Memory (elektrisch löschbarer, programmierbarer Festwertspeicher)
EF	Elementary File
EPROM	Erasable Programmable Read Only Memory (löschbarer, programmierbarer Festwertspeicher)
IDEA	Symmetrischer Verschlüsselungsalgorithmus
IEC	International Electrotechnical Commission
ISO	International Standardisation Organisation
IT	Informationstechnik
KB	Kilobyte

KT	Kartenterminal
KVK	Krankenversichertenkarte
MAC	Message Authentication Code
MB	Megabyte
MF	Masterfile
PC	Personal Computer
PIN	Persönliche Identifikations-Nummer
PUK	Personal Unblocking Key
RAM	Random Access Memory (Direktzugriffsspeicher)
RipeMD160	Hash-Algorithmus
ROM	Read Only Memory (Festwertspeicher)
RSA	Asymmetrischer Verschlüsselungsalgorithmus (Rivest-Shamir-Adleman)
SC 85	Symmetrischer Verschlüsselungsalgorithmus
SGB V	Sozialgesetzbuch V (Gesetzliche Krankenversicherung)
SHA	Secure Hash-Algorithmus

16 Materialien

16.1 Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 9. Mai 1996 zu Forderungen zur sicheren Übertragung elektronisch gespeicherter personenbezogener Daten

Der Schutz personenbezogener Daten ist während der Übertragung oder anderer Formen des Transportes nicht immer gewährleistet. Elektronisch gespeicherte, personenbezogene Daten können sowohl auf leitungsgebundenen oder drahtlosen Übertragungswegen als auch auf maschinell lesbaren Datenträgern weitergegeben werden. Oft sind die Eigenschaften des Transportweges dem Absender und dem Empfänger weder bekannt noch durch sie beeinflußbar. Vor allem die Vertraulichkeit, die Integrität (Unversehrtheit) und die Zurechenbarkeit der Daten (Authentizität) sind nicht sichergestellt, solange Manipulationen, unbefugte Kenntnisnahme und Fehler während des Transportes nicht ausgeschlossen werden können. Die Verletzung der Vertraulichkeit ist möglich, ohne daß Spuren hinterlassen werden.

Zahlreiche Rechtsvorschriften gebieten, das Grundrecht auf informationelle Selbstbestimmung auch während der automatisierten Verarbeitung personenbezogener Daten zu sichern (z. B. § 78 a SGB X mit Anlage, § 10 Abs. 8 Btx-Staatsvertrag, § 9 BDSG nebst Anlage und entsprechende landesgesetzliche Regelungen).

Kryptographische Verfahren (z. B. symmetrische und asymmetrische Verschlüsselung, digitale Signatur) sind besonders geeignet, um Verletzungen des Datenschutzes beim Transport schutzwürdiger elektronisch gespeicherter Daten zu verhindern. Mit ihrer Hilfe lassen sich Manipulationen und Übertragungsfehler nachweisen und die unberechtigte Kenntnisnahme verhindern. Derartige Verfahren sind heute Stand der Technik und können in vielen Anwendungsfällen mit vertretbarem Aufwand eingesetzt werden.

Angesichts der beschriebenen Situation und der vorhandenen technischen Möglichkeiten fordern die Datenschutzbeauftragten des Bundes und der Länder, geeignete, sichere kryptographische Verfahren beim Transport elektronisch gespeicherter personenbezogener Daten unter Berücksichtigung ihrer Schutzwürdigkeit anzuwenden.

16.2 Entschließungen der 52. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 22./23. Oktober 1996 in Hamburg

16.2.1 Zum Datenschutz bei der Vermittlung und Abrechnung digitaler Fernsehsendungen

Mit der Markteinführung des digitalen Fernsehens eröffnen sich für die Anbieter - neben einem deutlich ausgeweiteten Programmvolumen - neue Möglichkeiten für die

Vermittlung und Abrechnung von Sendungen. Hinzuweisen ist in erster Linie auf Systeme, bei denen die Kunden für die einzelnen empfangenen Sendungen bezahlen müssen. Dort entsteht die Gefahr, daß die individuellen Vorlieben, Interessen und Sehgewohnheiten registriert und damit Mediennutzungsprofile einzelner Zuschauer erstellt werden. Die zur Vermittlung und zur Abrechnung verfügbaren technischen Verfahren können die Privatsphäre des Zuschauers in unterschiedlicher Weise beeinträchtigen.

Die Datenschutzbeauftragten des Bundes und der Länder fordern die Anbieter und Programmlieferanten auf, den Nutzern zumindest alternativ auch solche Lösungen anzubieten, bei denen die Nutzung der einzelnen Programmangebote nicht personenbezogen registriert werden kann, wie es der Entwurf des Mediendienste-Staatsvertrages bereits vorsieht. Die technischen Voraussetzungen für derartige Lösungen sind gegeben.

Die technischen Verfahren sind so zu gestalten, daß möglichst keine personenbezogenen Daten erhoben, gespeichert und verarbeitet werden (Prinzip der Datensparsamkeit). Verfahren, die im voraus bezahlte Wertkarten - Chipkarten - nutzen, um die mit entsprechenden Entgeltinformationen ausgestrahlten Sendungen zu empfangen und zu entschlüsseln, entsprechen weitgehend dieser Forderung. Allerdings setzt eine anonyme Nutzung voraus, daß beim Zuschauer gespeicherte Informationen über die gesehenen Sendungen nicht durch den Anbieter abgerufen werden können.

Die Datenschutzbeauftragten sprechen sich außerdem dafür aus, daß für die Verfahren auf europäischer Ebene Vorgaben für eine einheitliche Architektur mit gleichwertigen Datenschutzvorkehrungen entwickelt werden.

16.2.2 Zu Eingriffsbefugnissen zur Strafverfolgung im Informations- und Telekommunikations-bereich

Die Entwicklung moderner Informations- und Telekommunikationstechniken führt zu einem grundlegend veränderten Kommunikationsverhalten der Bürger.

Die Privatisierung der Netze und die weite Verbreitung des Mobilfunks geht einher mit einer weitreichenden Digitalisierung der Kommunikation. Mailboxen und das Internet prägen die Informationsgewinnung und -verbreitung von Privatleuten, von Unternehmen und öffentlichen Institutionen gleichermaßen.

Neue Dienste wie Tele-Working, Tele-Banking, Tele-Shopping, digitale Videodienste und Rundfunk im Internet sind einfach überwachbar, weil personenbezogene Daten der Nutzer in digitaler Form vorliegen. Die herkömmlichen Befugnisse zur Überwachung des Fernmeldeverkehrs erhalten eine neue Dimension; weil immer mehr personenbezogene Daten elektronisch übertragen und gespeichert werden, können sie mit geringem Aufwand kontrolliert und ausgewertet werden. Dem gegenüber stehen

jedoch auch Gefahren durch die Nutzung der neuen Technik zu kriminellen Zwecken. Die Datenschutzbeauftragten erkennen an, daß die Strafverfolgungsbehörden in die Lage versetzt werden müssen, solchen mißbräuchlichen Nutzungen der neuen Techniken zu kriminellen Zwecken wirksam zu begegnen.

Sie betonen jedoch, daß die herkömmlichen weitreichenden Eingriffsbefugnisse auch unter wesentlich veränderten Bedingungen nicht einfach auf die neuen Formen der Individual- und Massenkommunikation übertragen werden können. Die zum Schutz der Persönlichkeitsrechte des einzelnen gezogenen Grenzen müssen auch unter den geänderten tatsächlichen Bedingungen der Verwendung der modernen Informationstechnologien aufrechterhalten und gewährleistet werden. Eine Wahrheitsfindung um jeden Preis darf es auch insoweit nicht geben. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat daher Thesen zur Bewältigung dieses Spannungsverhältnisses entwickelt.

Sie hebt insbesondere den Grundsatz der spurenlosen Kommunikation hervor. Kommunikationssysteme müssen mit personenbezogenen Daten möglichst sparsam umgehen. Daher verdienen solche Systeme und Technologien Vorrang, die keine oder möglichst wenige Daten zum Betrieb benötigen. Ein positives Beispiel ist die Telefonkarte, deren Nutzung keine personenbezogenen Daten hinterläßt und die deshalb für andere Bereiche als Vorbild angesehen werden kann. Daten allein zu dem Zweck einer künftig denkbaren Strafverfolgung bereitzuhalten ist unzulässig.

Bei digitalen Kommunikationsformen läßt sich anhand der Bestands- und Verbindungsdaten nachvollziehen, wer wann mit wem kommuniziert hat, wer welches Medium genutzt hat und damit wer welchen weltanschaulichen, religiösen und sonstigen persönlichen Interessen und Neigungen nachgeht. Eine staatliche Überwachung dieser Vorgänge greift tief in das Persönlichkeitsrecht der Betroffenen ein und berührt auf empfindliche Weise die Informationsfreiheit und den Schutz besonderer Vertrauensverhältnisse (z. B. Arztgeheimnis, anwaltliches Vertrauensverhältnis). Die Datenschutzbeauftragten fordern daher, daß der Gesetzgeber diesen Gesichtspunkten Rechnung trägt.

Die Datenschutzbeauftragten wenden sich nachhaltig dagegen, daß den Nutzern die Verschlüsselung des Inhalts ihrer Nachrichten verboten wird. Die Möglichkeit für den Bürger, seine Kommunikation durch geeignete Maßnahmen vor unberechtigten Zugriffen zu schützen, ist ein traditionelles verfassungsrechtlich verbürgtes Recht.

Aus Sicht des Datenschutzes besteht andererseits durchaus Verständnis für das Interesse der Sicherheits- und Strafverfolgungsbehörden, sich rechtlich zulässige Zugriffsmöglichkeiten nicht dadurch versperren zu lassen, daß Verschlüsselungen verwandt werden, zu denen sie keinen Zugriff haben. Eine Reglementierung der Verschlüsselung, z. B. durch Schlüsselhinterlegung, erscheint aber aus derzeitiger technischer Sicht kaum durchsetzbar, da entsprechende staatliche Maßnahmen - insbesondere im weltweiten Datenverkehr - ohnehin leicht zu umgehen und kaum

kontrollierbar wären.

16.2.3 Zur automatisierten Übermittlung von Abrechnungsdaten durch Kassenzahnärztliche Vereinigungen an gesetzliche Krankenkassen

Der in dem Schiedsspruch vom 20. Februar 1995 für die Abrechnung festgelegte Umfang der Datenübermittlung zwischen Kassenzahnärztlichen Vereinigungen und gesetzlichen Krankenkassen erfüllt nicht die Anforderungen des Sozialgesetzbuches an diesen Datenaustausch. § 295 SGB V fordert, daß Daten nur *im erforderlichen Umfang* und *nicht versichertenbezogen* übermittelt werden dürfen.

Die Datenschutzbeauftragten begrüßen es deshalb, daß der größte Teil der gesetzlichen Krankenkassen in "Protokollnotizen" - Stand 22. März 1996 - den Umfang der zu übermittelnden Daten reduziert hat. Das Risiko der Identifizierbarkeit des Versicherten wurde dadurch deutlich verringert. Zum letztlich erforderlichen Umfang haben die Spitzenverbände der gesetzlichen Krankenkassen erklärt, daß genauere Begründungen für die Erforderlichkeit der Daten erst gegeben werden könnten, wenn das DV-Projekt für das Abrechnungsverfahren auf Kassenseite weit genug entwickelt sei.

Der Verband der Angestellten-Ersatzkassen (VdAK) hat bisher als einziger Spitzenverband der gesetzlichen Krankenkassen diese Datenreduzierungen nicht mitgetragen. Die Datenschutzbeauftragten fordern den VdAK auf, sich für die Frage der Datenübermittlung zwischen Kassenzahnärztlichen Vereinigungen und gesetzlichen Krankenkassen der einheitlichen Linie anzuschließen. Dies liegt im gesetzlich geschützten Interesse der Versicherten.

Die besonderen Vorgaben des Sozialgesetzbuches für die Prüfung der Wirtschaftlichkeit der ärztlichen Abrechnung werden dadurch nicht berührt.

16.3 Entschließungen der 53. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 17./18. April 1997 in München

16.3.1 Zu Beratungen zum StVÄG 1996

Die Datenschutzbeauftragten des Bundes und der Länder wenden sich entschieden gegen die Entwicklung, im Gesetzgebungsverfahren zu einem Strafverfahrensänderungsgesetz 1996, die Gewährleistung der informationellen Selbstbestimmung im Strafverfahren nicht nur nicht zu verbessern, sondern vielmehr bestehende Rechte sogar noch zu beschränken. Dies gilt insbesondere für den Beschluß des Bundesrates, der gravierende datenschutzrechtliche Verschlechterungen vorsieht.

Bereits der Gesetzentwurf der Bundesregierung wird in Teilbereichen den Vorgaben des Bundesverfassungsgerichts nicht gerecht und fällt teilweise hinter den bereits

erreichten Standard der allgemeinen Datenschutzgesetze und anderer bereichsspezifischer Regelungen (wie z. B. dem Bundeszentralregistergesetz und den Polizeigesetzen der Länder) zurück.

Kritik erheben die Datenschutzbeauftragten des Bundes und der Länder insbesondere an folgenden Punkten:

- Die Voraussetzungen für Maßnahmen der Öffentlichkeitsfahndung sind nicht hinreichend bestimmt. So wird z. B. nicht angemessen zwischen Beschuldigten und Zeugen differenziert.
- Für Privatpersonen und Stellen, die nicht Verfahrensbeteiligte sind, wird als Voraussetzung zur Auskunfts- und Akteneinsicht lediglich ein vages "berechtigtes" statt eines rechtlichen Interesses gefordert.
- Die Regelungen über den Inhalt, Ausmaß und Umfang von Dateien und Informationssystemen mit personenbezogenen Daten bei Staatsanwaltschaften sind unzureichend. Das hat zur Folge, daß nahezu unbeschränkt Zentraldateien oder gemeinsame Dateien eingerichtet und Daten ohne Berücksichtigung der Begehungsweise und Schwere von Straftaten gespeichert werden können. Die Zugriffsmöglichkeiten der Strafverfolgungs- und Strafjustizbehörden auf diese Daten gehen zu weit. Darüber hinaus werden Standardmaßnahmen des technischen und organisatorischen Datenschutzes (z. B. Protokollierung, interne Zugriffsbeschränkungen etc.) weitgehend abgeschwächt.

Die Bedenken und Empfehlungen der Datenschutzbeauftragten des Bundes und der Länder fanden in den ersten Beratungen des Bundesrates zum Gesetzentwurf nahezu keinen Niederschlag.

Darüber hinaus hat der Bundesrat in seiner Stellungnahme weitergehende datenschutzrechtliche Verschlechterungen beschlossen, die vor allem die Entfernung mehrerer im Gesetzentwurf noch vorhandener Beschränkungen und verfahrensrechtlicher Sicherungen zum Schutz des Persönlichkeitsrechts und des Rechtes auf informationelle Selbstbestimmung der Betroffenen zum Inhalt haben.

Beispiele hierfür sind:

- Der Richtervorbehalt für die Anordnung der Öffentlichkeitsfahndung und der längerfristigen Observation soll gestrichen werden.
- Die Verwendungsbeschränkungen bei Daten, die mit besonderen Erhebungsmethoden nach dem Polizeirecht gewonnen wurden, sollen herausgenommen werden.
- Das Auskunfts- und Akteneinsichtsrecht auch für öffentliche Stellen soll erheblich erweitert werden.
- Detaillierte Regelungen für Fälle, in denen personenbezogene Daten von Amts wegen durch Strafverfolgungs- und Strafjustizbehörden an andere Stellen übermittelt werden dürfen, die im weitesten Sinne mit der Strafrechtspflege zu tun haben, sollen gestrichen werden.
- Das Verbot soll gestrichen werden, über die Grunddaten hinausgehende weitere

Angaben nach Freispruch, endgültiger Verfahrenseinstellung oder unanfechtbarer Ablehnung der Eröffnung des Hauptverfahrens Daten in Dateien zu speichern.
- Speicherungs- und Löschungsfristen für personenbezogene Daten in Dateien sollen ersatzlos gestrichen werden.
- Kontrollverfahren für automatisierte Abrufverfahren sollen aufgehoben werden und die Verwendungsbeschränkungen für Protokolldaten sollen entfallen.

Die Datenschutzbeauftragten des Bundes und der Länder fordern die Bundesregierung und den Deutschen Bundestag auf, bei den anstehenden weiteren Beratungen des Gesetzentwurfes die vom Bundesrat empfohlenen datenschutzrechtlichen Verschlechterungen nicht zu übernehmen und die noch bestehenden datenschutzrechtlichen Mängel zu beseitigen.

Hingegen sollten Vorschläge des Bundesrates für Regelungen für den Einsatz von Lichtbildvorlagen und für die Datenverarbeitung zur Durchführung des Täter-Opfer-Ausgleichs aufgegriffen werden.

16.3.2 Zu genetischen Informationen in Datenbanken der Polizei für erkennungsdienstliche Zwecke

Immer häufiger wird bei der Verfolgung von Straftaten am Tatort oder beim Opfer festgestelltes sog. biologisches Material als Spurenmaterial durch die Polizei sichergestellt, mittels DNA-Analyse untersucht und mit anderen DNA-Materialien verglichen. Die DNA-Analyse ist zur Standardmethode geworden, um die Herkunft von Spurenmaterial von bestimmten bekannten Personen (Verdächtigen, Opfern, unbeteiligten Dritten) oder die Identität mit anderem Spurenmaterial unbekannter Personen feststellen zu können.

Der Gesetzgeber hat zwar vor kurzem im Strafverfahrensänderungsgesetz-DNA-Analyse ("Genetischer Fingerabdruck") die Voraussetzungen und Grenzen genetischer Untersuchungen im Strafverfahren geregelt. Eine Festlegung, ob und in welchen Grenzen die Speicherung und Nutzung der durch eine DNA-Analyse gewonnenen Untersuchungsergebnisse in Datenbanken der Polizei zu erkennungsdienstlichen Zwecken zulässig ist, enthält dieses Gesetz jedoch nicht.

Bezüglich des Aussagegehalts der gespeicherten Daten der Analyseergebnisse ist ein grundsätzlich neuer Aspekt zu berücksichtigen:
Die automatisiert gespeicherten Informationen aus DNA-Merkmalen, die zum Zweck der Identitätsfeststellung erstellt worden sind, ermöglichen derzeit tatsächlich zwar keine über die Identifizierung hinausgehenden Aussagen zur jeweiligen Person oder deren Erbgut. In Einzelfällen können die analysierten nicht-codierenden persönlichkeitsneutralen DNA-Merkmale jedoch mit codierenden Merkmalen korrespondieren. In Anbetracht der weltweiten intensiven Forschung im Bereich der Genom-Analyse ist es nicht ausgeschlossen, daß künftig auch auf der Basis der Untersuchung von bisher als nicht-codierend angesehenen Merkmalen konkrete

Aussagen über genetische Dispositionen der betroffenen Personen mit inhaltlichem Informationswert getroffen werden können. Dieses Risiko ist deshalb nicht zu vernachlässigen, weil gegenwärtig weltweit mit erheblichem Aufwand die Entschlüsselung des gesamten menschlichen Genoms vorangetrieben wird.

Dieser Gefährdung kann dadurch begegnet werden, daß bei Bekanntwerden von Überschußinformationen durch die bisherigen Untersuchungsmethoden andere Untersuchungsmethoden (Analyse eines anderen Genomabschnitts) verwendet werden, die keine Informationen über die genetische Disposition liefern. Derartige Ausweichstrategien können jedoch zur Folge haben, daß die mit anderen Methoden erlangten Untersuchungsergebnisse nicht mit bereits vorliegenden vergleichbar sind. Datenspeicherungen über verformelte Untersuchungsergebnisse könnten daher dazu führen, daß einmal verwendete Untersuchungsformen im Interesse der Vergleichbarkeit beibehalten werden, obwohl sie sich als problematisch herausgestellt haben und unproblematische Alternativen zur Verfügung stehen, z. B. durch Verschlüsselung problematischer Informationen.

In Anbetracht dieser Situation und angesichts der Tendenz, mittels DNA-Analyse gewonnene Daten nicht nur in einem bestimmten Strafverfahren zu verwenden, sondern diese Daten in abrufbaren Datenbanken auch für andere Strafverfahren zugänglich zu machen, fordern die Datenschutzbeauftragten des Bundes und der Länder ergänzend zu §§ 81 e und f StPO für die automatisierte Speicherung und Nutzung von DNA-Identitätsdaten eine spezielle gesetzliche Regelung in der Strafprozeßordnung, um das Persönlichkeitsrecht der Betroffenen zu schützen:

1. Es muß ein grundsätzliches Verbot der Verformelung und Speicherung solcher Analyseergebnisse statuiert werden, die inhaltliche Aussagen über Erbanlagen ermöglichen.

   Im Hinblick auf die nicht auszuschließende Möglichkeit künftiger Rückschlüsse auf genetische Dispositionen ist bereits jetzt ein striktes Nutzungsverbot für persönlichkeitsrelevante Erkenntnisse zu statuieren, die aus den gespeicherten Verformelungen der DNA resultieren.

2. Wenn zum Zweck des Abgleichs mit Daten aus anderen Verfahren (also zu erkennungsdienstlichen Zwecken) DNA-Informationen automatisiert gespeichert werden sollen (DNA-Datenbank mit der Funktion, die bei Fingerabdrücken die AFIS-Datenbank des BKA besitzt), müssen darüber hinaus folgende Regelungen geschaffen werden:

   - Nicht jede DNA-Analyse, die zum Zweck der Aufklärung einer konkreten Straftat erfolgt ist, darf in diese Datei aufgenommen werden. Die Speicherung von Verformelungen der DNA-Struktur in eine Datenbank darf nur dann erfolgen, wenn tatsächliche Anhaltspunkte dafür vorliegen, daß der Beschuldigte künftig strafrechtlich in Erscheinung treten wird und daß die Speicherung aufgrund einer

Prognose unter Zugrundelegung des bisherigen Täterverhaltens die künftige Strafverfolgung fördern kann.

- Eine Speicherung kommt insbesondere dann nicht in Betracht, wenn der Tatverdacht gegen den Beschuldigten ausgeräumt wurde. Bereits erfolgte Speicherungen sind zu löschen. Gleiches gilt für den Fall, daß die Anordnung der DNA-Untersuchung oder die Art und Weise ihrer Durchführung unzulässig war.

- Die Aufbewahrungsdauer von Verformelungen der DNA-Struktur ist konkret festzulegen (z. B. gestaffelt nach der Schwere des Tatvorwurfs).

3. Voraussetzung für Gen-Analysen muß in jedem Fall mindestens die richterliche Anordnung sein, unabhängig davon, ob die Daten in einem anhängigen Strafverfahren zum Zweck der Straftatenaufklärung, wie in § 81 f Absatz 1 Satz 1 StPO normiert, oder ob sie zum Zweck der künftigen Strafverfolgung (also zu Zwecken des Erkennungsdienstes) benötigt werden.

4. Ein DNA-Screening von Personengruppen, deren Zusammensetzung nach abstrakt festgelegten Kriterien ohne konkreten Tatverdacht gegenüber einzelnen erfolgt, führt im Regelfall zur Erhebung von DNA-Daten zahlreicher völlig unbeteiligter und unschuldiger Bürger. Die Daten dieser Personen sind unmittelbar dann zu löschen, wenn sie für das Anlaßstrafverfahren nicht mehr erforderlich sind. Sie dürfen nicht in verfahrensübergreifenden DNA-Dateien gespeichert werden und auch nicht mit solchen Datenbeständen abgeglichen werden.

16.3.3 Zur geplanten Verpflichtung von Teledienstanbietern, Kundendaten an Sicherheitsbehörden zu übermitteln

Der Entwurf der Bundesregierung für ein Teledienstdatenschutzgesetz (Artikel 2 [§ 5 Absatz 3] des Informations- und Kommunikationsdienste-Gesetzes vom 20.12.1996 - BR-Drs. 966/96) sieht vor, daß die Anbieter von Telediensten (z. B. Home-Banking, Home-Shopping) dazu verpflichtet werden sollen, insbesondere der Polizei und den Nachrichtendiensten Auskunft über Daten zur Begründung, inhaltlichen Ausgestaltung oder Änderung der Vertragsverhältnisse mit ihren Kunden (sog. Bestandsdaten) zu erteilen.

Die Datenschutzbeauftragten des Bundes und der Länder wenden sich entschieden gegen die Aufnahme einer solchen Übermittlungsvorschrift in das Teledienstdatenschutzgesetz des Bundes. Eine Folge dieser Vorschrift wäre, daß Anbieter von elektronischen Informationsdiensten (z. B. Diskussionsforen) offenlegen müßten, welche ihrer Kunden welche Dienste z. B. mit einer bestimmten politischen Tendenz in Anspruch nehmen. Darin läge ein massiver Eingriff nicht nur in das Recht auf informationelle Selbstbestimmung, sondern auch in die Informations- und Meinungsfreiheit des Einzelnen. Das geltende Recht, insbesondere die Strafprozeßordnung und das Polizeirecht enthalten hinreichende Möglichkeiten, um

strafbaren und gefährlichen Handlungen auch im Bereich der Teledienste zu begegnen. Über die bisherige Rechtslage hinaus würde bei Verabschiedung der geplanten Regelung zudem den Nachrichtendiensten ein nichtöffentlicher Datenbestand offenstehen. In keinem anderen Wirtschaftsbereich sind vergleichbare Übermittlungspflichten der Anbieter von Gütern und Dienstleistungen hinsichtlich ihrer Kunden bekannt.

Mit guten Gründen haben deshalb die Länder davon abgesehen, in den inzwischen von den Ministerpräsidenten unterzeichneten Staatsvertrag über Mediendienste eine vergleichbare Vorschrift aufzunehmen. In der Praxis werden sich aber für Bürger und Online-Dienstanbieter schwierige Fragen der Abgrenzung zwischen den Geltungsbereichen des Mediendienste-Staatsvertrags und des Teledienstedatenschutzgesetzes ergeben. Auch aus diesem Grund halten die Datenschutzbeauftragten eine Streichung der Vorschrift des § 5 Absatz 3 aus dem Entwurf für ein Teledienstedatenschutzgesetz für geboten.

16.3.4 Zur Achtung der Menschenrechte in der Europäischen Union

Die DSB-Konferenz ist gemeinsam der Überzeugung, daß hinsichtlich nicht Verdächtiger und hinsichtlich nicht kriminalitätsbezogener Daten die Forderung des Europäischen Parlaments vom 17. September 1996 zu den Dateien von EUROPOL unterstützt werden soll.

Das Europäische Parlament hat in seiner Entschließung zur Achtung der Menschenrechte gefordert, "alle Informationen persönlichen Charakters, wie Angaben zur Religionszugehörigkeit, zu philosophischen oder religiösen Überzeugungen, Rasse, Gesundheit und sexuellen Gewohnheiten, von der Erfassung in Datenbanken von EUROPOL auszuschließen".

16.3.5 Zur Sicherstellung des Schutzes medizinischer Datenbestände außerhalb von ärztlichen Behandlungseinrichtungen

Die Datenschutzbeauftragten des Bundes und der Länder halten es für sehr problematisch, daß infolge technischer und gesellschaftlicher Veränderungen in einer zunehmenden Anzahl von Konstellationen personenbezogene medizinische Patientendaten außerhalb des ärztlichen Bereiches verarbeitet werden. Sie fordern, daß zunehmend die Möglichkeiten einer anonymen oder pseudonymen Datenverarbeitung mit Verschlüsselung genutzt werden. Soweit dennoch Patientendaten personenbezogen weitergegeben werden, ist ein wesentliches Problem, daß außerhalb des ärztlichen Gewahrsams der von der Strafprozeßordnung vorgesehene Schutz personenbezogener Patientendaten vor Inanspruchnahme als Beweismittel durch Zeugeneinvernahme oder Beschlagnahme nicht mehr zweifelsfrei sichergestellt ist bzw. überhaupt nicht existiert.

Die folgenden Beispiele machen dies deutlich:

1. Ärzte bzw. Krankenhäuser haben z. B. keinen Gewahrsam an den personenbezogenen Patientendaten, die der Patient auf einer (freiwilligen) Patientenchipkarte bei sich trägt/besitzt oder die von einer dritten Stelle außerhalb des ärztlichen Bereichs im Auftrag verarbeitet werden, wie z. B. bei Mailbox-Systemen, externer Archivierung oder der Vergabe von Schreibarbeiten an selbständige Schreibbüros.

   Fraglich ist auch die Aufrechterhaltung des ärztlichen Gewahrsams, wenn Hilfspersonal des Arztes oder Krankenhauses Patientendaten in der Privatwohnung bearbeitet.

2. Zunehmend werden einzelne Unternehmensfunktionen bzw. fachliche Aufgaben ausgelagert und einer externen Stelle - in der Regel einem Privatunternehmen - übertragen (sog. Outsourcing), z. B. bei Einschaltung eines externen Inkassounternehmens, bei externem Catering für stationäre Patienten, bei externer Archivierung oder bei Vergabe von Organisationsanalysen an externe Beratergesellschaften.

3. Medizinische Daten mit Patientenbezug sollen an Forscher oder Forschungsinstitute zu Zwecken wissenschaftlicher Forschung übermittelt werden. Je umfassender und komplizierter der Einsatz automatisierter Datenverarbeitung für Forschungszwecke vorgesehen wird, desto weniger werden die personenbezogenen Patientendaten ausschließlich durch ärztliches Personal verarbeitet. Hier setzt sich vielmehr die Verarbeitung durch Informatiker und Statistiker immer mehr durch. Aber auch bei Verarbeitung durch Ärzte, die in der Forschung tätig sind, ist keineswegs sichergestellt, daß die personenbezogenen Patientendaten diesen Ärzten "in ihrer Eigenschaft als Arzt" bekannt geworden sind, wie dies durch die Strafprozeßordnung für den Beschlagnahmeschutz als Voraussetzung festgelegt ist.

Die zunehmende Verlagerung personenbezogener Patientendaten aus dem Schutzbereich des Arztgeheimnisses nach außen verstößt nach Ansicht der Datenschutzbeauftragten massiv gegen Interessen der betroffenen Patienten, solange nicht ein gleichwertiger Schutz gewährleistet ist.

Die Datenschutzbeauftragten des Bundes und der Länder bitten daher den Bundesgesetzgeber - unabhängig von weiteren Fragen des Datenschutzes, die mit der Verarbeitung medizinischer Daten im Rahmen der Telemedizin verbunden sein können - für die sich zunehmend entwickelnden modernen Formen der Auslagerung medizinischer Patientendaten sowie für die Weitergabe medizinischer Patientendaten für Zwecke wissenschaftlicher medizinischer Forschung einen dem Arztgeheimnis entsprechenden Schutz der Patientendaten zu schaffen.