Sächsischer Landtag
2. Wahlperiode

DRUCKSACHE 2/11359

Schutz des Persönlichkeitsrechts im öffentlichen Bereich

7. Tätigkeitsbericht

des

Sächsischen Datenschutzbeauftragten

Dem Sächsischen Landtag

vorgelegt zum 31. März 1999

gemäß § 27 des Sächsischen Datenschutzgesetzes

Eingegangen am: 27. Mai 1999 Ausgegeben am: 28. Mai 1999

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 bisher gegen den Duden - schreibe ich den „Einzelnen“ groß. Dies betont seine Individualität, nie den Individualismus. Neuerdings habe ich die reformierte Rechtschreibung in diesem Punkt auf meiner Seite.

Herausgeber: Der Sächsische Datenschutzbeauftragte
Dr. Thomas Giesen
Holländische Str. 2 Postfach 120905
01067 Dresden 01008 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 nichtamtlichen Abkürzung*, ersatzweise der *amtlichen Kurzbezeichnung* aufgeführt.
Die genaue Fundstelle und Angabe der letzten Änderung sind bei bekannteren Bundesgesetzen (die in den gängigen Gesetzessammlungen leicht zu finden sind) weggelassen worden.

AAÜG	Gesetz zur Überführung der Ansprüche und Anwartschaften aus Zusatz- und Sonderversorgungssystemen des Beitrittsgebiets (Anspruchs- und Anwartschaftsüberführungsgesetz) vom 25. Juli 1991 (BGBl. I S. 1606), zuletzt geändert durch Art. 7 des Gesetzes vom 11. November 1996 (BGBl. I S. 1674)
AO	Abgabenordnung
BArchG	Gesetz über die Sicherung und Nutzung von Archivgut des Bundes (Bundesarchivgesetz) vom 6. Januar 1988 (BGBl. I S. 62), zuletzt geändert durch das Gesetz zur Änderung des Bundesarchivgesetzes vom 13. März 1992 (BGBl. I S. 506)
BAT(-O)	Erster Tarifvertrag zur Anpassung des Tarifrechts - Manteltarifliche Vorschriften (BAT-O) vom 10. Dezember 1990 (SächsABl. 1991 Nr. 10 S. 1), zuletzt geändert durch Änderungstarifvertrag Nr. 9 vom 5. Mai 1998 (GVBl. S. 162)
BauGB	Baugesetzbuch
BBesG	Bundesbesoldungsgesetz
BBiG	Berufsbildungsgesetz
BDO	Bundesdisziplinarordnung
BDSG	Gesetz zur Fortentwicklung der Datenverarbeitung und des Datenschutzes (Bundesdatenschutzgesetz)
BerRehaG	Gesetz über den Ausgleich beruflicher Benachteiligungen für Opfer politischer Verfolgung im Beitrittsgebiet (Berufliches Rehabilitierungsgesetz) vom 23. Juni 1994 (BGBl. I S. 1311, 1314), in der Neufassung vom 1. Juli 1997 (BGBl. I S. 1625)

BRAO	Bundesrechtsanwaltsordnung vom 1. August 1959 (BGBl. I S. 565), zuletzt geändert durch Art. 1 Nr. 2 des Gesetzes vom 19. Dezember 1998 (BGBl. I S. 3836; 1999 I S. 194)
BRRG	Beamtenrechtsrahmengesetz
BSHG	Bundessozialhilfegesetz in der Fassung der Bekanntmachung vom 23. März 1994 (BGBl. I S. 646, ber. S. 2975), zuletzt geändert durch Art. 2 des Ersten Gesetzes zur Änderung des Medizinproduktegesetzes vom 6. August 1998 (BGBl. I S. 2005)
BStatG	Gesetz über die Statistik für Bundeszwecke (Bundesstatistikgesetz) vom 22. Januar 1987 (BGBl. I S. 462, 565), zuletzt geändert durch Art. 2 des Gesetzes vom 16. Juni 1998 (BGBl. I S. 1300)
BWG	Bundeswahlgesetz
BWO	Bundeswahlordnung
BZRG	Gesetz über das Zentralregister und das Erziehungsregister (Bundeszentralregistergesetz) in der Fassung der Bekanntmachung vom 21. September 1984 (BGBl. I S. 1229, ber. 1985 S. 195), zuletzt geändert durch Art. 6 des Gesetzes vom 31. August 1998 (BGBl. I S. 2600)
DA	Dienstanweisung für die Standesbeamten und ihre Aufsichtsbehörden vom 23. November 1987 (BAnz. Nr. 227 a) in der Neufassung vom 20. Januar 1999 (BAnz. Nr. 27 a)
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)
EGGVG	Einführungsgesetz zum Gerichtsverfassungsgesetz
EinigVtr	Vertrag zwischen der Bundesrepublik Deutschland und der Deutschen Demokratischen Republik über die Herstellung der Einheit Deutschlands (Einigungsvertrag) vom 31. August 1990 (BGBl. II S. 889)
EU-Datenschutz-Richtlinie	Richtlinie 95/46/EG des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr vom 24. Oktober 1995 (Abl. EG L 281 vom 23. November 1995, S. 31)

FFG	Frauenfördergesetz
GBO	Grundbuchordnung
GBV	Grundbuchverfügung
GeschoSReg	Geschäftsordnung der Sächsischen Staatsregierung vom 27. Juli 1992 (SächsABl. S. 1116), geändert gemäß Bekanntmachung vom 12. November 1993 (SächsABl. S. 1266)
GG	Grundgesetz für die Bundesrepublik Deutschland (Grundgesetz)
HandwO	Gesetz zur Ordnung des Handwerks (Handwerksordnung)
IHK-G	Gesetz zur vorläufigen Regelung des Rechts der Industrie- und Handelskammern vom 18. Dezember 1956 (BGBl. I S. 920), zuletzt geändert durch Gesetz vom 23. Juli 1998 (BGBl. I S. 1887, 3158)
InsO	Insolvenzordnung vom 5. Oktober 1994 (BGBl. I S. 2866), zuletzt geändert durch Art. 2 des Gesetzes vom 19. Dezember 1998 (BGBl. I S. 3836)
JubV	Verordnung über die Gewährung von Jubiläumszuwendungen an Beamte und Richter des Bundes vom 24. Mai 1962 (BGBl I S. 363), zuletzt geändert durch Art. 2 Nr. 1 des Gesetzes vom 20. Dezember 1991 (BGBl. I S. 2317)
JuMiG	Justizmitteilungsgesetz und Gesetz zur Änderung kostenrechtlicher Vorschriften und anderer Gesetze (JuMiG) vom 18. Juni 1997 (BGBl. I S. 1430, 2779), zuletzt geändert durch Art. 25 des Gesetzes vom 16. Dezember 1997 (BGBl. I S. 2970)
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)
KomWG	Gesetz über die Kommunalwahlen im Freistaat Sachsen (Kommunalwahlgesetz - KomWG) vom 18. Oktober 1993 (GVBl. S. 937), zuletzt geändert durch Gesetz vom 10. Dezember 1998 (GVBl. S. 664)
KRG	Gesetz über Krebsregister (Krebsregistergesetz) vom 4. November 1994 (BGBl. I S. 3351)

KunstUrhG	Gesetz betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie vom 9. Januar 1907 (RGBl. S. 7), zuletzt geändert durch Art. 145 des Gesetzes von 2. März 1974 (BGBl. I S. 469)
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)
LWO	Verordnung des Sächsischen Staatsministeriums des Innern über die Durchführung der Wahlen zum Sächsischen Landtag (Landeswahlordnung) vom 11. Februar 1994 (GVBl. S. 369)
MHRG	Gesetz zur Regelung der Miethöhe vom 18. Dezember 1974 (BGBl. I S. 3603, 3604), zuletzt geändert durch Art. 10 des Gesetzes vom 9. Juni 1998 (BGBl. I S. 1242)
MiZi	Anordnungen über Mitteilungen in Zivilsachen in der Neufassung vom 29. April 1998 (BAnz. Nr. 138 a)
MVVO	Erste Verordnung des Sächsischen Staatsministeriums des Innern zur Durchführung des Sächsischen Meldegesetzes (Meldevordruckverordnung) vom 6. September 1993 (GVBl. S. 863)
OWiG	Gesetz über Ordnungswidrigkeiten (Ordnungswidrigkeitengesetz)
PaßG	Paßgesetz vom 19. April 1986 (BGBl. I S. 537), zuletzt geändert durch Art. 7 § 7 Betreuungsgesetz vom 12. September 1990 (BGBl. I S. 2002) und Art. 2 Änderungsgesetz vom 30. Juli 1996 (BGBl. I S. 1182)
PAuswG	Gesetz über Personalausweise in der Fassung der Bekanntmachung vom 21. April 1986 (BGBl. I S. 548), zuletzt geändert durch Art. 1 Änderungsgesetz vom 30. Juli 1996 (BGBl. I S. 1182)
RiStBV	Richtlinien für das Strafverfahren und das Bußgeldverfahren vom 1. Januar 1977, zuletzt geändert am 30. Juni 1998 (SächsJMBl. S. 93)

SächsAGLMBG	Gesetz zur Ausführung des Lebensmittel- und Bedarfsgegenständegesetzes im Freistaat Sachsen vom 31. März 1994 (GVBl. S. 682)
SächsArchivG	Archivgesetz für den Freistaat Sachsen vom 17. Mai 1993 (GVBl. S. 449), zuletzt geändert durch Art. 2 des Gesetzes vom 17. April 1998 (GVBl. S. 151)
SächsBestG	Sächsisches Gesetz über das Friedhofs-, Leichen- und Bestattungswesen (Sächsisches Bestattungsgesetz) vom 8. Juli 1994 (GVBl. S. 1321)
SächsBeurtVO	Verordnung der Sächsischen Staatsregierung über die dienstliche Beurteilung der Beamten vom 21. April 1998 (GVBl. S. 169)
SächsBeurtVO-VwV-SMI	Verwaltungsvorschrift des Sächsischen Staatsministeriums des Innern über die dienstliche Beurteilung der Beamten im Geschäftsbereich des Sächsischen Staatsministeriums des Innern vom 28. Oktober 1998 (SächsABl. S. 813)
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 10. Januar 1997 (GVBl. S. 2)
SächsDO	Disziplinarordnung für den Freistaat Sachsen vom 28. Februar 1994 (GVBl. S. 333), zuletzt geändert durch Art. 3 des Gesetzes vom 16. März 1999 (GVBl. S. 121)
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)
SächsErwStatG	Gesetz über eine repräsentative Statistik der Erwerbssituation im Freistaat Sachsen vom 12. Februar 1999 (GVBl. S. 49)
SächsEigBG	Gesetz über kommunale Eigenbetriebe im Freistaat Sachsen (Sächsisches Eigenbetriebsgesetz) vom 19. April 1994 (GVBl. S. 773)
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)

SächsFrTrSchulG	Gesetz über Schulen in freier Trägerschaft vom 4. Februar 1992 (GVBl. S. 37)
SächsGemO	Gemeindeordnung für den Freistaat Sachsen vom 21. April 1993 (GVBl. S. 301), zuletzt geändert durch Art. 3 des Gesetzes vom 10. Dezember 1998 (GVBl. S. 662)
SächsHfVO	Verordnung des Sächsischen Staatsministeriums des Innern über die Heilfürsorge für Polizeibeamte, Beamte des Landesamtes für Verfassungsschutz und feuerwehrtechnische Beamte (Entwurf)
SäHO	Vorläufige Haushaltsordnung des Freistaates Sachsen vom 19. Dezember 1990 (GVBl. S. 213), zuletzt geändert durch Art. 4 des Gesetzes vom 19. Oktober 1998 (GVBl. S. 505)
SächsKHG	Gesetz zur Neuordnung des Krankenhauswesens (Sächsisches Krankenhausgesetz) vom 19. August 1993 (GVBl. S. 675), zuletzt geändert durch Art. 2 Haushaltbegleitgesetz 1997 vom 12. Dezember 1997 (GVBl. S. 537)
SächsKRGAG	Sächsisches Ausführungsgesetz zum Krebsregistergesetz (Sächsisches Krebsregistergesetz) vom 7. April 1997 (GVBl. S. 352), geändert durch Gesetz vom 6. November 1998 (GVBl. S. 594)
SächsLKrO	Landkreisordnung für den Freistaat Sachsen vom 19. Juli 1993 (GVBl. S. 577), zuletzt geändert durch Gesetz vom 20. Februar 1997 (GVBl. S. 105)
SächsMeldDÜVO	Dritte Verordnung des Sächsischen Staatsministeriums des Innern zur Durchführung des Sächsischen Meldegesetzes (Sächsische Meldedaten-Übermittlungsverordnung) vom 10. September 1997 (GVBl. S. 557)
SächsMG	Sächsisches Meldegesetz vom 21. April 1993 (GVBl. S. 353), in der Fassung der Bekanntmachung vom 11. April 1997 (GVBl. S. 377)
SächsPersVG	Sächsisches Personalvertretungsgesetz vom 21. Januar 1993 (GVBl. S. 29), zuletzt geändert durch Art. 3 des Gesetzes vom 29. Juni 1998 (GVBl. S. 271)
SächsPolG	Polizeigesetz des Freistaates Sachsen in der Fassung der Bekanntmachung vom 15. August 1994 (GVBl. S. 1541)
SächsPsychKG	Sächsisches Gesetz über die Hilfen und die Unterbringung bei psychischen Krankheiten vom 16. Juni 1994 (GVBl. S. 1097)

SächsRettDG	Gesetz über Rettungsdienst, Notfallrettung und Krankentransport für den Freistaat Sachsen vom 7. Januar 1993 (GVBl. S. 9)
SächsStatG	Sächsisches Statistikgesetz vom 17. Mai 1993 (GVBl. S. 453), zuletzt geändert durch Art. 2 des Gesetzes von 12. Februar 1999 (GVBl. S. 49)
SächsVerf	Verfassung des Freistaates Sachsen vom 27. Mai 1992 (GVBl. S. 243)
SächsVertrG	Gesetz zur Regelung der Vertretung des Freistaates Sachsen in gerichtlichen Verfahren vom 20. Februar 1997 (GVBl. S. 108)
SächsVwVG	Sächsisches Verwaltungsvollstreckungsgesetz vom 17. Juli 1992 (GVBl. S. 327), zuletzt geändert durch Gesetz vom 19. Oktober 1998 (GVBl. S. 505)
SächsWahlG	Gesetz über die Wahlen zum Sächsischen Landtag vom 5. August 1993 (GVBl. S. 723), zuletzt geändert durch Art. 1 des Gesetzes zur Änderung des Sächsischen Wahlgesetzes und des Abgeordnetengesetzes vom 12. Januar 1995 (GVBl. S. 1)
SchulG	Schulgesetz für den Freistaat Sachsen vom 3. Juli 1991 (GVBl. S. 213), zuletzt geändert durch Gesetz vom 29. Juni 1998 (GVBl. S. 271)
SGB I	Sozialgesetzbuch - Allgemeiner Teil - vom 11. Dezember 1975 (BGBl. I S. 3015), zuletzt geändert durch Art. 2 des Gesetzes zur Reform der gesetzlichen Rentenversicherung vom 16. Dezember 1997 (BGBl. I S. 2998)
SGB III	Sozialgesetzbuch - Arbeitsförderung - Gesetz zur Reform der Arbeitsförderung (Arbeitsförderungs-Reformgesetz - AFRG) vom 24. März 1997 (BGBl. I S. 594), zuletzt geändert durch Artikel 1 § 4 und Art. 2 des Gesetzes vom 19. Dezember 1998 (BGBl. I S. 3843)
SGB V	Sozialgesetzbuch - Gesetzliche Krankenversicherung - vom 20. Dezember 1988 (BGBl. I S. 2477), zuletzt geändert durch Artikel 9 Nr. 2 des Gesetzes vom 19. Dezember 1998 (BGBl. I S. 3853)
SGB VIII	Sozialgesetzbuch - Kinder- und Jugendhilfe - in der Fassung der Bekanntmachung vom 8. Dezember 1998 (BGBl. I S. 3547)
SGB X	Sozialgesetzbuch - Verwaltungsverfahren - vom 18. August 1980 (BGBl. I S. 1469) und 4. November 1982 (BGBl. I S. 1450), zuletzt geändert durch Artikel 1a des Gesetzes vom 6. August 1998 (BGBl. I S. 2022)

SHG	Gesetz über die Hochschulen im Freistaat Sachsen (Sächsisches Hochschulgesetz) vom 4. August 1993 (GVBl. S. 693), zuletzt geändert durch Artikel 3 des Gesetzes zur Änderung dienstrechtlicher Vorschriften vom 7. April 1997 (GVBl. S. 353)
SOFS	Verordnung des Sächsischen Staatsministeriums für Kultus über Förderschulen im Freistaat Sachsen (Schulordnung Förderschulen) vom 27. März 1996 (GVBl. S. 167)
StGB	Strafgesetzbuch
StPO	Strafprozeßordnung
StVG	Straßenverkehrsgesetz
StVZO	Straßenverkehrs-Zulassungs-Ordnung
UWG	Gesetz gegen den unlauteren Wettbewerb
VertrVO	Verordnung der Sächsischen Staatsregierung über die Vertretung des Freistaates Sachsen in gerichtlichen Verfahren (Vertretungsverordnung) vom 8. April 1997 (GVBl. I S. 358)
VertrZuwG	Gesetz über eine einmalige Zuwendung an die im Beitrittsgebiet lebenden Vertriebenen (Vertriebenenzuwendungsgesetz) vom 27. September 1994 (BGBl. I S. 2624)
VwGO	Verwaltungsgerichtsordnung
VwRehaG	Gesetz über die Aufhebung rechtsstaatswidriger Verwaltungsentscheidungen im Beitrittsgebiet und die daran anknüpfenden Folgeansprüche (Verwaltungsrechtliches Rehabilitierungsgesetz) vom 23. Juni 1994 (BGBl. I S. 1311) in der Neufassung vom 1. Juli 1997 (BGBl. I S. 1620)
VwVAufAus	Verwaltungsvorschrift des Sächsischen Staatsministeriums der Justiz über die Aufbewahrung und Aussonderung von Unterlagen bei den ordentlichen Gerichten, Gerichten für Arbeitssachen, Staatsanwaltschaften und Justizvollzugsanstalten (VwV Aufbewahrung und Aussonderung) vom 12. Juni 1998 (SächsJMBl. S. 80)
VwVfG	Verwaltungsverfahrensgesetz
ZPO	Zivilprozeßordnung
ZuschussVO	Verordnung der Sächsischen Staatsregierung über die Gewährung von Zuschüssen für Schulen in freier Trägerschaft vom 16. Dezember 1997 (GVBl. S. 682)

Sonstiges

ÄndVO	Änderungs-Verordnung
a. E.	am Ende
a. F.	alte Fassung
AfL/ÄfL	Amt/Ämter für Landwirtschaft
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
BfA	Bundesanstalt für Artbeit
BfD	Der Bundesbeauftragte für den Datenschutz
BFH	Bundesfinanzhof
BND	Bundesnachrichtendienst
BGBl.	Bundesgesetzblatt
BGH	Bundesgerichtshof
BGHZ	Amtliche Sammlung der Entscheidungen des Bundesgerichtshofs in Zivilsachen
BHW	Beamtenheimstättenwerk

BKA	Bundeskriminalamt
BKK	Betriebskrankenkasse
BMF	Bundesministerium der Finanzen
BMI	Bundesministerium des Innern
BMJ	Bundesministerium der Justiz
BMJFFG	Bundesministerium für Jugend, Familie, Frauen und Gesundheit [Organisationsstand 1986]
BML	Bundesministerium für Ernährung, Landwirtschaft und Forsten
BMPT	Bundesministerium für Post und Telekommunikation
BMWi	Bundesministerium für Wirtschaft
BSI	Bundesamt für Sicherheit in der Informationstechnik
BStBl.	Bundessteuerblatt
BStU	Der Bundesbeauftragte für die Unterlagen des Staatssicherheitsdienstes der ehemaligen Deutschen Demokratischen Republik
BT-Drs	Bundestags-Drucksache
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 Gemeinschaft
EGN	Einzelgesprächsnachweis
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
GKR	Gemeinsames Krebsregister
GMBl.	Gemeinsames Ministerialblatt, hrsg. vom Bundesministerium des Innern
GVBl.	Sächsisches Gesetz- und Verordnungsblatt
GWZ 1995	Gebäude- und Wohnungszählung 1995
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

KIN-S	Kommunales Informationsnetz - Sachsen
LARoV	Landesamt zur Regelung offener Vermögensfragen
LfF	Landesamt für Finanzen des Freistaates Sachsen
LfV	Landesamt für Verfassungsschutz des Freistaates Sachsen
LG	Landgericht
LKA	Landeskriminalamt Sachsen
LPDK	Lehrpersonaldatenbank
LRA	Landratsamt
LUA	Landesuntersuchungsanstalt für das Gesundheits- und Veterinärwesen
LÜVA	Lebensmittelüberwachungs- und Veterinäramt
MdI	Ministerium des Innern (DDR)
MDR	Mitteldeutscher Rundfunk
MedR	Medizinrecht (Zeitschrift)
MfS	Ministerium für Staatssicherheit
MPU-Stelle	Medizinisch-Psychologische Untersuchungsstelle
NJW	Neue Juristische Wochenschrift
NVwZ	Neue Zeitschrift für Verwaltungsrecht
ÖbV	Öffentlich bestellter Vermessungsingenieur
OFD	Oberfinanzdirektion
OSA	Oberschulamt
OVG	Oberverwaltungsgericht
PersR	Zeitschrift Personalvertretungsrecht
PIN	Personal identification number (Persönliche Identifikationsnummer)

PersV	Die Personalvertretung (Zeitschrift)
RDV	Recht der Datenverarbeitung (Zeitschrift)
RGBl.	Reichsgesetzblatt
RP	Regierungspräsidium
RPA	Rechnungsprüfungsamt
SächsABl.	Sächsisches Amtsblatt
SächsJMBl.	Sächsisches Justizministerialblatt
SAKD	Sächsische Anstalt für Kommunale Datenverarbeitung
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
SMS	Sächsisches Staatsministerium für Soziales, Gesundheit und Familie
SMUL	Sächsisches Staatsministerium für Umwelt und Landwirtschaft
SMWA	Sächsisches Staatsministerium für Wirtschaft und Arbeit
SMWK	Sächsisches Staatsministerium für Wissenschaft und Kunst
SSG	Sächsischer Städte- und Gemeindetag e. V.
StaLA	Statistisches Landesamt
StUFA	Staatliches Umweltfachamt

TB	Tätigkeitsbericht
TCP/IP	Transmission control protocol/Internet protocol
TdL	Tarifgemeinschaft deutscher Länder
THA	Treuhandanstalt
TK-Anlage	Telekommunikationsanlage
TÜV	Technischer Überwachungsverein
VG	Verwaltungsgericht
VIZ	Zeitschrift für Vermögens- und Investitionsrecht
VwV	Verwaltungsvorschift
VZR	Verkehrszentralregister
WWW	World wide web

Verweise im Text auf Ausführungen in früheren Tätigkeitsberichten des Sächsischen Datenschutzbeauftragten sind durch Angabe der Nummer des jeweiligen Tätigkeitsberichtes sowie der jeweiligen Abschnitt-Nr. - getrennt durch einen Schrägstrich - gekennzeichnet (z. B. 4/5.1.2.6).

1 Datenschutz im Freistaat Sachsen

Ich freue mich, dem Sächsischen Landtag nunmehr den 7. Tätigkeitsbericht meiner Behörde vorlegen zu dürfen. Die Siebenzahl ist der Ausdruck für Vielfalt, Vielschichtigkeit, Komplexität. Bei der Abfassung dieses Berichts ist mir wie nie zuvor klargeworden, dass meine Behörde nun doch schon auf langjährige und breite Erfahrungen verweisen kann. Ich danke bei dieser Gelegenheit allen Mitarbeitern der Behörde des Sächsischen Datenschutzbeauftragten für ihren langen Atem, ihren Fleiß und ihr Augenmaß. Diesen Dank haben auch alle im Landtag vertretenen Parteien in der Plenarsitzung vom 17. März 1999 zum Ausdruck gebracht. Zu danken habe ich aber auch dem Präsidenten des Sächsischen Landtages und dessen Verwaltung für tagtägliche Unterstützung und so manchen guten Rat.

Im Berichtsjahr hat der Freistaat Sachsen zur Rechtsfortbildung im deutschen Datenschutzrecht beigetragen. Nachdem eine öffentliche Stelle des Freistaates Sachsen mir Auskünfte im Zusammenhang mit der Aufklärung einer datenschutzrechtlichen Angelegenheit verweigert hatte, habe ich die Gerichte bemüht. Das Sächsische Oberverwaltungsgericht hat letztinstanzlich Folgendes festgestellt:

1. Für Streitigkeiten des Sächsischen Datenschutzbeauftragten gegen ... (eine öffentliche Stelle) wegen Auskunftserteilung ist der Rechtsweg zu den Verwaltungsgerichten gegeben.
2. Bei den dem Sächsischen Datenschutzbeauftragten durch das Sächsische Datenschutzgesetz zugewiesenen Auskunfts- und Einsichtsrechten handelt es sich um eigenständige Rechte des Datenschutzbeauftragten und damit wehrfähige Rechtspositionen im Sinne des § 42 Abs. 2 VwGO. Dies gilt auch dann, wenn der Sächsische Datenschutzbeauftragte den Anspruch gegen eine Behörde des Freistaates Sachsen geltend macht.
3. Der Sächsische Datenschutzbeauftragte hat einen Anspruch darauf, in einem unmittelbaren zeitlichen Zusammenhang mit dem von ihm zu überprüfenden datenschutzrechtlich beachtlichen Vorgang über die zur Wahrnehmung seiner ihm durch das Sächsische Datenschutzgesetz übertragenen Aufgaben erforderlichen Umstände umfassend informiert zu werden.

Dieser Beschluss hat Konsequenzen:
So muss beispielsweise ein sächsischer Landrat, der mir die Einsicht in die von ihm persönlich aufbewahrten Stasi-Unterlagen der Mitarbeiter des Landratsamtes verweigerte, jetzt damit rechnen, dass mein Anspruch gerichtlich durchgesetzt wird, wenn er sich weiterhin weigern würde, mir die notwendige Einsicht in die Akten zu gewähren. Diese Einsicht ist nicht deshalb notwendig, weil ich bewerten möchte, ob jemand für den öffentlichen Dienst geeignet ist, sondern weil ich zu kontrollieren habe, ob mit den Daten ordnungsgemäß im Sinne des Stasi-Unterlagengesetzes aber auch des Sächsischen Datenschutzgesetzes, des Personalvertretungsrechts, des Sächsischen Beamtengesetzes und des Tarifvertrages umgegangen wird.

5 Inneres

5.1 Personalwesen

5.1.1 Änderung der Verwaltungsvorschrift des SMI über die Führung und Verwaltung von Personalakten der Beamten

Im Frühsommer 1998 hat mir das SMI einen Entwurf zur Änderung der Verwaltungsvorschrift über die Führung und Verwaltung von Personalakten der Beamten vom 4. November 1993 übersandt.

Verwaltungsvorschriften sollen die allgemeinen Regelungen eines Gesetzes konkretisieren, um der Verwaltung Entscheidungshilfen an die Hand zu geben und so die zutreffende, zweckmäßige und einheitliche Gesetzesanwendung zu gewährleisten. Diesem Anspruch genügte der Entwurf nicht. Er widersprach teilweise dem Gesetzestext, gab ihn unvollständig oder entstellt wieder, wobei auch der systematische Aufbau nicht immer nachzuvollziehen war. Ich habe den Entwurf in über 70 Punkten kritisiert. Die Mängel sind im Wesentlichen behoben worden.

Auch wenn in einigen Einzelfragen keine Übereinstimmung mit dem SMI erzielt werden konnte, stellt die Verwaltungsvorschrift nun eine brauchbare Grundlage für die personalverwaltenden Stellen dar.

5.1.2 Entwurf der Verwaltungsvorschrift des SMI zur Sächsischen Beurteilungsverordnung

Zum SächsBeurtVO-VwV-SMI-Entwurf habe ich u. a. wie folgt Stellung genommen:

1. *Mitarbeitergespräche*
   Nach § 9 SächsBeurtVO sind Zeitpunkt und inhaltliche Schwerpunkte des Mitarbeitergesprächs *aktenkundig* zu machen. Sowohl die SächsBeurtVO als auch der Entwurf der SächsBeurt-VwV-SMI schweigen sich über die Qualität solcher Aktennotizen aus. Da sich das Mitarbeitergespräch im Vorfeld der eigentlichen Beurteilung auf die dienstlichen Anforderungen, die gezeigten Leistungen und auf Verwendungsmöglichkeiten erstrecken soll, besteht ein unmittelbarer innerer Zusammenhang mit dem Dienstverhältnis (§ 117 Abs. 1 Satz 2 SächsBG) mit der Folge, dass die darüber entstehenden Aufzeichnungen Personalaktenqualität besitzen und nach §§ 117 ff., insbesondere § 119 SächsBG zu behandeln wären. Auf ein Zitat in BVerwGE 62, 140, 141, das meine Ansicht stützt, möchte ich in diesem Zusammenhang hinweisen:

   „Zu den Vorgängen, die in einem inneren Zusammenhang mit dem Beamten- oder Richterverhältnis stehen und deshalb zu den Personalakten genommen werden müssen, gehören hiernach - neben Personalunterlagen und dienstlichen Beurteilungen - nicht nur die Vorgänge, die den Inhalt des Dienstverhältnisses insgesamt oder einzelner aus ihm fließender Rechte und Pflichten bestimmen oder verändern, sondern auch die Unterlagen, die die Art und Weise erhellen, in der die jeweilige Entscheidung vorbereitet worden ist, oder die Aufschluß über die Ge-

sichtspunkte und Erwägungen geben, die für die einzelne das Dienstverhältnis berührende Maßnahme oder dafür, daß sie unterblieben ist, maßgebend waren (Urteil vom 6. Januar 1972 - BVerwG 6 C 96, 67 - [Buchholz 232 § 90 BBGNr. 16] sowie BVerwGE 49, 89 [91]).“

Jedenfalls sind (hand-)schriftliche Dokumente (oder auch Tonbänder etc.) über Mitarbeitergespräche nicht mit Notizen gleichzusetzen, die ihrer rechtlichen Natur nach lediglich als Gedächtnisstützen für den beurteilenden Vorgesetzten *selbst* die Ausarbeitung der jeweils bevorstehenden Beurteilungen erleichtern sollen. Solche Beurteilungsnotizen haben nämlich nach der Rechtsprechung (BVerwGE 33, 183 ff., BVerwGE 62, 135 ff.) keine Personalaktenqualität, soweit ihre Kenntnis auf den beurteilenden Vorgesetzten beschränkt bleibt (was bei Mitarbeitergesprächen nicht der Fall ist).

Das SMI hat sich meinen Argumenten nicht verschlossen und in der SächsBeurtVO-VwV-SMI klarstellend Qualität und weitere Behandlung der Aufzeichnungen über Mitarbeitergespräche geregelt. Nach Nr. 13 der SächsBeurtVO-VwV-SMI dürfen nur Aufzeichnungen über den *Zeitpunkt* des Mitarbeiter-Vorgesetzten-Gesprächs sowie zur Frage, *ob* Zielvereinbarungen getroffen wurden, zur Personalakte genommen werden, also keinesfalls der Inhalt des Gesprächs.

2. *Beurteilungskommissionen*
   Die obersten Dienstbehörden dürfen nach § 115 Satz 3 SächsBG die Einzelheiten der Beurteilung für ihren Dienstbereich regeln. § 8 Abs. 2 SächsBeurtVO sieht die Einrichtung von Beurteilungskommissionen vor, trifft aber keine Aussage über deren Zusammensetzung und ermächtigt stattdessen das SMI, das Nähere durch Verwaltungsvorschrift zu bestimmen. Dem SMI habe ich mitgeteilt, dass die Festlegung des Teilnehmerkreises nicht an den Grundsätzen des § 117 Abs. 3 SächsBG und der Nr. A II der Verwaltungsvorschrift des SMI über die Führung und Verwaltung von Personalakten vom 11. Dezember 1998 vorbeigehen darf. Danach sind Personaldaten vertraulich zu behandeln und dürfen wegen Ihrer Sensibilität nur dem originär mit Personalangelegenheiten betrauten eng begrenzten Personenkreis zugänglich sein. Bei der Festlegung des Teilnehmerkreises der Beurteilungskommission wurde zunächst hierauf nicht ausreichend Rücksicht genommen. Insbesondere war vorgesehen, in die Beurteilungskommissionen - außer den eigentlichen Vorgesetzten und dem Vertreter der personalverwaltenden Stelle - auch Bedienstete zu entsenden, die *nicht* Vorgesetzte der zu Beurteilenden sind.

   Auch hier wurde in Nr. 7 SächsBeurtVO-VwV-SMI eine datenschutzgerechte Regelung getroffen.

5.1.3 Richtlinie des Präsidiums der Bereitschaftspolizei Sachsen zur Führung von Beurteilungsunterlagen und zur Erstellung von Beurteilungen für Beamte des Polizeivollzugsdienstes vom 10.7.1997

Auf den in 6/5.1.2 dargestellten Sachverhalt hat das Präsidium der Bereitschaftspoli-

zei Sachsen reagiert und zu begründen versucht, weshalb es sich für den Erlass der Beurteilungsrichtlinie im Rahmen seiner Organisationshoheit für legitimiert hält.

Selbstverständlich dürfen Behörden im Rahmen ihrer Organisationshoheit Verwaltungsvorschriften erlassen. So bestehen keine Bedenken, wenn das Präsidium der Bereitschaftspolizei Sachsen Richtlinien z. B. über den Einsatz, die Bereitschaft, das Verhalten bei Demonstrationen oder im Katastrophenfall, also Regelungen für einen ordnungsgemäßen Dienstablauf, erlässt.

Die Organisationshoheit findet allerdings in der Verfassung und den Gesetzen ihre Grenzen. Mit dem Erlass der im Betreff genannten Beurteilungsrichtlinie, mit der ein vom SächsBG nicht vorgesehenes zusätzliches Personalaktenrecht geschaffen wird, werden diese Grenzen überschritten.

Nach Art. 75 Abs. 2 SächsVerf erlässt die Staatsregierung die zur Ausführung der Gesetze erforderlichen Verwaltungsvorschriften, soweit die Gesetze nichts anderes bestimmen. § 115 Abs. 1 Satz 3 SächsBG ermächtigt die *Obersten Dienstbehörden* (und nur diese) die Einzelheiten der Beurteilung für ihren Dienstbereich (also einschließlich der Bereitschaftspolizei) zu bestimmen. Eben dies hat das SMI mit der SächsBeurtR-Pol und dem Erlass vom 13.6.1996, Az.: 35-0312.20/19, *abschließend* getan. Ich halte die gesamte Richtlinie des Präsidiums der Bereitschaftspolizei Sachsen mangels Kompetenz zu deren Erlass für rechtswidrig.

Ungeachtet dessen ist zu Nr. 3 der Beurteilungsrichtlinie der Bereitschaftspolizei (abgedruckt unter 6/5.1.2) Folgendes zu sagen:

Nach § 117 Abs. 1 Satz 2 SächsBG gehören zur Personalakte alle Unterlagen (einschließlich der in Dateien gespeicherten), die den Beamten betreffen, soweit sie mit seinem Dienstverhältnis in einem *unmittelbaren inneren Zusammenhang* stehen (Personalakten). Die in Nr. 3 der Beurteilungsrichtlinie der Bereitschaftspolizei vorgesehene Verfahrensweise, nämlich dass (im Vorfeld des eigentlichen Beurteilungsverfahrens)

- Leistungsnotizen mit negativen Aussagen zeitnah zum Ereignis *zu eröffnen sind, damit der Betroffene Stellung nehmen kann*,
- mündlich vorgetragene Remonstrationen in einem Aktenvermerk festzuhalten und ebenso wie schriftliche Äußerungen des Betroffenen zu den Beurteilungsakten zu nehmen sind,
- die Gründe für eine Nichtabhilfe schriftlich zu den Beurteilungsunterlagen zu nehmen sind,
- die Beurteilungsakten über Beamte des höheren Dienstes beim Präsidium der Bereitschaftspolizei geführt werden,
- alle im Zusammenhang mit Beurteilungen gefertigten Aufzeichnungen *vertrauliche Personalangelegenheiten* sind,

weist eindeutig auf eine Personalaktenqualität der gesammelten Daten hin. Hinzu kommt, dass die gemäß Nr. 6.3 der Beurteilungsrichtlinie der Bereitschaftspolizei von

den Hilfsbeurteilern zu führenden Beurteilungsunterlagen und zu erstellenden Leistungsnotizen vom Beurteiler kontrolliert werden (Nr. 6.2 der Beurteilungsrichtlinie). Der von der Bereitschaftspolizei herangezogene Beschluss des I. Wehrdienstsenats vom 10. September 1968 - I WB 19.68 (BVerwGE 33, 183 ff.) befasst sich ausschließlich mit der Frage ob und ggf. wann Leistungsnotizen Personalaktenqualität besitzen (nicht also mit den übrigen Maßnahmen und Regelungen wie sie Nr. 3 der Beurteilungsrichtlinie der Bereitschaftspolizei enthält).

Zitate aus dem Beschluss:

„Die Aufbewahrung der vorbereitenden Beurteilungsnotizen in den Personalakten und ihre Weitergabe an vorgesetzte Dienststellen sind unzulässig."

„Vorbereitende Beurteilungsnotizen sind ihrer rechtlichen Natur nach lediglich Gedächtnisstützen für den beurteilenden Vorgesetzten selbst, die ihm die Ausarbeitung der jeweils bevorstehenden Beurteilungen erleichtern sollen und diesen Zweck nach ihrer Sichtung anläßlich der Fertigung der Beurteilung erfüllt haben. Schon aus dieser Zielrichtung ergibt sich das in Abs. 2 der genannten Verwaltungsbestimmung enthaltene Verbot der Aufbewahrung der vorbereitenden Beurteilungsnotizen in den Personalunterlagen und ihrer Weitergabe an vorgesetzte Dienststellen sowie das Gebot, sie - spätestens einen Monat - nach Eröffnung der Beurteilung zu vernichten. Ihre Kenntnis muß eben in jedem Fall auf den beurteilenden Vorgesetzten beschränkt bleiben, nur so läßt sich, wenn überhaupt, ihre Führung in Abweichung vom Wortlaut des § 29 Abs. 3 SG (Anmerkung: Einsichtsrecht des Soldaten in seine vollständige Personalakte) rechtfertigen. Daraus folgt, daß sich ihre rechtliche Natur jedenfalls dann ändert, wenn sie mit dem Willen des Fertigers zur Kenntnis Dritter gelangen, insbesondere an - in der Bestimmung noch ausdrücklich als Empfänger ausgeschlossene - vorgesetzte Dienststellen weitergegeben werden. In diesem Falle unterliegen sie voll den Vorschriften des § 29 SG." (Anmerkung: Sie haben dann also Personalaktenqualität!)

Auch das Urteil des 2. Senats vom 2. April 1981 - BVerwG 2 C 34.79 (BVerwGE 62, 135 ff.) befasst sich (nur) mit der Frage, ob *Leistungsnotizen* Personalaktenqualität besitzen oder nicht.

Das in Nr. 3 der Beurteilungsrichtlinie der Bereitschaftspolizei gewählte Verfahren geht jedoch weit über das Erstellen von Beurteilungsnotizen hinaus, so dass mir an dieser Stelle das Zitat auf den Seiten 140 unten und 141 des vorgenannten Urteils erwähnenswert erscheint:

„Zu den Vorgängen, die in einem inneren Zusammenhang mit dem Beamten- oder Richterverhältnis stehen und deshalb zu den Personalakten genommen werden müssen, gehören hiernach - neben Personalunterlagen und dienstlichen Beurteilungen - nicht nur die Vorgänge, die den Inhalt des Dienstverhältnisses insgesamt oder einzelner aus ihm fließender Rechte und Pflichten bestimmen oder verändern, sondern auch die Unterlagen, die die Art und Weise erhellen, in der die jeweilige Entscheidung vorbereitet worden ist, oder die Aufschluß über die Gesichtspunkte und

Erwägungen geben, die für die einzelne das Dienstverhältnis berührende Maßnahme oder dafür, daß sie unterblieben ist, maßgebend waren (Urteil vom 6. Januar 1972 - BVerwG 6 C 96,67 - [Buchholz 232 § 90 BBGNr. 16] sowie BVerwGE 49, 89 [91]).“

Beurteilungsnotizen für sich gesehen fallen nach der Rechtsprechung nicht hierunter. Jedoch erlangen diese durch die Regelungen in Nr. 3 der Richtlinie der Bereitschaftspolizei eine völlig neue Qualität, so dass das Verfahren sowie die Beurteilungsakten - falls sie nicht schon an der fehlenden Kompetenz zum Erlass der Richtlinie scheitern würden - an §§ 117 ff. SächsBG mit der Folge zu messen sind, dass die Führung solcher „Personalnebenakten“ bei der Bereitschaftspolizei - so wie vorgesehen - unzulässig ist.

Das Erstellen von Beurteilungsnotizen für den Beurteilenden selbst (als Gedankenstütze) halte ich aufgrund der o. a. Rechtsprechung für zulässig. Einer Regelung in einer Richtlinie, die vom SMI zu erlassen wäre, bedarf es hierzu grundsätzlich nicht.

In einer gemeinsamen Erörterung vertrat das SMI (später auch schriftlich) entgegen der m. E. eindeutigen Rechtslage nach wie vor die Ansicht, dass die Bereitschaftspolizei nicht gehindert sei, für ihren Bereich die Beurteilungsrichtlinien des SMI für ihre Belange in Form einer eigenen Richtlinie „auszufüllen“, soweit sie im Einklang mit der Verwaltungsvorschrift der übergeordneten Behörde steht. Eben das war bei der von mir kritisierten Nr. 3, in der quasi ein neues Personalaktenrecht geschaffen wurde, nicht der Fall.

Die Angelegenheit fand mit dem Erlass der SächsBeurtVO-VwV-SMI, die auch für den Polizeibereich gilt, ihren Abschluss. Nach Nr. 13 dieser VwV dürfen nur der *Zeitpunkt* des (stattgefundenen) Mitarbeiter-Vorgesetztengesprächs sowie die Frage, *ob* Zielvereinbarungen getroffen wurden, aufgezeichnet und zur Personalakte genommen werden (siehe oben Nr. 5.1.2). Die Bereitschaftspolizei darf demnach keine abweichenden eigenen Regelungen mehr treffen.

5.1.4 Feststellung des Jubiläumsdienstalters

Zur Feststellung des Jubiläumsdienstalters wurden in der Landtagsverwaltung und in anderen obersten Landesbehörden Datenerhebungen auch bei den Beamten vorgenommen, deren Jubiläumsdienstalter bereits vor ihrer Versetzung von einem der alten Bundesländer zum Freistaat Sachsen von den seinerzeitigen Dienstherrn durch bestandskräftigen Verwaltungsakt festgestellt worden ist (was aus den Personalakten ersichtlich ist). Zumindest in einer mir bekannten obersten Landesbehörde wurden außer Fragen nach dem Werdegang (Teil 1 des Erhebungsbogens) auch die von mir bereits 1997 beanstandeten Fragen nach Funktionen in einer Partei und sonstigen gesellschaftlichen Organisationen, und zwar undifferenziert nach Herkunft der Beamten, gestellt (Teil 2, Spalte 5 des Erhebungsbogens). Diese Fragen sind im Zusammenhang mit der Feststellung des Jubiläumsdienstalters unzulässig (vgl. 5/5.1.18).

Ebenso halte ich die Frage nach dem lückenlosen Werdegang vom Verlassen der allgemeinbildenden Schule bis zum derzeitigen Beamtenverhältnis (Teil 1 des

Erhebungsbogens) bei den Beamten, bei denen das Jubiläumsdienstalter bereits durch einen früheren Dienstherrn bestandskräftig festgestellt wurde, für nicht erforderlich i. S. v. §§ 31 Abs. 1 SächsDSG, 117 Abs. 4 SächsBG und daher für unzulässig. Einer *erneuten* Feststellung des Jubiläumsdienstalters, die mit einer umfangreichen, jedoch nicht erforderlichen Datenerhebung einhergeht, bedarf es in diesen Fällen durch den Freistaat Sachsen nicht. Eine legitimierende Rechtsgrundlage ist nicht ersichtlich.

Keine Einwände bestehen hingegen im Hinblick auf §§ 3, 4 JubV gegen die Datenerhebung bei den Beamten, bei denen bisher noch kein Dienstherr das Jubiläumsdatum festgestellt hat (vorausgesetzt, die Angaben sind nicht bereits aus der Personalakte ersichtlich).

Anlässlich einer Erörterung mit dem SMF im September 1998 wurde deutlich, dass es bei den Datenerhebungen zur Feststellung des Jubiläumsdienstalters sowohl beim LfF als auch bei Personalstellen an Sensibilität mangelte. In vielen Fällen hätte eine Datenerhebung zumindest bei den Betroffenen, die als Beamte der alten Bundesländer zum Freistaat Sachsen versetzt wurden, nicht unmittelbar zu erfolgen brauchen (deren Werdegang ist aus der Personalakte ersichtlich). Das SMF vertritt allerdings im Gegensatz zu mir die Auffassung, dass die auf der Grundlage des Einigungsvertrages in Sachsen anzuwendende Verordnung über die Gewährung von Jubiläumszuwendungen an Beamte und Richter des Bundes (JubV) eine Neufestsetzung des Jubiläumsdienstalters auch für die aus den alten Bundesländern zum Freistaat Sachsen versetzten Beamten erforderlich mache. Es spiele keine Rolle, dass in diesen Fällen das Jubiläumsdienstalter durch den bisherigen Dienstherrn bestandskräftig festgestellt worden sei. Bestandsschutz sei in der JubV nicht vorgesehen.

In einem ergänzenden Gespräch mit dem LfF wurde deutlich, dass es in einer ganzen Reihe von Fällen (insbesondere bei Beamten, die von Baden-Württemberg und von Niedersachsen zum Freistaat Sachsen versetzt wurden) zu einer ungünstigeren Neufestsetzung des Jubiläumsdienstalters gekommen ist. Vereinzelten Widersprüchen wurde nicht abgeholfen. Anfechtungsklagen wurden (soweit bekannt) bisher nicht erhoben.

Die Missachtung der Bestandskraft von beamtenrechtlichen Entscheidungen früherer Dienstherrn ist aus meiner Sicht umso unverständlicher, als das SMF selbst in seinem Schreiben vom 29. Juli 1996, Az.: 13 a-P 1544-6/33-43039, auf seine Bekanntmachung vom 26. November 1993, Az.: 13 a-P 1520-7/34-59473, verweist, wonach solche Berechnungen grundsätzlich nur bei *erstmals im Beitrittsgebiet ernannten Beamten* zu erfolgen haben. Eine Neufestsetzung für Beamte, die von einem anderen Dienstherrn zum Freistaat Sachsen versetzt wurden, erfolgt nur, sofern anhand der in der Personalakte vorhandenen Unterlagen nicht berücksichtigungsfähige Zeiten (z. B. § 30 BBesG - MfS-Zugehörigkeit) erkennbar sind (was bei aus den alten Bundesländern stammenden Beamten wohl die absolute Ausnahme sein dürfte).

Vor dem Hintergrund, dass die Staatsregierung die ersatzlose Streichung der Jubiläumszuwendung mit einiger Aussicht auf Erfolg betreibt, werde ich die nunmehr überflüssigen und nach meinem Dafürhalten auch rechtswidrigen Datenerhebungen vorerst nicht weiter thematisieren.

Sollten denkbare Anfechtungsklagen benachteiligter Betroffener die Rechtswidrigkeit bestätigen und sollte es wider Erwarten zu keiner Streichung der Jubiläumszuwendung kommen, habe ich mir ein erneutes Tätigwerden vorbehalten.

5.1.5 Beamtenvereidigung

In 6/5.1.20 habe ich es für ausreichend erachtet, als Nachweis, dass ein Beamter ordnungsgemäß vereidigt wurde, lediglich zu dokumentieren,
- wer
- wann
- durch wen
- gemäß § 70 Abs. 1 SächsBG

(und zwar ohne Wiederholung der Eidesformel und der religiösen Beteuerung) vereidigt worden ist.

Die Staatsregierung hat in ihrer Stellungnahme zu meinem 6. Tätigkeitsbericht eine Prüfung zugesagt.

Anlässlich einer gemeinsamen Erörterung wurde vom SMI folgender Lösungsvorschlag unterbreitet:

„*Grundsätzlich werde nur noch protokolliert, dass die Vereidigung ordnungsgemäß erfolgt ist. auf die Möglichkeit, den Eid mit religiöser Beteuerung vorzunehmen, werde der angehende Beamte mündlich aufmerksam gemacht. Nach der Vereidigung werde der Beamte, der sich für den Eid mit religiöser Beteuerung entschieden habe, mündlich darauf hingewiesen, dass er dies auch protokollieren lassen könne. Bejahe er dies, so werde auf dem Formblatt nachträglich handschriftlich vermerkt, dass der Beamte den Eid mit religiöser Beteuerung gesprochen hat. Mit dieser Regelung müssten alle Bedenken ausgeräumt sein. Aus Effektivitätsgründen könne man aber nicht die alten Fälle wieder aufrollen und sämtliche Personalakten ‘bereinigen’*."

Mit dieser Vorgehensweise habe ich mich einverstanden erklärt.

5.1.6 Verfahren bei Gehaltspfändungen im LfF

Meinen Feststellungen zufolge unterrichtet die Bezügestelle des LfF seit Jahren die personalverwaltenden Stellen ausnahmslos über jeden Gehaltspfändungs- und Überweisungsbeschluss, und zwar unabhängig von der Höhe des Betrages und der Häufigkeit solcher Maßnahmen. Diese Mitteilungsverpflichtung fußte zunächst auf einer Verfügung des Präsidenten des LfF vom 3. März 1992, die nach meinem Dafürhalten mit dem erst später erlassenen Personalaktenrecht und dem datenschutzrechtlichen Erforderlichkeitsgrundsatz kollidiert. Weil ich entgegen § 13 Abs. 5 Satz 4 GeschoSReg nicht beteiligt wurde, wurde von mir unbemerkt in § 12 Abs. 2 VertrVO vom 8. April 1997 eine Rechtsgrundlage für das LfF geschaffen, wonach die personalverwaltende Stelle von den Pfändungsbeschlüssen zu benachrichtigen ist. Dem SMF habe ich mitgeteilt, dass diese Verfahrensregelung durch die Verordnungsermächtigung in § 1 Abs. 1 Nr. 2 SächsVertrG nicht gedeckt sein dürfte (Art. 80

Satz 2 GG). § 1 Abs. 1 Nr. 2 SächsVertrG lautet: „*Die Staatsregierung wird ermächtigt, durch Rechtsverordnung die Vertretung des Freistaates und seiner Behörden zu regeln ... für die vom Freistaat als Drittschuldner vorzunehmenden Rechtshandlungen.*“

Gemäß § 117 Abs. 2 SächsBG (vom 17.12.1992) und der VwV über die Führung und Verwaltung von Personalakten (vom 11.12.1998) enthalten Personal*teil*akten nur Unterlagen, die *nicht* in der Personal*grund*akte enthalten sind. Mit der vom LfF praktizierten und durch § 12 Abs. 2 VertrVO vorgeschriebenen Verfahrensweise gelangen jedoch undifferenziert - also unabhängig von der Höhe des Betrages und der Häufigkeit solcher Maßnahmen - Mitteilungen über Gehaltspfändungen (auch) in die Personal*grund*akte. Es liegt auf der Hand, dass undifferenzierte Mitteilungen nicht unerheblich das Persönlichkeitsrecht der Betroffenen berühren und möglicherweise auf Dauer nachteilig wirken können.

Neben der Feststellung, dass § 12 Abs. 2 VertrVO durch die Verordnungsermächtigung (s. o.) nicht gedeckt ist, gilt es, das SMF und das SMI (als für das Beamtenrecht federführendes Ressort) zu überzeugen, dass eine Mitteilung an den Dienstvorgesetzten allenfalls nur dann angemessen ist, wenn die Höhe der Pfändung und/oder die Häufigkeit der Pfändungsmaßnahmen konkrete Personalmaßnahmen z. B. aus Fürsorgegründen erforderlich machen. Einmalige oder gelegentliche Pfändungsbeschlüsse, die nicht existenzbedrohend sind, haben den Dienstvorgesetzten nicht zu interessieren und deshalb nichts in der Personal*grund*akte verloren.

Die Gespräche dauern noch an.

5.1.7 „Personalbogen Europa“

Die Arbeitsgemeinschaft der Hauptpersonalräte der obersten Landesbehörden im Freistaat Sachsen hat mir Unterlagen vorgelegt, wonach aufgrund einer Vereinbarung zwischen den Ministerien jeweils ressortintern eine Übersicht über geeignete Bedienstete für europabezogene Aufgaben zu führen ist. Ziel ist es, im Bedarfsfall eine schnelle und fachlich kompetente Auswahl eines sächsischen Bediensteten für eine Stellenbesetzung bei den europäischen Institutionen zu ermöglichen. Zur Erstellung der Übersicht sind die Einrichtungen der Geschäftsbereiche aufgefordert worden, für Europainstitutionen *geeignete* Mitarbeiter zu ermitteln, deren Daten auf dem „Personalbogen Europa“ einzutragen und diesen an das Personalreferat des Ministeriums zurückzusenden. Dort werden die ausgefüllten „Personalbögen Europa“ gesammelt (gespeichert), obgleich keinem Betroffenen konkret ein europabezogener Einsatz überhaupt in Aussicht gestellt werden kann.

Der SK und den Ressorts habe ich mitgeteilt, dass es sich hier höchstwahrscheinlich um einen klassischen Fall einer unzulässigen Vorratsdatenerhebung und -speicherung handelt. „Unverbindliche Personalwartelisten“ zu erstellen wäre datenschutzrechtlich verboten.

Nach §§ 117 Abs. 4, 121 Abs. 2 SächsBG, 31 Abs. 1 SächsDSG dürfen Beschäftigtendaten zwar für Zwecke der Personalplanung und des Personaleinsatzes erhoben und

verarbeitet werden, jedoch muss die Datenverarbeitung *erforderlich* sein, und zwar unabhängig davon, ob die Datenerhebung durch die jeweiligen Personalstellen aus den Personalakten oder bei den Betroffenen selbst erfolgt.

Der Grundsatz der Erforderlichkeit bedeutet, dass die öffentliche Stelle ohne die Daten im konkreten Einzelfall ihre Aufgabe nicht, nicht vollständig oder nicht in rechtmäßiger Weise erfüllen kann. Es genügt demnach nicht, dass die Daten zur Aufgabenerfüllung (hier im weitesten Sinne Personalplanung) „geeignet und zweckmäßig" sind; vielmehr sind Geeignetheit und Zweckmäßigkeit weitere Voraussetzungen für die Erforderlichkeit. Ebenso wenig reicht es aus, wenn die Daten zur Aufgabenerfüllung der erhebenden Stelle nur „dienlich" oder z. B. als Hintergrundinformation (wer könnte für Europa geeignet sein) nützlich sind.

Da „Europa-Stellen" ausgeschrieben werden, hat jeder Interessent die Möglichkeit, sich regulär zu bewerben.

Ich habe die SK gebeten zu veranlassen, dass der weitere Vollzug (Ausfüllen der „Personalbögen Europa") ausgesetzt wird und die bereits in den Ressorts vorliegenden „Personalbögen Europa" vorerst zuverlässig gesperrt werden (§§ 3 Abs. 2 Nr. 7, 20 SächsDSG; die Sammlung der Personalbögen stellt eine Datei i. S. v. § 3 Abs. 5 Nr. 2 SächsDSG dar). Auch habe ich zu bedenken gegeben, dass die bereits ausgefüllten Personalbögen gemäß § 19 Abs. 1 Nr. 1 SächsDSG zu löschen sind, sobald die Unzulässigkeit der Datenerhebung feststeht.

Die SK, die sich von meinen Argumenten überzeugen ließ, hat im Spätsommer 1998 die Aktion gestoppt und veranlasst, dass bereits ausgefüllte „Personalbögen Europa" zuverlässig vernichtet werden.

5.1.8 Datenschutz-/beamtenrechtliche Bewertung der beim Polizeiarzt entstehenden Patientenunterlagen

Bereitschaftspolizisten müssen, die sonstigen Beamten des Polizeivollzugsdienstes können sich im Rahmen der Heilfürsorge nach § 7 Abs. 2 Satz 2 Abs. 3 SächsHfVO vom Polizeiarzt behandeln lassen. In solchen Fällen werden die den Patienten betreffenden Daten vom Polizeiarzt nach der ärztlichen Berufsordnung in einer Patientenakte dokumentiert.

§ 118 SächsBG besagt u. a., dass Unterlagen über Heilfürsorge stets als *Teilpersonalakte* zu führen seien. Ich hatte zu prüfen, ob diese Bestimmung auch auf die beim Polizeiarzt im Rahmen der Heilfürsorge entstandenen Patientenakten zutrifft.

Unter verfassungskonformer Auslegung des § 118 SächsBG zugunsten des Rechts auf informationelle Selbstbestimmung habe ich die Angelegenheit wie folgt bewertet und das SMI über meine Auffassung unterrichtet:

Auch wenn der Polizeiarzt nach der *Heilfürsorgeverordnung* als behandelnder Arzt tätig wird, stellen die dabei entstehenden Unterlagen keine Heilfürsorgedaten i. S. v.

§ 118 SächsBG dar. Die Dokumentationspflicht des behandelnden (Polizei-)Arztes nach der ärztlichen Berufsordnung geht üblicherweise erheblich über die im Rahmen der Heilfürsorge erforderlichen Personalaktendaten hinaus. Es handelt sich auch begrifflich nicht um Personalaktendaten, so dass nicht die beamtenrechtlichen, sondern nur die für die ärztliche Dokumentation geltenden Verarbeitungsregeln einschlägig sind. Für die vom Polizeiarzt dokumentierten Patientendaten kann demnach nichts anderes gelten als für die Unterlagen, die im Rahmen der Heilfürsorge bei einem niedergelassenen Vertragsarzt (vgl. § 7 Abs. 2 Satz 1 SächsHfVO) in dessen Patientenakte dokumentiert wurden. Die Patientenakten sowohl beim Polizeiarzt als auch beim Vertragsarzt unterliegen in vollem Umfang der ärztlichen Schweigepflicht.

§ 118 SächsBG gilt allerdings für Heilfürsorgeunterlagen, die außerhalb der ärztlichen Dokumentation, etwa vergleichbar mit dem Beihilfeverfahren, zum Zwecke der Abrechnung entstanden sind. Ein Indiz für diese Auffassung findet sich auch in § 123 Abs. 2 Satz 2 SächsBG, wonach Unterlagen über Beihilfe und Heilfürsorge, aus denen die Art einer Erkrankung ersichtlich ist, unverzüglich zurückzugeben sind, wenn sie für den Zweck, für den sie vorgelegt wurden, nicht mehr benötigt werden (die in der Patientenakte dokumentierten Patientendaten wurden nicht vorgelegt, so dass sich die Rückgabeverpflichtung nur auf die Abrechnungsunterlagen erstrecken kann).

5.1.9 Unzulässige Datenübermittlungen in einem Kündigungsverfahren

Ich erhielt Kenntnis von einem Rechtsstreit zwischen dem Landrat und dem Intendanten eines kommunalen Volkstheaters, in dem es um die Entlassung des Intendanten nach langen Querelen mit dem Theaterpersonal ging.

In seinem Bestreben, Schaden vom Theater abzuwenden, übermittelte der Landrat dem Theater den kompletten Klageschriftsatz samt ausführlicher Begründung des Intendanten mit der Folge, dass außer der „Schauspielleitung“ auch der Personalrat und viele Theaterbedienstete Kenntnis vom Inhalt der Schriftsätze nahmen, um ihrerseits schriftlich gegen den Intendanten zu opponieren. Erst das Urteil des Sächsischen Landesarbeitsgerichts über die Unzulässigkeit solcher Datenübermittlungen bewirkte, dass in dieser Angelegenheit keine weiteren Schriftsätze mehr an sachlich unzuständige Stellen im Theater übermittelt wurden.

Ferner übermittelte der Landrat ein ausschließlich für den Intendanten bestimmtes und für dessen weitere Theaterarbeit einschneidendes Schreiben mit personenbezogenem Inhalt per Telefax an das Theater, wo eine Kenntnisnahme durch unbefugte Dritte nicht per se auszuschließen war.

Ich informierte den Landrat darüber, dass mit der Übersendung der Schriftsätze an Unbefugte (Schauspielleitung, Personalrat, Beschäftigte) gegen § 31 Abs. 1 und Abs. 2 SächsDSG verstoßen wurde und dass ferner bei der Versendung von personenbezogenen Schreiben per Telefax meine Bekanntmachung zum Datenschutz bei Telefax-Übertragungen vom 14. Juni 1993 (2/16.1.1) hätte beachtet werden müssen.

Der Landrat hat mir daraufhin bestätigt, dass künftig mit Beschäftigtendaten noch sorgsamer als bisher umgegangen wird.

5.1.10 Telefonverzeichnis einer Technischen Hochschule im Internet

Eine TU fragte, unter welchen Voraussetzungen das Telefonverzeichnis der Hochschule ins Internet gestellt werden dürfe. Meine Antwort:

Telefonverzeichnisse sind ihrem Wesen nach für den Dienstgebrauch zweckgebunden. Die darin enthaltenen Beschäftigtendaten dürfen gemäß § 31 Abs. 2 Satz 1 SächsDSG (abweichend von § 15) nur auf gesetzlicher Grundlage oder mit Einwilligung der Betroffenen an Stellen außerhalb des öffentlichen Bereichs übermittelt werden, es sei denn, es handelt sich um im Dienstverkehr zwingend erforderliche Auskünfte (§ 31 Abs. 2 Satz 3 SächsDSG).

In den letzten Jahren kann man mehr und mehr von einer Globalisierung des Wissenschaftsbetriebes sprechen. Weltweite Kontakte sind für die „vollwertigen" Mitglieder der Wissenschaftsgemeinschaft üblich und notwendig. Deshalb können *derartige* personenbezogene Daten auch ohne Einwilligung der einzelnen Betroffenen ins Internet eingestellt werden. Dies bedeutet, dass Institute, ihre Direktoren, die Professoren sowie die übrigen habilitierten Personen, z. B. Privatdozenten, im Internet zu nennen sind, und zwar unabhängig davon, ob sie dem zugestimmt haben oder nicht. Ich kann auch nicht ausschließen, dass es über die Professoren hinaus einige wenige Personen an der TU gibt, deren dienstliche Erreichbarkeit über Internet von der Hochschule garantiert werden muss.

Anderes gilt grundsätzlich für die Mitarbeiter der Professoren und ihre Hilfskräfte. Denn ich kann nicht feststellen, dass der weltweite Wissenschaftsbetrieb es erfordern würde, dass derartige Personen sich im Internet anbieten, ständig weltweite Kontakte zu pflegen. Die Einwilligungslösung wäre dort die einzige rechtlich saubere Möglichkeit, eine Verletzung des Persönlichkeitsrechts zu vermeiden. Andererseits dürfen durch das Instrument der Einwilligung die gesetzlichen Aufgaben und Befugnisse öffentlicher Stellen nicht erweitert werden. Dies folgt letztlich aus dem Grundsatz der Gesetzmäßigkeit der Verwaltung. Wie weit die „Wissenschaftsverwaltung" einer öffentlichen Hochschule an diesen Grundsatz gebunden ist, mag allerdings fraglich sein, weil die Hochschule insoweit nicht hoheitsrechtlich, sondern als Grundrechtsträger tätig wird. Ich neige im Ergebnis jedoch dazu, dass die Veröffentlichung der Daten von Hilfspersonen des Wissenschaftsbetriebs im Internet nicht zu den Aufgaben einer Hochschule gehört.

Dies hat weit über den Datenschutz hinausgehende gute Gründe: Zum einen wird damit der Internet-Kontakt über die Träger des Wissenschaftsbetriebes, nämlich die Professoren, kanalisiert, zum anderen werden unnötige Pflege- und Kostenaufwendungen vermieden, die allein wegen der hohen Personalfluktuation notwendig wären.

In Bezug auf die nicht-habilitierten Personen habe ich der TU einen Aufruf zur Anmeldung vorgeschlagen, der allerdings von den jeweiligen Institutsdirektoren abgezeichnet sein sollte. Wer sich dann anmeldet, hat in die Einstellung seines Namens im Internet eingewilligt.

5.1.11 Einblick in Personalakten durch die Innenrevision der AOK Sachsen zu Prüfungszwecken

Der Innenrevision der AOK Sachsen habe ich auf die Frage, ob ihr die eigene Personalstelle die Einsicht in die Personalakten der AOK-Bediensteten zu Prüfungszwecken verweigern dürfe, wie folgt geantwortet:

Sollte es für die Innenrevision der AOK Rechtsgrundlagen geben, wie sie beispielsweise in der Sächsischen Haushaltsordnung oder in der Sächsischen Kommunalprüfungsordnung enthalten sind, halte ich die Einsichtnahme in Personalakten je nach Prüfungsauftrag auch ohne Einwilligung der Betroffenen für gerechtfertigt. Ebenso zulässig halte ich die Einsichtnahme in Personalakten ohne Einwilligung der Betroffenen, wenn in einer die Aufgaben der Innenrevision beschreibenden Geschäftsanweisung des Vorstandes die Einsichtnahme in Personalakten nicht ausdrücklich ausgeschlossen wurde. Da die Innenrevision als verlängerter Arm des Vorstandes handelt, darf die Personalstelle nach meinem Dafürhalten ihre Weigerung nicht damit begründen, der Vorstand könne ja persönlich die Personalakten einsehen (bei den ca. 3000 Beschäftigten der AOK Sachsen ein schier unmögliches Ansinnen). Vielmehr gilt es zu bedenken, dass eine nicht durchgeführte Prüfung der Personalakten durch die Innenrevision mit Sicherheit anlässlich einer Prüfung durch das Sächsische Landesprüfungsamt für Sozialversicherung gemäß § 274 SGB V eine Beanstandung nach sich ziehen würde.

5.1.12 Keine Einsichtnahme in ärztliche Gutachten durch Fachämter

Bestehen aufgrund einer gesundheitlichen Beeinträchtigung bei einem Beschäftigten Zweifel über Art und Umfang seiner weiteren Einsatzfähigkeit (z. B. bückende und hebende Tätigkeiten bei Gärtnern oder Archivaren, Allergien bei Bibliotheksmitarbeitern, Umgang mit Publikum bei psychischen Störungen, Augenerkrankungen), werden von der personalverwaltenden Stelle in der Regel ärztliche Gutachten als Entscheidungsgrundlage eingeholt.

In einer Gemeinde verlangten die Fachämter vom Personalamt die Weitergabe der vollständigen Gutachten. Das Personalamt hat dies verweigert und dem Fachamt lediglich das gutachterliche Ergebnis mitgeteilt oder Auszüge übersandt. Da die Meinungsverschiedenheiten nicht beigelegt werden konnten, wurde ich um eine datenschutzrechtliche Bewertung der gegenwärtigen Praxis gebeten.

Nach § 31 Abs. 1 SächsDSG dürfen öffentliche Stellen Beschäftigtendaten nur verarbeiten, „*soweit* dies zur Eingehung, Durchführung oder Beendigung des Dienst- oder Arbeitsverhältnisses oder zur Durchführung organisatorischer, personeller oder sozialer Maßnahmen, insbesondere auch zu Zwecken der Personalplanung oder des

Personaleinsatzes *erforderlich* ist oder ein Gesetz, ein Tarifvertrag oder eine Dienstvereinbarung dies vorsieht".

Da die Weitergabe von ärztlichen Gutachten innerhalb einer Gemeinde weder gesetzlich noch tarifvertraglich geregelt ist und Dienstvereinbarungen für diesen Fall vom Sächsischen Personalvertretungsgesetz nicht vorgesehen sind, darf das Personalamt aus dem Gutachten nur diejenigen Daten mitteilen, deren Kenntnis für das Fachamt erforderlich ist, damit der Beschäftigte entsprechend eingesetzt werden kann. Arztgutachten enthalten jedoch meist darüber hinausgehende Informationen, deren Kenntnis jedenfalls für ein Fachamt nicht erforderlich ist.

Die übliche Praxis entspricht insoweit datenschutzrechtlichen Grundsätzen.

5.1.13 Teilnehmereinschätzungen im Rahmen von Fortbildungsveranstaltungen

Das SMF informierte mich über die Absicht, künftig bei Fortbildungsveranstaltungen von mindestens einwöchiger Dauer, die durchgängig von demselben Dozenten abgehalten werden, eine Einschätzung der Teilnehmer durchzuführen, welche sich in einem „qualifizierten Fortbildungsnachweis" („mit großem Erfolg", „mit Erfolg" oder „teilgenommen") niederschlagen soll.

Weil die Deutsche Steuer-Gewerkschaft datenschutzrechtliche Bedenken angemeldet hat, bat mich das SMF um Stellungnahme:

Ich hielt die Absicht, bestimmte Fortbildungslehrgänge an einen „qualifizierten Fortbildungsnachweis" zu binden, im Hinblick auf Art. 33 Abs. 2 GG, § 72 Abs. 2 SächsBG für einen interessanten Ansatz. Einen Konflikt zu § 31 Abs. 1 SächsDSG - wie ihn die Deutsche Steuer-Gewerkschaft sieht - vermochte ich zunächst nicht zu erkennen, zumal qualifizierte Fortbildung u. a. für das Fortkommen der Beschäftigten (also für die Durchführung des Dienst- oder Arbeitsverhältnisses) mitentscheidend ist.

Vor meiner abschließenden Bewertung wollte ich aber vom SMF wissen, nach welchen Kriterien der Nachweis der erfolgreichen oder weniger erfolgreichen Teilnahme zu erbringen ist (z. B. in einer Fortbildungsordnung). Außerdem müsste die Qualifikation des Dozenten für eine *objektive und gerechte* Bewertung der Kursteilnehmer gewährleistet sein.

Die vom SMF daraufhin angeführten *Kritierien*, wie *„Einsatz jedes einzelnen Teilnehmers und die Qualität seiner Wortbeiträge*" vermochten mich keineswegs zu überzeugen und veranlassten mich zu folgenden Gegenargumenten:

Die Bewertung des „*Einsatzes*" und der „*Qualität der Wortbeiträge*" eines Kursteilnehmers führt zu einer subjektiven Beurteilung durch den Dozenten, die mehr schadet als nützt. Beispielsweise beherrscht der eine Kursteilnehmer bereits bestens die Materie, ohne viel zu sagen, für einen anderen ist alles „Neuland", er stellt aber

aktiv Fragen, die aus der subjektiven Sicht des Dozenten „nur den Betrieb aufhalten“, in Wahrheit aber klärend wirken.

Mein Wunsch war es, dass *Kriterien* aufgestellt werden, die gerade eine solche subjektive Einschätzung der Kursteilnehmer vermeiden. Eine *objektive* Einschätzung, ob die Kursteilnahme erfolgreich oder weniger erfolgreich war, ist z. B. dann möglich, wenn das eindeutig zu definierende Lehrgangsziel durch (schriftliche) Beantwortung von Fragen oder Lösung von Aufgaben kontrolliert wird. Die dabei erzielten Wissensdurchschnitte würden - sozusagen als (aus eigener Erfahrung oftmals notwendiges) Nebenprodukt - auch auf die Qualität der Wissensvermittlung durch den Dozenten schließen lassen.

Im Hinblick auf den rein subjektiven Charakter der Teilnehmereinschätzung habe ich der vom SMF vorgesehenen Verfahrensweise eine Absage erteilt und verlangt, dass an dem von mir kritisierten Bewertungsverfahren, jedenfalls in der mir vorgestellten Form, nicht mehr festgehalten wird, solange objektive Kriterien über die Qualifikation der Dozenten, das Vorwissen der Teilnehmer und die Bewertungskriterien ihrer „Leistung“ nicht bestehen.
Fortbildung soll bilden und nicht zum Sammeln guter Noten genutzt werden; deshalb sollten nicht Datensammlungen veranstaltet, sondern andere Formen der Motivation gesucht werden.

Die Reaktion des SMF bleibt abzuwarten.

5.1.14 Erfordernis einer Dienstvereinbarung beim Einsatz von Personalinformationssystemen

Immer häufiger werden von öffentlichen Stellen zur Unterstützung der Personalverwaltung und Personalwirtschaft automatisierte Personalinformationssysteme eingesetzt. Diese Systeme haben gegenüber der manuellen Datenverarbeitung zwar viele Vorteile, wie z. B. größere Verfügbarkeit und Verknüpfbarkeit der Beschäftigtendaten sowie schnellere Auswertungsmöglichkeiten der Informationen. Sie bringen aber auch ein erhöhtes Risiko des Datenmissbrauchs mit sich. Daher müssen vor Inbetriebnahme der Systeme detaillierte Regelungen zum Datenschutz schriftlich festgelegt werden. Beispielsweise sind in einer Verfahrensbeschreibung alle möglichen und tatsächlichen Auswertungen zu nennen. Des Weiteren muss der Verfahrenszweck eindeutig festgelegt sein. Wegen der näheren Einzelheiten nehme ich auf 5/5.1.4 Bezug.

Ich habe wegen des großen Regelungsbedarfs und insbesondere aufgrund der hohen Sensibilität von Beschäftigtendaten die öffentlichen Stellen aufgefordert, Dienstvereinbarungen abzuschließen, in denen die datenschutzrechtlichen Anforderungen berücksichtigt werden.

Teilweise wurde von den öffentlichen Stellen hiergegen eingewandt, dass es für diese Forderung keine gesetzliche Grundlage gebe. Die Vorschrift des § 31 Abs. 1 SächsDSG überlasse es ihrem Wortlaut nach der datenverarbeitenden Stelle, ob sie

eine Dienstvereinbarung schließt („... *oder* eine Dienstvereinbarung dies vorsieht"). Auch lasse sich ein „Zwang zur Dienstvereinbarung" nicht aus § 80 Abs. 3 SächsPersVG ableiten. Der Abschluss von Dienstvereinbarungen sei hier nur als eine Möglichkeit der Mitbestimmung genannt („gegebenenfalls").

Ich habe dem entgegengehalten, dass der Abschluss von Dienstvereinbarungen hier aus verfassungsrechtlichen Gründen zwingend erforderlich ist: Nach dem Volkszählungsurteil des Bundesverfassungsgerichts (BVerfGE 65, 1 ff. [45]) muss sich aus Rechtsvorschriften, die das Grundrecht auf informationelle Selbstbestimmung einschränken, klar und für den Einzelnen erkennbar ergeben, wie weit diese Beschränkungen gehen (Gebot der Normenklarheit oder Bestimmtheitsgebot). An die Bestimmtheit einer grundrechtseinschränkenden Rechtsvorschrift stellt das Bundesverfassungsgericht (BVerfGE 56, 12) folgende Anforderungen: *„Der Grad der jeweils zu fordernden Bestimmtheit einer Regelung hängt ... von der Eigenart des Sachverhalts ab, insbesondere ... davon, in welchem Umfang der zu regelnde Sachbereich einer genaueren begrifflichen Umschreibung ... zugänglich ist. Darüber hinaus ist auch auf die Intensität der Auswirkungen der Regelung für den Betroffenen Bedacht zu nehmen. Je schwerwiegender die Auswirkungen sind, desto höhere Anforderungen werden an die Bestimmtheit der Ermächtigung zu stellen sein.*"

Wie bereits dargelegt, besteht beim Betrieb von Personalinformationssystemen ein sehr hoher (datenschutzrechtlicher) Regelungsbedarf. Die erhebliche Gefahr für das Persönlichkeitsrecht bei der automatisierten Datenverarbeitung hat das Bundesverfassungsgericht (BVerfGE 65, 42, 46) zudem ausdrücklich betont. Daher kann für den Einsatz automatisierter Personalinformationssysteme nicht auf die allgemeine Ermächtigungsgrundlage des § 31 Abs. 1 (1. Alternative) SächsDSG zurückgegriffen werden, der lediglich den Grundsatz der Erforderlichkeit als Voraussetzung der Datenverarbeitung nennt. Sie kommt - auch deswegen, weil das Datenschutzgesetz lediglich ein „Auffanggesetz" ist - nur bei geringen Eingriffen in das Grundrecht auf informationelle Selbstbestimmung in Betracht. Aus verfassungsrechtlicher Sicht ist es also geboten, dass die Dienststellen und Personalvertretungen insoweit (datenschutzgerechte) Dienstvereinbarungen abschließen. Nur Dienstvereinbarungen (und nicht Dienstanweisungen) haben „normative Wirkung" (vgl. 2/5.1.12) und sind daher Rechtsvorschriften im Sinne von § 4 Abs. 1 Nr. 1 SächsDSG, die einen Grundrechtseingriff rechtfertigen können.

5.1.15 Vollzug der Leistungsstufen- und der Leistungsprämienverordnung

Erbringt ein Beamter, der Bezüge nach der Besoldungsordnung A erhält, dauerhaft herausragende Leistungen und ist zu erwarten, dass er dies auch in Zukunft tun wird, kann er nach der Leistungsstufenverordnung vorzeitig in die nächsthöhere Besoldungsstufe aufsteigen; solange seine Gesamtleistungen den Anforderungen nicht genügen, steigt er nicht in die nächsthöhere Besoldungsstufe auf. Bei einer herausragenden Einzelleistung besteht die Möglichkeit, dem Beamten eine Leistungsprämie nach der Leistungsprämienverordnung zu gewähren. Beide Verordnungen begrenzen die Zahl der jährlichen Empfänger auf 10 v. H. der am 1. Januar des laufenden Kalenderjahrs vorhandenen Beamten der Besoldungsordnung A und schließen Probe-

beamte sowie Beamte auf Zeit aus. Die Entscheidung über die einzelne Maßnahme trifft die oberste Dienstbehörde oder die von ihr bestimmte Stelle.

Zum Vollzug der Leistungsstufen- und Leistungsprämienverordnung beabsichtigte das SMF, das LfF anzuweisen, den obersten Landesbehörden Namenslisten mit den benötigten Besoldungsdaten *aller* Beamten des Geschäftsbereichs zur Verfügung zu stellen, die von den Verordnungen betroffen sein können.

Mein Einwand richtete sich dagegen, dass stets die oberste Landesbehörde die Listen erhalten sollte, obwohl sie nicht in jedem Fall die für die Vergabe von Leistungsstufen oder Leistungsprämien entscheidende Stelle ist. Zur Überwachung der Zehn-Prozent-Quote sind keine Listen erforderlich; dazu genügt rein statistisches, nicht personenbezogenes Zahlenmaterial.

Das SMF hat daraufhin die obersten Landesbehörden gebeten, dem LfF die für den Vollzug der Verordnungen zuständigen Stellen mitzuteilen. Diese erhalten nunmehr die Namenslisten. Für die Ermittlung und Überwachung der Quoten werden gesonderte Listen mit den entsprechenden Zahlen erstellt.

5.1.16 Umgang mit Bescheiden des Bundesbeauftragten für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR (BStU)

Ein Bürger einer kleinen Gemeinde beschwerte sich bei mir darüber, dass die Sekretärin des Bürgermeisters die Posteingänge des BStU geöffnet hatte. Ich habe dem Bürgermeister, der von einem „Versehen“ seiner Mitarbeiterin sprach und sich hierfür entschuldigte, zur Problematik Folgendes mitgeteilt:

Schriftstücke des BStU mit Auskünften zur Tätigkeit für den Staatssicherheitsdienst der ehemaligen DDR sind vertrauliche Personalsachen und auf dem Umschlag als solche gekennzeichnet. Diese Schriftstücke dürfen nach der Verwaltungsvorschrift des SMI über die Führung und Verwaltung von Personalakten vom 11. Dezember 1998 nur von den Personen geöffnet werden, die unmittelbar entsprechende Erklärungen bearbeiten oder dazu befugt sind.

Darüber hinaus empfahl ich dem Bürgermeister, die korrekte Verfahrensweise beim Umgang mit derartigen Schriftstücken auch für den Vertretungsfall (Urlaub, Krankheit) in eine Dienstanweisung für das Sekretariat aufzunehmen. Der Bürgermeister griff meinen Vorschlag auf, überarbeitete die bereits vorliegende Dienstordnung der Gemeinde und legte sie sodann dem Gemeinderat zur Verabschiedung vor.

5.1.17 Umgang mit BStU-Unterlagen im SMWK

Bei einer Querschnittskontrolle des Umgangs mit personenbezogenen Unterlagen des BStU im SMWK musste ich schwere Verstöße gegen gesetzliche Bestimmungen der Personaldatenverarbeitung feststellen. Wegen des Ausmaßes der datenschutzrechtlichen Defizite habe ich von meinem Recht gemäß § 27 Abs. 2 SächsDSG Gebrauch gemacht und mich mit einem Bericht an den Landtag gewandt. Weil die

Ergebnisse der Kontrolle der Landtags-Drucksache 2/9996 zu entnehmen sind, möchte ich an dieser Stelle lediglich in Stichpunkten die gravierendsten Rechtsverstöße anführen:

- Zu Beginn der angekündigten Kontrolle konnte vom SMWK das Dateien- und Geräteverzeichnis nach § 10 Abs. 1 SächsDSG nicht vorgelegt werden. Erst nachträglich wurde ein Verzeichnis erstellt. Darin waren auch automatisierte Dateien mit Beschäftigtendaten aufgeführt, über deren Inbetriebnahme ich entgegen dem Gebot des § 31 Abs. 7 SächsDSG nicht informiert worden war.

- In einem Kellerraum lagerten ca. 2700 Teilpersonalakten mit Stasi-Bezug in offenstehenden Schränken. Der Schlüssel zu diesem Raum befand sich an der Pforte in der allgemeinen Schlüsselverwaltung. Eine Protokollierung der Schlüsselverwaltung gab es nicht. Nach Ende der Dienstzeit sowie an den Wochenenden hatte ein privater Wachdienst den Schlüssel zu diesem Raum zur Verfügung und mithin ungehinderten Zugang zu den dort verwahrten Unterlagen - Verstöße gegen § 9 SächsDSG. Erst aufgrund meiner Kontrolle wurden diese Mängel abgestellt.

- Die Protokollierung der Entnahmen dieser Stasi-Akten war unzureichend, weil in den meisten Fällen keine Zugangs- und Entnahmeprotokolle existierten. Eine 450 Fälle umfassende Stichprobenkontrolle zweier Buchstaben ergab eine Quote von acht Prozent bzw. fünf Prozent nicht lokalisierbarer Akten.

- Die Koordinierung der Überprüfung von Bediensteten des nachgeordneten Bereichs des SMWK war (und ist) einem Mitarbeiter einer Fachabteilung übertragen, der in diesem Aufgabenbereich weder seinem eigenen Abteilungsleiter noch dem für Personalfragen zuständigen Abteilungsleiter unterstand/untersteht. Dieser Bedienstete führt seit 1993 eine automatisierte Datei (Dateiname: „Gauck“) mit personenbezogenen Daten über durchgeführte/eingeleitete BStU-Überprüfungen. Bei der Kontrolle war dieser PC-Datenbestand völlig ungesichert. Regeln für Löschung, Sperrung und Protokollierung existierten nicht. Eine gesetzlich vorgeschriebene Datenpflege war somit unmöglich.

Der Staatsminister hat meine Beanstandung zu bagatellisieren versucht.

5.2 Personalvertretung

5.2.1 Teilnahme der Frauenbeauftragten an Personalratssitzungen und Schweigepflicht

Der Personalrat hat der Frauenbeauftragten bei der Behandlung von Angelegenheiten, die ihre Aufgaben nach § 20 SächsFFG betreffen, Gelegenheit zur Teilnahme an den Sitzungen zu geben (§ 41 Abs. 3 SächsPersVG n. F.). Dies erschien einigen Personalräten mit ihrer nach § 10 SächsPersVG bestehenden Schweigepflicht unvereinbar.

Obwohl weder das Sächsische Personalvertretungsgesetz noch das Sächsische Frauenförderungsgesetz spezialgesetzliche Vorschriften enthalten, die eine Durch-

brechung der Schweigepflicht bei der Teilnahme an gemeinsamen Sitzungen ausdrücklich legitimieren, ergibt sich aus der Teilnahmeberechtigung eine Durchbrechung der Schweigepflicht in den Personalratssitzungen bezüglich der Frauenförderung. Dies hat mir das SMI in einer Stellungnahme mitgeteilt und dazu folgende Begründung gegeben:

„Dem Wortlaut der Vorschrift zufolge sind die Personalratsmitglieder nur gegenüber den übrigen Mitgliedern der Personalvertretung von ihrer Schweigepflicht befreit. Der Jugend- und Auszubildendenvertretung, der Schwerbehindertenvertretung, dem Vertrauensmann der Zivildienstleistenden oder der Frauenbeauftragten gegenüber hätten die Personalratsmitglieder demgegenüber Stillschweigen zu bewahren.

Um jedoch den für die Willensbildung innerhalb der Personalvertretung erforderlichen offenen Meinungsaustausch zu ermöglichen, entfällt die Verschwiegenheitspflicht abweichend vom Wortlaut der Vorschrift für die verschiedenen Vertretungsrichtungen in ihren untereinander bestehenden Beziehungen, soweit es sich um Vorgänge handelt, die Gegenstand der Zusammenarbeit dieser verschiedenen Vertretungsorgane sind. Obwohl dies nicht ausdrücklich geregelt ist, muss im Rahmen der gesetzlich gebotenen Zusammenarbeit die Schweigepflicht auch gegenüber der Schwerbehindertenvertretung als aufgehoben angesehen werden, da sich andernfalls die Teilnahme der Schwerbehindertenvertretung an den Personalratssitzungen (§ 41 Abs. 1 SächsPersVG) sowie die nach § 73 Abs. 1 Nr. 4 SächsPersVG gebotene Zusammenarbeit mit der Personalvertretung nicht realisieren ließe (vgl. Fischer/Goeres, GKÖD V, K § 10 Rdnr. 14).

Im Hinblick auf das in § 41 Abs. 3 SächsPersVG genannte Teilnahmerecht der Frauenbeauftragten und auf die Regelung des § 73 Abs. 1 Nr. 6 SächsPersVG müssen die o. a. Erwägungen auch für die Frauenbeauftragte gelten, so dass dieser gegenüber die Schweigepflicht der Personalratsmitglieder ebenfalls als aufgehoben anzusehen ist."

Dem ist nichts hinzuzufügen.

5.2.2 Darf die Frauenbeauftragte auch an Personalratssitzungen teilnehmen, soweit Personaleinzelfälle behandelt werden, die ausschließlich männliche Beschäftigte betreffen?

Diese Frage beschäftigte einige Personalvertretungen; denn nach der Änderung des Sächsischen Personalvertretungsgesetzes im Jahr 1998 ist der Frauenbeauftragten bei der Behandlung von Angelegenheiten, die *ihre* Aufgaben nach § 20 SächsFFG betreffen, Gelegenheit zur Teilnahme an Personalratssitzungen zu geben (§ 41 Abs. 3 SächsPersVG).

Dazu habe ich mich wie folgt geäußert:

Bei Personaleinzelfällen, die *ausschließlich* männliche Beschäftigte betreffen, hat sie kein Teilnahmerecht. Allerdings muss dieses „ausschließlich" kritisch hinterfragt

werden. Manche Angelegenheit, die auf den ersten Blick nur männliche Beschäftigte betrifft, hat bei näherem Hinsehen durchaus Auswirkungen auf die Gleichstellung der weiblichen Beschäftigten oder auf ihre berufliche Situation. Dies muss von Fall zu Fall vom Personalrat geklärt werden. In schwierigen Fällen sollte dazu die Frauenbeauftragte - selbstverständlich abstrakt - gehört werden.

5.3 Einwohnermeldewesen

5.3.1 Rechtliche Entwicklung: Entwurf einer Ersten Verordnung des Sächsischen Staatsministeriums des Innern zur Durchführung des Sächsischen Meldegesetzes (Meldevordruckverordnung - MVVO)

Durch das Gesetz zur Änderung des Sächsischen Meldegesetzes und des Sächsischen Datenschutzgesetzes vom 7. April 1997 wurden die Bestimmungen des SächsMG über die Erhebung von personenbezogenen Daten bei der An-, Ab- oder Ummeldung geändert. Die umfangreichen Änderungen machen eine Neufassung der Meldevordruckverordnung erforderlich.

Aus datenschutzrechtlicher Sicht habe ich mich insbesondere zu § 4 Abs. 2 MVVO-Entwurf geäußert, wo es heißt: „*Daten, die nach § 6 Abs. 2 SächsMG erhoben wurden, sind nach deren Übermittlung bis zur Vernichtung der Meldescheine nicht mehr zu verarbeiten.*“

§ 6 Abs. 2 SächsMG lautet:

„*Außer den in Absatz 1 genannten Daten dürfen bei der Anmeldung nach § 10 Abs. 1 folgende Daten erhoben werden:*

1. *für Zwecke des Suchdienstes von den Einwohnern, die aus den in § 1 Abs. 2 Nr. 3 des Bundesvertriebenengesetzes in der Fassung der Bekanntmachung vom 2. Juni 1993 (BGBl. I S. 829), zuletzt geändert durch Artikel 25 des Gesetzes vom 26. Mai 1994 (BGBl. I S. 1014, 1060) bezeichneten Gebieten stammen, die Anschrift vom 1. September 1939,*
2. *soweit eine gesetzlich angeordnete statistische Erhebung dies erfordert, die rechtliche Zugehörigkeit zu einer privat-rechtlichen Religionsgesellschaft,*
3. *für die Anforderung des Familienbuches die Tatsache, daß ein Familienbuch auf Antrag angelegt wurde.*

Die Meldebehörden dürfen diese Daten nur so lange speichern, wie dies zur ordnungsgemäßen Übermittlung der Daten erforderlich ist.“

Dem SMI und dem Normprüfungsausschuss im SMJus habe ich deshalb mitgeteilt, dass die in § 4 Abs. 2 MVVO-Entwurf getroffene Regelung im Widerspruch zum eindeutigen Wortlaut des § 6 Abs. 2 letzer Satz SächsMG steht, wonach die Meldebehörden die „Durchlaufdaten“ nur so lange speichern dürfen, wie dies zur ordnungsgemäßen Übermittlung der Daten erforderlich ist. D. h. nach erfolgter Datenübermittlung besteht keine Erforderlichkeit mehr, die Daten weiterhin vorzuhalten; sie sind zu löschen.

Auch §§ 23 Abs. 1 Nr. 3, 26 Abs. 1 Nr. 2 SächsMG bestimmen, dass die Meldebehörde gespeicherte Daten zu löschen hat, wenn ihre Kenntnis zur Erfüllung der der Meldebehörde obliegenden Aufgaben nicht mehr erforderlich ist. Eben dies ist nach erfolgter Übermittlung der „Durchlaufdaten" der Fall. Es liegt auch keine „besondere Art der Speicherung *im Melderegister*" vor, die eine Löschung nicht oder nur mit unverhältnismäßig hohem Aufwand zuließe. Die Meldescheine, auf denen sich die „Durchlaufdaten" befinden, sind grundsätzlich nicht Bestandteil des Melderegisters, so dass die Ausnahmeregelung des § 26 Abs. 5 SächsMG nicht greift.

§ 4 Abs. 2 MVVO-Entwurf ist in der vorliegenden Fassung demnach rechtswidrig.

Außerdem habe ich auf Unstimmigkeiten bei der Angabe der die Datenerhebung rechtfertigenden Rechtsgrundlagen in den Meldescheinvordrucken sowie in den Erläuterungen zum Ausfüllen der Meldescheine hingewiesen. Während nämlich auf den Meldevordrucken als Rechtsgrundlagen für die Erhebung der Meldedaten auf §§ 5, 6 SächsMG verwiesen wird, heißt es in den Erläuterungen zum Ausfüllen der Meldescheine: „Rechtsgrundlage für den Umfang der zu erhebenden Daten sind die §§ 10 und 13 SächsMG".

Wie bereits in früheren Stellungnahmen habe ich empfohlen, sowohl auf den Meldescheinen als auch in den Erläuterungen alle vier Rechtsgrundlagen anzugeben.

Es bleibt abzuwarten, ob meine Stellungnahme beim Erlass der MVVO berücksichtigt wird.

5.3.2 Meldedatenübermittlung an die Bürgermeister der Verbandsgemeinden

Einem Verwaltungsverband wurde von den Verbandsgemeinden u. a. das Meldewesen übertragen. Die Bürgermeister der Verbandsgemeinden verlangten (regelmäßig) Daten der Zuzüge, Wegzüge, Sterbefälle bzw. eine komplette Einwohnerliste. Als Begründung gaben die Bürgermeister an, sie wollen wissen, wer in ihrer Gemeinde wohnt, um beispielsweise Auskünfte erteilen zu können.

Diese Auskunftsbegehren habe ich wie folgt bewertet:

Eine Übermittlung der in § 29 SächsMG aufgeführten Daten darf nur erfolgen, wenn dies zur Erfüllung der Aufgaben der Meldebehörde - also des Verwaltungsverbandes - oder der Datenempfänger (Bürgermeister) *erforderlich* ist. Die Bürgermeister der Verbandsgemeinden dürfen deshalb von der Meldebehörde nur die Einwohnerdaten verlangen, die sie zu ihrer Aufgabenerfüllung benötigen. Da es ausschließlich Aufgabe der Meldebehörde (und nicht der Bürgermeister) ist, das Melderegister zu führen, kommt die Überlassung einer Kopie des kompletten Melderegisters (z. B. in Listenform, auf Diskette) an die Bürgermeister grundsätzlich nicht in Betracht, es sei denn, sie würden konkret angeben, für welche Aufgabe die Meldedaten sämtlicher Einwohner ständig erforderlich sind. Die von den Bürgermeistern beabsichtigten gelegentlichen Auskunftserteilungen rechtfertigen jedenfalls die Übermittlung der

Meldedaten nicht, zumal für Melderegisterauskünfte gemäß § 1 Abs. 1 Satz 2 SächsMG ausschließlich die Meldebehörde zuständig ist. Auch eine regelmäßige Meldedatenübermittlung der Veränderungen (Zuzüge, Wegzüge, Sterbefälle, Eheschließungen, Geburten) scheitert an §§ 29 Abs. 5 i. V. m. 36 Nr. 4 SächsMG, weil diese Fälle nicht in der Sächsischen Meldedatenübermittlungsverordnung geregelt wurden.

Es dürfte vielfach genügen, die Bürgermeister anlassbezogen mit Namen, Doktorgrad und Anschriften (ggf. Alter) von Personengruppen (z. B. aller Senioren zwecks Einladung zu Altenveranstaltungen) zu versorgen. Für jeden Fall einer Datenübermittlung an die Bürgermeister gilt der Zweckbindungsgrundsatz nach § 29 Abs. 6 SächsMG. Sie tragen demnach auch die Verantwortung dafür, dass die ihnen übermittelten Daten nur zu ihrer Aufgabenerfüllung verwendet und datenschutzgerecht behandelt werden.

5.4 Personenstandswesen

In diesem Jahr nicht belegt.

5.5 Kommunale Selbstverwaltung

5.5.1 Kommunales Informationsnetz Sachsen KIN-S - Präsentation von Beschäftigtendaten im Internet und im Intranet

Im Herbst 1998 erfuhr ich von der Existenz des KIN-S und dass darin behördliche Telefonverzeichnisse und personenbezogene Organigramme, also Beschäftigtendaten i. S. v. § 31 SächsDSG, §§ 117 ff. SächsBG sowohl im *Intranet* als auch im *Internet* präsentiert werden können. Dem SSG und den kommunalen Datenverarbeitungszweckverbänden teilte ich mit, dass nach § 31 Abs. 1 SächsDSG sächsische öffentliche Stellen Daten von Beschäftigten nur verarbeiten dürfen, soweit dies zur Eingehung, Durchführung oder Beendigung des Dienst- oder Arbeitsverhältnisses oder zur Durchführung organisatorischer, personeller und sozialer Maßnahmen, insbesondere auch zu Zwecken der Personalplanung und des Personaleinsatzes *erforderlich* ist oder ein Gesetz, ein Tarifvertrag oder eine Dienstvereinbarung dies vorsieht (ähnlich auch § 117 Abs. 4 SächsBG).
Mögen auch behördliche Telefonverzeichnisse und Organigramme für den *internen* Dienstgebrauch erforderlich sein, so stößt ihre Veröffentlichung, insbesondere im Internet, an datenschutzrechtliche Grenzen.

Die Übermittlung von Beschäftigtendaten an Personen oder Stellen *außerhalb* des öffentlichen Bereichs ist gemäß § 31 Abs. 2 SächsDSG (ähnlich § 121 SächsBG) nur auf gesetzlicher Grundlage oder mit Einwilligung der Betroffenen zulässig. Die Behörden haben allerdings auch bei Vorliegen der Einwilligung stets den datenschutzrechtlichen Erforderlichkeitsgrundsatz zu beachten. So muss jede Form der Datenverarbeitung für die rechtmäßige Aufgabenerfüllung der öffentlichen Stellen *erforderlich* sein. Ein Einstellen der Beschäftigtendaten ins *Internet*, also

einer weltweiten Präsentation von Namen, behördlichen Anschriften, Telefonnummern usw. ist grundsätzlich für die in § 31 Abs. 1 SächsDSG genannten Aufgaben und Zwecke nicht erforderlich. Der Gesetzesvorbehalt des § 31 Abs. 2 SächsDSG lässt auch „Serviceleistungen“ aus Gründen der Bürgerfreundlichkeit grundsätzlich nicht zu. Allenfalls käme eine Veröffentlichung der Daten von Beschäftigten in herausgehobener Position (Bürgermeister, Dezernenten, Amtsleiter, Referatsleiter) in den Netzen (im behördeninternen Intranet *ohne*, im weltweit zugänglichen Internet, jedoch im Hinblick auf § 31 Abs. 2 SächsDSG nur *mit* Einwilligung) in Betracht. Allerdings dürfte eine Übermittlung der Daten der übrigen Beschäftigten (auch mit deren Einwilligung) an Private bzw. die Veröffentlichung nur dann erfolgen, wenn es zur Erfüllung der in § 31 Abs. 1 SächsDSG genannten Aufgaben, Zwecke und sonstigen Voraussetzungen *erforderlich* wäre. Dies ist bei Präsentationen in den Netzen ersichtlich nicht der Fall.

Der Grundsatz der Erforderlichkeit ist selbstverständlich auch bei einem Einstellen der Beschäftigtendaten ins *Intranet*, also einem geschlossenen Informationskreis zwischen Datenverarbeitungszweckverband und den angeschlossenen Kommunen, zu beachten. So kann es zwar ausgesprochen sinnvoll (erforderlich) sein, die Ansprechpartner im Zweckverband (oder im SSG), deren jeweiliges Sachgebiet (z. B. Einwohnerwesen, Personalwesen, Haushaltskassen- und Rechnungswesen - HKR) sowie deren dienstliche Telefonnummern für die Verbandsgemeinden jederzeit abrufbar ins Intranet zu stellen. Nicht erforderlich und damit unzulässig wäre es jedoch, wenn sich alle Verbandsgemeinden gleichermaßen im Intranet präsentieren würden (die Beschäftigtendaten z. B. der Stadt Görlitz gehen die anderen sächsischen Gemeinden grundsätzlich nichts an).

Schließlich - und das gilt für jede Form der automatisierten Verarbeitung von Beschäftigtendaten - ist stets § 31 Abs. 7 SächsDSG zu beachten, wonach sie nur im Benehmen mit dem Sächsischen Datenschutzbeauftragten eingeführt, angewendet, geändert oder erweitert werden darf. Mir scheint, dass vorstehende Gesichtspunkte bei der Konzeption des KIN-S nicht im erforderlichen Maße von allen Beteiligten (SSG, Datenverarbeitungszweckverbände, Verbandsgemeinden) beachtet wurden.

Über den Entwicklungs-/Verfahrensstand des KIN-S werde ich mich laufend informieren. Meine Erkenntnisse sowie meine rechtliche Bewertung werde ich den beteiligten Stellen mitteilen und bei Bedarf gemeinsam mit ihnen erörtern. Bis auf weiteres habe ich geraten, von der Veröffentlichung von Beschäftigtendaten im *Internet* gänzlich abzusehen und im *Intranet* mit der gebotenen Zurückhaltung vorzugehen.

5.5.2 Schutzwürdige Daten der Gemeindebediensteten

Ein Gemeinderatsmitglied fragte, ob es zulässig sei, dem Gemeinderat im Zusammenhang mit der Haushaltsdebatte über den Haushaltsansatz der Personalkosten folgende Beschäftigtendaten mitzuteilen:

Name, Geburtsdatum (Alter), beschäftigt seit, Tätigkeit, Verantwortlichkeiten, Qualifikation, Gehalts- bzw. Lohneinstufung.

Ich habe wie folgt geantwortet:

Im Hinblick auf Art. 33 SächsVerf, § 31 SächsDSG und §§ 117 ff. SächsBG (die Vorschriften des Sächsischen Beamtengesetzes gelten sinngemäß auch bei Angestellten) sind personenbezogene Beschäftigtendaten, insbesondere Personalaktendaten, vertraulich zu behandeln und dürfen wegen ihrer besonderen Schutzwürdigkeit im Rahmen der Gesetze nur im *erforderlichen* Maße verarbeitet, d. h. auch an den Gemeinderat übermittelt werden.

Nach § 28 Abs. 3 SächsGemO entscheidet der Gemeinderat im Einvernehmen mit dem Bürgermeister u. a. über die Ernennung, Höhergruppierung und Entlassung der Gemeindebediensteten, also im Einzelfall über konkrete Personalmaßnahmen. Dabei ist das Recht auf informationelle Selbstbestimmung der Gemeindebediensteten zu beachten. Gleichzeitig ist aber auch dem Informationsbedürfnis des Gemeinderates Rechnung zu tragen. Denn nur ein ausreichend informierter Gemeinderat kann richtige Entscheidungen treffen. Das bedeutet, dass dem Gemeinderat personenbezogene Beschäftigtendaten in dem Umfang mitgeteilt werden dürfen, der zur Behandlung der konkreten Personalmaßnahme und Beschlussfassung *erforderlich* ist.

Diese Begrenzung der Daten auf das erforderliche Maß gilt umso mehr für Beratungsgegenstände, die nichts mit einer konkreten Personalmaßnahme zu tun haben. Insbesondere vermag ich nicht zu erkennen, weshalb die oben aufgezählten Beschäftigtendaten für die Haushaltsdebatte zum Haushaltsansatz der Personalkosten erforderlich sein sollen. Hier reicht nach meinem Dafürhalten der kommunale Stellenplan (§§ 63, 75 Abs. 2 SächsGemO) - ohne Namensnennung - völlig aus. Dies gebieten schon die Öffentlichkeitsgrundsätze der §§ 37 Abs. 1, 76 Abs. 4 SächsGemO. Die oben aufgeführten Beschäftigtendaten haben aber in öffentlichen Gemeinderatssitzungen nichts verloren.

Eine andere Frage ist es, wenn der Gemeinderat konkrete Personalbewirtschaftungsvorhaben beraten will, z. B. über Entlassungen oder „Freisetzungen“ (ein Unwort) entscheiden will. Dann muss er die konkreten Daten der in Betracht kommenden Bediensteten kennen (einschließlich Dienstalter, Lebensalter und Zahl der unterhaltsberechtigten Kinder).

5.5.3 Beanstandung eines Bürgermeisters wegen unzulässiger Übermittlung von Personaldaten an einen Investor

Ein Bürgermeister hatte einem an der Übernahme eines kommunalen Eigenbetriebs interessierten Investor im Zuge der Verhandlungen eine Namensliste aller dort Beschäftigten mit deren Personalaktendaten übergeben. Dies war eine unzulässige Datenübermittlung, die ich beanstandet habe.

Der Bürgermeister ist gemäß § 11 Abs. 1 SächsEigBG Dienstvorgesetzter und oberste Dienstbehörde der beim Eigenbetrieb Beschäftigten.

Nach § 31 Abs. 2 SächsDSG „ist eine Übermittlung der Daten von Beschäftigten an Personen oder Stellen außerhalb des öffentlichen Bereiches nur auf gesetzlicher

Grundlage oder mit *Einwilligung* der Betroffenen zulässig. Dies gilt auch für Datenübermittlungen an einen künftigen Dienstherrn oder Arbeitgeber des Betroffenen."

Weder die Einwilligung der Beschäftigten noch eine die Datenübermittlung erlaubende Rechtsvorschrift lagen hier vor. Die Datenübermittlung war rechtswidrig, was gemäß § 32 Abs. 1 Nr. 1a SächsDSG als Ordnungswidrigkeit geahndet werden kann.

Der Bürgermeister rechtfertigte sein Handeln damit, dass der Investor den Arbeitskräftebestand vorab kennen müsse. Bei einer Nichteinwilligung einzelner Mitarbeiter erhöhe sich dessen Risiko, so dass er möglicherweise von seinem Kaufvorhaben Abstand nehme, was letztlich den Erhalt der Arbeitsplätze gefährde.

Zutreffend ist, dass die Entscheidung eines Investors nicht zuletzt von der Kenntnis des zu übernehmenden Personalbestands abhängig ist. Das für die Kaufentscheidung des Investors relevante Datenmaterial hätte jedoch in anonymisierter Form zur Verfügung gestellt werden müssen (z. B. die *Anzahl* der in den einzelnen Vergütungsgruppen beschäftigten Personen, *Anzahl* der sich in Erziehungsurlaub oder Mutterschutz befindenden Beschäftigten). Das Informationsbedürfnis des Investors wäre dadurch nicht beeinträchtigt worden.

Die Motive einer Datenübermittlung, also die „gute" oder „schlechte" Absicht, ist für die Zulässigkeitsprüfung einer Datenverarbeitung unerheblich.

Die rechtswidrig übersandten Listen sind zurückgefordet und vernichtet worden.

5.5.4 Mitteilungspflicht von Bediensteten im öffentlichen Dienst bei Verlust der Fahrerlaubnis

Der Datenschutzbeauftragte eines Landratsamts übersandte mir den Entwurf einer Fuhrparkordnung zur datenschutzrechtlichen Überprüfung, der vom Wortlaut her sämtliche Bedienstete des Landratsamts verpflichten sollte, den Verlust der Fahrerlaubnis (z. B. Entzug der Fahrerlaubnis) dem Dienststellenleiter zu melden. Somit wären auch solche Bedienstete zur Mitteilung verpflichtet, die nie oder äußerst selten Dienstfahrzeuge führen.

Dem Landratsamt teilte ich mit, dass ich eine solche generelle Verpflichtung aller Bediensteten mangels Erforderlichkeit für unzulässig halte. Zulässig wäre z. B. eine Regelung, die vorsieht, dass der Bedienstete, der mit dem Dienstfahrzeug eine Dienstreise durchführen will, auf dem Dienstreiseantrag den Besitz einer gültigen Fahrerlaubnis versichert, die er ggf. vor Fahrtantritt vorzuzeigen hat.

5.5.5 Veröffentlichung von Grundeigentümerdaten im Rahmen der Globalberechnung von grundstücksbezogenen Kommunalabgaben

Eine Gemeinde hat ihrer Abwassersatzung ein komplettes Grundeigentümerverzeichnis als Anlage beigefügt und je ein Exemplar an alle Haushalte verteilt. Diese Veröffentlichung/Übermittlung war mit § 15 SächsDSG nicht zu vereinbaren.

Von der kommunalen Beratungsstelle im RP Dresden, an die sich die von mir beanstandete Gemeinde gewandt hatte, erfuhr ich, dass es zumindest in kleinen Gemeinden nicht unüblich sei, die entsprechende Satzung im Falle von beabsichtigter Globalberechnung grundstücksbezogener Kommunalabgaben *einschließlich eines Grundeigentümerverzeichnisses* öffentlich auszulegen.

Meines Wissens liegen einer Globalberechnung stets die Herstellungskosten und die (Gesamt-)Grundstücksfläche als Verteilermaßstab zugrunde. Nur diese Angaben sind mit der Satzung öffentlich auszulegen, *personenbezogene* Grundstücksinformationen hingegen nicht (dem Schutz von Grundeigentümerdaten kommt im Hinblick auf §§ 30, 31 Abs. 3 AO ein hoher Stellenwert zu).

Ich habe das SMI, den SSG und den SLT gebeten, den sächsischen Kommunalbereich zu unterrichten, damit künftig personenbezogene Grundeigentümerverzeichnisse nicht mehr veröffentlicht werden. Der SLT hat inzwischen ein Schreiben des SMI, in dem meine Rechtsauffassung uneingeschränkt geteilt wird, den Landratsämtern zugeleitet.

5.5.6 Weitergabe personenbezogener Daten an Ortschronisten zur Erstellung eines „Heimatbuches“

Ein Landratsamt fragte, unter welchen Voraussetzungen personenbezogene Daten an Ortschronisten zur Erstellung eines „Heimatbuches“ herausgegeben werden dürfen.

Wie bereits aus 4/5.5.9 ersichtlich, müssen die Ortschronisten ordnungsgemäß nach §§ 17 Abs. 2 SächsGemO, 15 Abs. 2 SächsLkrO für das Ehrenamt „Ortschronist“ bestellt sein, sofern sie nicht hauptamtlich tätig sind.

Insbesondere sind Datenerhebungen bei betroffenen Bürgern nur auf freiwilliger Basis zulässig (§ 11 Abs. 2 SächsDSG). Die später folgende Veröffentlichung der personenbezogenen Daten im „Heimatbuch“ ist von der Einwilligung der Betroffenen abhängig (§ 4 Abs. 1 Nr. 2, Abs. 2 und 3 SächsDSG).

Der Umfang der von den Chronisten geforderten Daten, nämlich
- Geburten 1997 (Name, Adresse)
- Sterbefälle 1997 (Name, Datum, Adresse)
- Zuzüge 1997 (Name, Datum, Zuzugsadresse)
- Wegzüge 1997 (Name, Datum, Wegzugsort)
- Liste der Gewerbetreibenden

sprengt nach meinem Dafürhalten den Rahmen einer Chronik, die sich mit historisch Bedeutsamem, nicht aber mit aktuellen Einwohner- und Gewerbetreibenden-Daten befassen sollte und stößt - ohne die Einwilligung der Betroffenen - in der Tat auf datenschutzrechtliche Grenzen. Insbesondere aus 1/5.5.5 ist ersichtlich, dass die Gemeinden solche Daten (ohne Einwilligung) nicht in ihren Mitteilungsblättern veröffentlichen dürfen. Dieses Verbot kann und darf über den Umweg „Ortschronik“ nicht umgangen werden.

Da offensichtlich solche Informationen in den vergangenen Jahren bereits von den Ortschronisten gesammelt wurden, vermutlich ohne die Belange des Datenschutzes zu beachten, dürfte das in der Entstehung befindliche Heimatbuch insofern als problematisch anzusehen sein.

Ich habe gebeten, die Verantwortlichen auf diese Situation hinzuweisen und anheim gestellt, die erforderlichen schriftlichen Einwilligungen der Betroffenen noch vor dem Erscheinen des Heimatbuchs einzuholen. Eine Veröffentlichung personenbezogener Daten im Heimatbuch ohne Einwilligung ist jedenfalls unzulässig.

5.5.7 Vorkaufsrecht der Gemeinde - Behandlung im Gemeinderat

Im Zusammenhang mit der Ausübung des Vorkaufsrechts einer Gemeinde habe ich zur Wahrung der persönlichen Interessen der Betroffenen ein zweistufiges Verfahren empfohlen (siehe auch unter 8.5):

Zur Entscheidung über die Frage, *ob* die Gemeinde überhaupt von ihrem Vorkaufsrecht Gebrauch machen will, reicht es aus, wenn sie zunächst nur bestimmte Mindestangaben über die Art des Vertrages, die Vertragsparteien, die katastermäßige Bezeichnung und die Bebauung des Grundstücks vom jeweiligen Notar erhält.

Erst wenn die Gemeinde aufgrund dieser Mitteilung beabsichtigt, von ihrem Vorkaufsrecht tatsächlich Gebrauch zu machen, fordert sie vom Notar den vollständigen Kaufvertrag an. Sofern bei der Beratung im Gemeinderat Interna aus dem Kaufvertrag erörtert werden sollen, ist die Öffentlichkeit gemäß § 37 Abs. 1 Satz 1 SächsGemO auszuschließen. Die *Tatsache*, dass die Gemeinde für ein bestimmtes Grundstück von ihrem Vorkaufsrecht Gebrauch machen möchte, kann sodann in öffentlicher Sitzung beschlossen werden.

5.5.8 Abhören eines Tonbandmitschnitts einer Kreistagssitzung durch einen Kreisrat

Ein Kreisrat beantragte etliche Wochen nach der vorgesehenen vierwöchigen Einwendungsfrist, den Tonbandmitschnitt einer Kreistagssitzung abhören zu dürfen, was ihm verweigert wurde. Er wollte einen Redebeitrag des Landrates kontrollieren.

In der Geschäftsordnung des Kreistags ist u. a. geregelt, *dass es dem Schriftführer zur Erleichterung der Aufnahme der Niederschrift gestattet ist, für die Aufzeichnungen einen Tonträger zu verwenden*. Die Aufbewahrungszeit solcher Tonbandmitschnitte beträgt nach der Geschäftsordnung ein Jahr.

Dem Kreisrat musste ich mitteilen, dass es die Zweckbindung (Erleichterung der Aufnahme der Niederschrift) nicht gestattet, den Tonträger aus anderen Gründen als Einwendungen gegen die Niederschrift und schon gar nicht nach Verstreichen der vierwöchigen Einspruchsfrist abzuhören.

Dem Landratsamt habe ich empfohlen, die in der Geschäftsordnung vorgesehene einjährige Aufbewahrungsfrist drastisch zu verkürzen und die Tonbänder nach Verstreichen der Einwendungsfrist zu löschen.

5.5.9 Forderungen der öffentlichen Hand - Beauftragung eines Inkassounternehmens mit der Vorbereitung von Vollstreckungsmaßnahmen der Gemeinden

In 6/5.5.6 habe ich gegen eine Beauftragung eines privaten Inkassobüros mit Vollstreckungs- und Beitreibungsaufgaben erhebliche Vorbehalte geäußert.

Die Creditreform Dresden, der meine ablehnende Haltung wohl nicht sonderlich gefiel, versuchte über den Verband der Vereine Creditreform e. V. in Neuss am Rhein eine Meinungsänderung zu erreichen. Vergeblich!

Ich vermag nämlich nicht nachzuvollziehen, dass sächsische Gemeinden und Zweckverbände - wie behauptet - *verstärkt* die Unterstützung privater spezialisierter Unternehmen im Bereich des Forderungsmanagements suchen sollen, zumal ich von den vom Verband der Vereine Creditreform e. V. angeführten erheblichen personellen Engpässen nichts weiß. Im Gegenteil: Ich entnehme der Presse, dass nach allgemeiner Auffassung der Personalstand in manchen Kommunen zu hoch ist.

1. *Öffentlich-rechtliche Forderungen*
   Nach meinem Dafürhalten sind die sächsischen Kommunalbehörden entgegen der Ansicht der Creditreform sehr wohl in der Lage, *öffentlich-rechtliche* Forderungen selbst zu vollstrecken oder durch eine leistungsstarke und sachkundige Vollstreckungsbehörde vollstrecken zu lassen. Eine Unterscheidung zwischen sensiblen und weniger sensiblen/nicht-sensiblen Bereichen lässt das für die Vollstreckung von Verwaltungsverfahren konzipierte Sächsische Verwaltungsvollstreckungsgesetz nicht zu. Soweit das Steuergeheimnis und andere besondere Geheimhaltungsvorschriften nicht greifen, haben die Beteiligten an einem Verwaltungsverfahren nach § 30 VwVfG Anspruch darauf, dass ihre Geheimnisse, insbesondere die zum persönlichen Lebensbereich gehörenden Geheimnisse sowie Betriebs- und Geschäftsgeheimnisse, von der Behörde nicht unbefugt offenbart werden. Einen Gestaltungsspielraum bei Aufgabenübertragung auf die Creditreform (z. B. Müll- und Wassergebühren) sehe ich deshalb nicht. Dies gilt auch für die Übertragung von vor- und/oder nachbereiteten Teilaufgaben der Vollstreckungsbehörde auf Private. Zitat aus dem Aufsatz „Möglichkeiten und Grenzen der Übertragung von Aufgaben der kommunalen Vollstreckungsbehörden auf Dritte“ von Helmut Hagemann (Kommunalkassenzeitschrift Nr. 5 vom Mai 1996):

   „Die Vollstreckung öffentlich-rechtlicher Kommunalforderungen ist durch die Ländervollstreckungsgesetze als Verwaltungsverfahren ausgestaltet worden. Die Normen lassen ein Ausweichen in den zivilrechtlichen Bereich nicht zu. Eine solche Vorgehensweise macht auch keinen Sinn. Öffentlich-rechtliche Forderungen sind vollstreckbar, wenn der Schuldner zur Leistung durch Bescheid aufgefor-

dert wurde, die Forderung fällig ist, der Schuldner gemahnt wurde, die Mahn- und Schonfrist abgelaufen ist und die Vollziehbarkeit (§ 80 VwGO) gegeben ist. Die Vollstreckungsbehörde kann nunmehr die Forderungen mit dem gesamten Instrumentarium des Verwaltungsvollstreckungsrechtes zwangsweise beitreiben. Die Zwischenschaltung eines Inkassounternehmens, das keinerlei Sanktionsrechte gegenüber dem Schuldner hat, ist dagegen ineffektiv. Die Möglichkeit des Vorgehens des Inkassogewerbes gegen Schuldner ist Mixtur aus Psychologie, Taktik und Beharrlichkeit. Es besteht auch nicht die Möglichkeit, die Kosten des Inkasso-Dienstes vom Schuldner zu verlangen, da hierfür keine Ermächtigungsnorm vorhanden ist. Die Einschaltung von Inkassodiensten dürfte schließlich auch an den Bestimmungen des Steuer- und Abgabengeheimnisses (§ 30 AO) und des Datenschutzes scheitern."

2. *Privatrechtliche Forderungen*
   Auch wenn *privatrechtliche* Forderungen der kommunalen Gebietskörperschaften hinsichtlich ihres Einzugs durch Dritte sicherlich nicht den strengen Restriktionen öffentlich-rechtlicher Geldforderungen unterworfen sind, halte ich die Einschaltung eines Inkassounternehmens für äußerst problematisch.

   Soweit ich weiß, verfügen die sächsischen Gemeinden durch ihre Erfahrungen aus der Verwaltungsvollstreckung und aufgrund der flächendeckenden Infrastruktur mit Innen- und Außendienst über gute Voraussetzungen, um die privatrechtlichen Forderungen *selbst* wirkungsvoll außergerichtlich geltend zu machen. Die Schuldnerdaten bleiben dann „im Haus".

   Auch unter wirtschaftlichen Aspekten macht das Eigeninkasso der Kommunalbehörden Sinn (Einsparung von Erfolgshonoraren), so dass es der Inanspruchnahme eines Inkassounternehmens aus Effizienz- und Wirtschaftlichkeitsgründen vorzuziehen ist.

Ich habe das SMI sowie den SSG entsprechend unterrichtet und bislang keinen Widerspruch zu meinen Ausführungen erhalten. Im Gegenteil: Der SSG hat inzwischen dankenswerterweise meine Äußerungen zur Leistungsfähigkeit der sächsischen kommunalen Vollstreckungsbehörden voll bestätigt und ein entsprechendes Mitgliederrundschreiben verfasst.

5.5.10 Bekanntgabe von Interessentendaten durch die Fremdenverkehrsgemeinden an örtliche Beherbergungsbetriebe

Im Rahmen der Fremdenverkehrsförderung ist es üblich, dass die Fremdenverkehrsgemeinden und Kurorte für sich auch überregionale Werbung z. B. in Fremdenverkehrsbroschüren, in überregionalen Zeitschriften und durch Präsentation im Internet betreiben. Interessenten erhalten nach Kontaktaufnahme einschlägiges Prospektmaterial über die Vorzüge und Sehenswürdigkeiten der Gemeinde und der Umgebung, aber auch über Kategorien und Preise der Übernachtungsmöglichkeiten übersandt. Verschiedene Hoteliers hätten gern die Adressen der Interessenten, um ihrerseits Direktwerbung zu betreiben und auf die Vorzüge ihres Beherbergungs-

betriebs sowie auf besondere Aktionen (z. B. „Schlemmerwochenende zum Sonderpreis“) hinzuweisen.

Datenschutzrechtlich habe ich die von den Hotelbetreibern gewünschten Datenübermittlungen wie folgt bewertet: Bei den von einigen Beherbergungsstätten gewünschten Informationen über Interessenten ist die Rechtmäßigkeit der Datenübermittlungen an § 15 SächsDSG zu messen. Insbesondere ist zu prüfen, ob der Empfänger ein berechtigtes Interesse (hierzu zählt jedes von der Rechtsordnung erlaubte, also auch ein wirtschaftliches Interesse) an der Kenntnis der zu übermittelnden Daten glaubhaft dargelegt hat *und* ob der Betroffene (Interessent) kein schutzwürdiges Interesse am Unterbleiben der Übermittlung hat (§ 15 Abs. 1 Nr. 2 SächsDSG). Um dies festzustellen, müssten die Gemeinden die Betroffenen *vor* der (evtl. beabsichtigten) Übermittlung anhören und nach (evtl. erfolgter) Übermittlung benachrichtigen (welche Daten wurden an wen übermittelt). Der dabei entstehende Verwaltungsaufwand dürfte jedenfalls bei der Vielzahl der Interessenten so beträchtlich sein, dass ich den Gemeinden nicht unbedingt zu solchen Übermittlungsaktionen raten kann. Ich habe auch zu bedenken gegeben, was auf die Gemeinden und die Betroffenen zukommt, wenn aus Wettbewerbsgründen sämtliche in Frage kommenden Beherbergungsstätten solche Informationen wünschen.

Es wäre denkbar, dass sich die Interessenten durch eine daraufhin einsetzende Werbeflut in ihrem schutzwürdigen Belangen beeinträchtigt fühlen, so dass die Entscheidung der Gemeinden (Datenübermittlung ja oder nein) zu Gunsten der Betroffenen ausfallen sollte. Allenfalls käme eine Datenübermittlung an die Beherbergungsbetriebe mit (vorheriger) schriftlicher Einwilligung der Betroffenen in Betracht (vgl. § 4 Abs. 1 Nr. 2, Abs. 2 und 3 SächsDSG). Aber auch hier wäre der Verwaltungsaufwand beträchtlich.

5.5.11 Auslagerung von kommunalem Registraturgut

Ein sächsisches Unternehmen beabsichtigte, den Gemeindeverwaltungen im Freistaat, die unter Raumnot leiden, die Übernahme und Aufbewahrung des kommunalen Registraturbestandes anzubieten.

Das Angebot reichte vom einfachen Einlagern in Regalen einschließlich automatisierter Registrierung zum Auffinden des Registraturguts bis zu Datenverarbeitungsschritten, wie Scannen, Mikroverfilmung, automatisierter Fristenüberwachung mit anschließender Vernichtung/ Löschung von Akten und sonstigen Datenträgern.

Um dem Unternehmen meine mit der obersten Kommunalaufsichtsbehörde abgestimmte datenschutzrechtliche Einschätzung mitteilen zu können, habe ich das SMI auf folgende Problematik hingewiesen und mit dem Ziel um Stellungnahme gebeten, unnötige Werbekampagnen im sächsischen Kommunalbereich von vornherein zu vermeiden:

Im Hinblick auf die im Angebot enthaltenen Datenverarbeitungsschritte (Scannen, Mikroverfilmen, Vernichtung/Löschung von Datenträgern) kommt nach meinem

Dafürhalten § 7 SächsDSG bei einer Auftragsvergabe zur Anwendung (siehe auch meine Bekanntmachung zur Datenverarbeitung im Auftrag vom 3. November 1993 - SächsABl. S. 1304, geändert durch Bekanntmachung vom 29. Juni 1994 - SächsABl. S. 979).

Aber auch dann, wenn vorstehende Leistungen nicht in Anspruch genommen werden, die Aktenbestände also lediglich in Regalen deponiert und zur Wiederauffindung in einem automatisierten Verfahren (ohne Personenbezug) registriert werden sollen, sind datenschutzrechtliche Gesichtspunkte außerordentlich bedeutsam. Mit der Übergabe der (kommunalen) Aktenbestände werden nämlich schützenswerte Inhalte offenbart. Bedenken habe ich deshalb gegen eine Auslagerung und der damit verbundenen Offenbarung von sensiblen Datenbeständen, z. B. aus den kommunalen Steuerämtern (§ 30 AO - Steuergeheimnis), aus dem Sozialbereich (§ 35 SGB I - Sozialgeheimnis), aus dem kommunalen Gesundheitsbereich (§ 203 StGB, § 33 SächsKHG - Patientengeheimnis), aus dem Personalbereich (§§ 117 ff. SächsBG - Vertraulichkeit der Personalakten), aber auch von Vollstreckungsangelegenheiten und sonstigen Verwaltungsverfahren, die nach § 30 VwVfG geheim zu halten sind. Unterlagen aus den Standesämtern sind im Hinblick auf §§ 31, 43, 46 Abs. 1 Satz 1 DA per se von einer Auslagerung ausgeschlossen.

Das SMI wollte sich wegen der Vielschichtigkeit nicht abschließend festlegen, ist aber - so wie ich - in konkreten Einzelfällen bereit, die an dem Angebot interessierten Gemeinden individuell zu beraten.

5.5.12 Outsourcing der kommunalen Datenverarbeitung der Stadt Leipzig

Der Presse habe ich entnommen, dass die Stadt Leipzig ein Outsourcing der kommunalen Datenverarbeitung plant.

Unter Hinweis auf § 25 SächsDSG habe ich um Unterrichtung über die Einzelheiten gebeten. Gleichzeitig habe ich zu bedenken gegeben, dass eine Privatisierung der kommunalen Datenverarbeitung insbesondere im Hinblick auf § 30 AO, §§ 117 ff. SächsBG, § 3 SächsMG problematisch, wenn nicht gar unzulässig ist.

Von Bedeutung ist dabei, dass das Rechenzentrum der Stadt Leipzig nicht nur die städtische Datenverarbeitung erledigt, sondern auch als Auftragnehmer der sächsischen Datenverarbeitungszweckverbände die Datenverarbeitung der Verbandsgemeinden abwickelt.
Die Entwicklung werde ich kritisch beobachten. Die Stadt Leipzig hat mir im Dezember 1998 eine rechtzeitige Beteiligung zugesagt.

5.6 Baurecht; Wohnungswesen

In diesem Jahr nicht belegt.

5.7 Statistikwesen

5.7.1 Gesetz zur Durchführung der Erwerbsstatistik im Freistaat Sachsen

Am 20. Januar 1999 hat der Landtag den von der Staatsregierung eingebrachten Gesetzentwurf verabschiedet. Das Gesetz - kurz Sächsisches Erwerbsstatistikgesetz (SächsErwStatG) genannt - ordnet eine Statistik an, die es in Deutschland anderswo noch nicht gibt: Es wird in dichterer Folge als derzeit beim Mikrozensus (Bundesstatistik), nämlich dreimal jährlich, fast ausschließlich mit Auskunftspflicht, ein umfangreiches, über das des Mikrozensus hinausgehendes Erhebungsprogramm durchgeführt. Es versucht, die Erwerbstätigkeit (und zwar in ihrem Verlauf seit 1989) und die Einkommenssituation, dabei insbesondere die Arbeitslosigkeit und überhaupt sozialrechtliche Gegebenheiten, ferner die Bildungssituation und auch ehrenamtliche Tätigkeiten, in unterschiedlich detaillierter Weise und unter Abbildung der Haushaltsgemeinschaft, zu erfassen. Die Stichprobengröße ist 0,5 v. H.

Ich bin von der Staatskanzlei von Anfang an an der Erarbeitung des Gesetzentwurfes beteiligt worden, und ich habe zur Gestaltung des Entwurfes im Einzelnen, insbesondere auch was die langen Aufzählungen von Erhebungsmerkmalen betrifft, aus denen das Gesetz hauptsächlich besteht, eine Menge beitragen können. Die Zusammenarbeit (SK, SMWA, SMI mit StaLA) kann ich nur als erfreulich bezeichnen.

Die grundlegende Frage, welche das Gesetz in datenschutzrechtlicher Hinsicht aufwirft, ist folgende: Verstößt es gegen das *Übermaßverbot*, ist es *unangemessen*, wenn zu statistischen Zwecken ein so genaues und dabei so weite Lebensbereiche einer Person erfassendes Bild zusammengestellt wird?
Das Bundesverfassungsgericht hat im Volkszählungsurteil (BVerfGE 65, 1, 53) von 1983 diese verfassungsrechtliche Grenze des Übermaßverbotes für das Statistikrecht mit den recht bildhaften Ausdrücken *Persönlichkeitsprofil, Totalabbild* und *menschenwürdewidriges Teilabbild der Persönlichkeit* umschrieben. Das Gericht hat im Mikrozensus-Beschluss von 1969 (BVerfGE 27, 1, 6 f.) dies genauer dahingehend bestimmt, dass Entwürdigung und Bedrohung des Selbstbestimmungsrechtes des Einzelnen durch die statistische Erfassung dort zu besorgen sind, „wo sie den Bereich menschlichen Eigenlebens erfasst, der von Natur aus Geheimnischarakter hat". „Wo dagegen", so das Bundesverfassungsgericht weiter, „die statistische Erhebung nur an das Verhalten des Menschen in der Außenwelt anknüpft, wird die menschliche Persönlichkeit von ihr in aller Regel noch nicht in ihrem unantastbaren Bereich privater Lebensgestaltung 'erfasst'. Das gilt jedenfalls dann, wenn diese Angaben durch die Anonymität ihrer Auswertung den Persönlichkeitsbezug verlieren."

Der öffentlichen Gewalt ist es zum Schutz von Menschenwürde und Selbstbestimmungsrecht des Einzelnen versagt, zur Offenlegung der Intimsphäre zu zwingen oder dazu, dem Staat Einsicht in einzelne Beziehungen zu gewähren, die der Außenwelt nicht zugänglich sind und deshalb von Natur aus 'Geheimnischarakter' haben (so BVerfGE a. a. O. S. 8).

Vor diesen Maßstäben, welche die verfassungsrechtlich gebotene Angemessenheit

konkretisieren, kann das Gesetz zur Durchführung der Erwerbsstatistik im Freistaat Sachsen bestehen.
Es ist ferner auch nicht zu erkennen und im Gesetzgebungsverfahren auch von den Kritikern des Entwurfes nicht dargetan worden, dass etwa einzelne Merkmale ungeeignet oder nicht erforderlich sind zur Erreichung dessen, was Zweck der Statistik ist: In zeitlich genauerer, insbesondere zeitnäherer Verfolgung der gerade in Sachsen rasanten Entwicklung seit dem Übergang von der Plan- zur Marktwirtschaft Näheres über die Verhältnisse im Land, was Erwerbs- und andere Arbeit, Einkommen, Ausbildung und Haushaltszusammensetzungen in ihren Zusammenhängen betrifft, zu wissen. Solch statistisches Wissen ist Bedingung der Planmäßigkeit des staatlichen Handelns (BVerfGE a. a. O. S. 7). Es schafft die für eine am Sozialstaatsprinzip ausgerichtete staatliche Politik unentbehrliche Handlungsgrundlage (BVerfGE 65, 1, 47 unter Berufung auf E 27, 1, 9).

Im Gegensatz zu dem, was aus einer anderen datenschutzrechtlichen 'Ecke' dazu im Gesetzgebungsverfahren zu hören war, habe ich von Anfang an die Auffassung vertreten, dass die dem Gesetz zugrunde liegende Grund-Konzeption verfassungsgemäß ist, nämlich nicht gegen das Angemessenheits-Gebot verstößt. Die datenschutzrechtlichen Bedenken werden die Landtagsdebatte - in der meine Stellungnahme weder bei Befürwortern noch bei Gegnern der Gesetzesvorlage zur Sprache gekommen ist - insofern überdauern, als, wie beim Mikrozensus, Auskunftspflichtige anfragen werden, ob denn die ihnen auferlegte Belastung rechtmäßig sei: Die Überzeugungsarbeit wird sich meine Behörde in der vom Mikrozensus gewohnten Weise mit dem Statistischen Landesamt teilen.

5.7.2 Mietspiegel: Darf der Bürgermeister die Erstellung aussetzen?

Gemäß § 2 Abs. 5 Satz 1 des Gesetzes zur Regelung der Miethöhe (MHG) sollen Gemeinden, soweit hierfür ein Bedürfnis besteht und dies mit einem für sie vertretbaren Aufwand möglich ist, Mietspiegel erstellen.
Die Erstellung eines empirischen Mietspiegels ist als Statistik im Rechtssinne anzusehen (vgl. 5/5.7.2). Rechtsgrundlage der Datenverarbeitung zum Zweck der Durchführung einer solchen Kommunalstatistik ist gemäß § 8 Abs. 1 SächsStatG eine Satzung.

Nach § 2 Abs. 5 Satz 3 MHG sollen Mietspiegel im Abstand von zwei Jahren der Marktentwicklung angepasst werden. Um dem gerecht zu werden, wollten Gemeinden die Regelung treffen, die Statistik regelmäßig im Abstand von zwei Jahren durchzuführen, dem Bürgermeister aber das Recht geben, die Durchführung auszusetzen, also anzuordnen, dass der Mietspiegel nicht angepasst wird, also keine Datenerhebung stattfindet, weil die Verhältnisse stabil geblieben sind.
Eine solche Regelung wäre unzulässig, da eine vom Gemeinderat wahrzunehmende Aufgabe unzulässigerweise auf den Bürgermeister delegiert würde:

Als Delegierung der Satzungsgewalt wäre die Regelung gesetzwidrig. Zuständig für den Erlass der Satzung (§ 8 Abs. 1 Satz 2 SächsStatG) ist gemäß § 28 Abs. 1 SächsGemO der Gemeinderat. Zwar darf der Gemeinderat bestimmte Angelegenheiten auf den Bürgermeister übertragen (vgl. §§ 28 Abs. 1, 53 Abs. 2 Satz 1 SächsGemO), jedoch ist eine solche Übertragung in den Fällen des § 53 Abs. 2 Satz 3

i. V. m. § 41 Abs. 2 SächsGemO ausgeschlossen. Nach § 41 Abs. 2 Nr. 3 SächsGemO darf die Beschlussfassung über Satzungen nicht auf den Bürgermeister übertragen werden.
Die Regelung wäre aber auch rechtswidrig, wenn sie den Sinn hätte, den Oberbürgermeister zu ermächtigen, durch Weisung die Durchführung der Statistik insgesamt oder die Erhebung einzelner Merkmale auszusetzen, die Periodizität zu verlängern, Erhebungstermine zu verschieben sowie den Kreis der zu Befragenden einzuschränken, wenn und soweit die Ergebnisse nicht mehr benötigt werden. Wie § 6 Abs. 7 SächsStatG, § 5 Abs. 4 BStatG zu entnehmen ist, verbietet es der Vorrang des Gesetzes (Gesetzesbindung der Verwaltung als Bindung an alle Rechtsvorschriften, also einschließlich der Satzung), kraft bloßer Verwaltungsentscheidung von einer Rechtsvorschrift, welche die Durchführung einer Statistik anordnet, abzuweichen.
Der Ausweg, statt die Satzungsgebungszuständigkeit zu übertragen oder ein Abweichen von der Satzung auf bloßer Weisungsgrundlage zu ermöglichen, den Bürgermeister zum Erlass einer Verordnung zu ermächtigen, ist verbaut:
Der bereits erwähnte § 41 Abs. 2 Nr. 3 SächsGemO behält die Beschlussfassung über „anderes Ortsrecht“ dem Gemeinderat vor.

Zur Aussetzung der Erstellung des Mietspiegels, und damit insbesondere der dafür nötigen Datensammlung, hat die Gemeinde mehrere Möglichkeiten:

1. Sie ordnet eine lediglich einmalige Mietspiegelerstellung an. Jede erneute Erstellung kann dann erneut durch Satzung angeordnet werden.
2. Die Satzung sieht eine mehrmalige regelmäßige Durchführung der Kommunalstatistik vor, die Aussetzung kann durch eine Änderungssatzung erfolgen.
3. Diejenige Satzung, in der die Mietspiegelerstellung sowie deren regelmäßige Anpassung angeordnet wird, regelt unter Beachtung des Bestimmtheitsgrundsatzes, unter welchen materiellen Voraussetzungen eine Aussetzung erfolgt. Hierbei darf die Befugnis, diese Voraussetzungen festzulegen oder ohne Voraussetzungen durch bloße Weisung auszusetzen, wie oben dargelegt, nicht auf den Bürgermeister übertragen werden.

In diesem Beispielfall ist unsere Rechtsordnung schon so kompliziert geworden, dass die Unterlassung einer Datenerhebung nur durch Rechtsvorschrift (hier: Satzung) angeordnet werden muss, weil das Unterlassen einer angeordneten Statistik etwas „Wesentliches“ ist. Ich kann nichts dafür.

5.7.3 Kommunalstatistiken: Grenzen der Vereinfachung

Eine sächsische Stadt wollte auf Satzungsgrundlage (vgl. § 8 Abs. 1 SächsStatG) ihre Einwohner „zu ausgewählten Themen der Stadtentwicklung“ befragen, um das Ergebnis bei der Entwicklung der „Stadtentwicklungskonzeption“ zu nutzen; sie beteiligte mich gemäß § 8 Abs. 3 SächsStatG.

Interessant war vor allem Folgendes: Die Stadt wollte - wie sich herausstellte aus Kostenersparnisgründen - die Befragung der Einwohner dadurch bewerkstelligen, dass sie jedem Exemplar des „Mitteilungsblattes“ der Stadt je zwei Fragebögen beilegte; vertrieben wird das Mitteilungsblatt durch Auslegen an verschiedenen Stellen der Stadt. Die ausgefüllten Fragebögen sollten dann in verschlossene Kästen

eingeworfen werden, die sich in Gebäuden der Stadtverwaltung, nichtstädtischen Behörden, einem Einkaufszentrum und an ähnlichen Örtlichkeiten befinden sollten.

Die Befragung wäre keineswegs von vornherein hinreichend anonym gewesen. Denn die Angabe der Straße, in welcher die Auskunftsperson wohnte, hätte zusammen mit etlichen anderen Angaben wie Altersgruppe, Anzahl der Personen im Haushalt und ausgeübte Tätigkeit eine Zuordnung zu einer bestimmten Person recht leicht gemacht.

Aus Gründen, die hier vernachlässigt werden können, lag es auf der Hand, dass der eine oder andere Einwohner der Stadt ein Interesse daran haben konnte, wie das Ergebnis der Befragung zu diesem oder jenem Thema sein würde. Auch für einen statistischen Laien sollte klar sein, dass eine solche statistische Erhebung ungeeignet ist, ein Zahlenergebnis zu bekommen, welches als Grundlage für eine verantwortbare Planung taugt: Interessierte hätten sich eine größere Zahl von Mitteilungsblättern bzw. Fragebögen besorgen und diese mit bestimmter Zweckbestimmung ausfüllen können.
Die Antwort, die ich auf meinen dahingehenden Einwand erhielt, bestärkte mich in meiner Einschätzung: Keine Erhebungsmethode, hieß es, sei zuverlässig (mit anderen Worten: ‘Alle Katzen sind grau!’), und man wolle ja erklärtermaßen nur „Tendenzen“ ermitteln, und aus denen lasse sich ‘direkt für Verwaltungshandeln nichts ableiten’.

Gleichwohl hat die Stadt dann in einem neuen Satzungsentwurf meinem Einwand Rechnung getragen, und zwar dadurch, dass zusätzlich Hilfsmerkmale (Name, Anschrift, Alter) erhoben werden sollten. Damit wäre die Korrektheit des Rücklaufes, also der Umstand, dass eine Auskunftsperson nicht mehr als einen Bogen abgibt, nachprüfbar gewesen - keineswegs eine paradoxe Folge meiner Kritik: Auch für die Datenverarbeitung gilt nicht selten, dass sie entweder ganz oder gar nicht durchgeführt zu werden hat.

In anderer Hinsicht freilich stellte sich mir auch bei dieser Erhebung eine gegenteilige Frage: Es ist mir weiterhin bei vielen Merkmalen, die Stadtplaner erheben wollen, ein Rätsel, warum sie wissen wollen, wie diese Merkmale mit dem Geschlecht, dem Alter und dem Einkommen sowie der Art der Teilnahme am Erwerbsleben (Merkmalsausprägungen u. a. Hausfrau, Arbeiter, Beamter, Vorruheständler) korreliert sind. Denn die Stadtplanung hat fast keinen Einfluss auf die diesbezügliche Zusammensetzung und Verteilung der Bevölkerung. (Dies ist sicherlich differenziert zu sehen, vgl. 6/5.7.5, S. 80 f.)

Die geplante Erhebung und der Satzungsentwurf wiesen noch andere datenschutzrechtliche Probleme auf - am Ende hat die Stadt auf die Erhebung, jedenfalls als amtliche Statistik, verzichtet. Ich wage zu vermuten: nicht zum Schaden der Stadtentwicklung.

5.7.4 Musterentwürfe für kommunale Fremdenverkehrsstatistiken

Die in 5/5.7.9 geschilderten Aktivitäten haben leider nicht verhindern können, dass im Jahr 1998 im ersten Heft des „Sachsenlandkuriers“, der Zeitschrift des SSG, ein

„Satzungsmuster Kurtaxe-Satzung“ veröffentlicht wurde, welches in § 8 Abs. 4 eine Regelung enthält, die zwar gegenüber vorhergehenden Vorstellungen schon verbessert ist, gleichwohl aber eindeutig gegen höherrangiges Recht verstößt.

Vorgesehen wird dort eine statistischen Zwecken dienende Erhebung von Kurgast-Daten. Das wäre eine erkennbar von der Kommune veranlasste und daher amtliche Statistik auch dann, wenn, wie in der mitveröffentlichten Entwurfs-Begründung angegeben, die Auswertung der Erhebungsbögen, namentlich die Aggregierung der Daten, beim örtlichen oder gebietsgemeinschaftlichen Fremdenverkehrsverein, also nicht durch die Gemeindeverwaltung selbst, stattfinden sollte. An der Eigenschaft einer amtlichen Statistik ändert sich auch nicht etwa dadurch etwas, dass im Satzungstext als Erhebungszweck „Gästegewinnung/Kundenpflege im örtlichen Marketing“ angegeben wird.

Einige der Anforderungen, die §§ 6 Abs. 6 Satz 1 und 2 i. V. m. 8 Abs. 1 Satz 2, 2. Halbsatz sowie § 9 Abs. 1 SächsStatG stellen, hält die vorgeschlagene Regelung nicht ein.

Ich habe Verbesserungsvorschläge gemacht, für die Einvernehmen mit dem SMWA und dem für Fragen des Statistikrechts zuständigen SMI hat erzielt werden können. Auf diese Weise ergibt sich eine gründlich veränderte Muster-Vorschrift für die Kurgäste-Statistik. Als eigenständiger Paragraph der Kurtaxen-Satzung lautet die Regelung in der zuletzt vom SMWA festgehaltenen Formulierung folgendermaßen:

> (1) Zum Zwecke der Gästegewinnung und Kundenpflege [*besser wäre: zum Zwecke der Förderung des Fremdenverkehrs*] kann die Gemeinde bei den Kurtaxepflichtigen (§§ 2, 4 [*Verweisung auf die einschlägigen Regelungen der Muster-Satzung*]) die folgenden Angaben erheben:
>
> - Informationsquelle für die Wahl des Reiseziels (Druckmaterialien, Messen, Medien, Verwandte/Bekannte)
> - Reiseanlass (privat/touristisch/geschäftlich)
> - Organisationsform (Reisebüro/individuell)
> - Reisegruppengröße (allein/Ehepaar/Familie)
> - Motivation zur Auswahl des Reiseziels (Landschaft/Natur, Kultur, Erlebnis, Gastfreundlichkeit)
> - Verkehrsmittel zur Erreichung des Aufenthaltsortes (Bahn/Bus/Pkw)
> - Beherbergungsform (Hotel/Pension/Ferienwohnung/privat)
> - Bewertung des Umfanges an Angebot und zur Freizeitgestaltung (umfassend/eher ausreichend/eher nicht ausreichend/mangelhaft)
> - Besuchshäufigkeit des Aufenthaltes im Ort (einmalig/zweimalig/mehrfach)
> - Alter des Gastes und mitreisender Personen.
>
> Diese Erhebung findet jeweils in der Saison (Sommer/Winter) statt.
>
> (2) Eine Auskunftspflicht besteht nicht, die Beteiligung an der Erhebung ist freiwillig.

(3) Der Bürgermeister wird ermächtigt, die Durchführung der Statistik ganz oder teilweise einem Privaten, namentlich dem örtlichen Fremdenverkehrsverein oder einem gebietlichen Zusammenschluss der örtlichen Fremdenverkehrsvereine, zu übertragen.

Die Aufzählung der Merkmalsausprägungen (in den Klammern hinter den einzelnen Erhebungsmerkmalen aufgeführt) ist meiner Auffassung nach in allen Fällen entbehrlich.

Gemäß Absatz 3 handelt es sich um eine weitgehend privatisierte amtliche Statistik (auf Satzungsgrundlage).

In vieler Hinsicht sinnvoller, weil wesentlich einfacher, insbesondere auch nicht mit Vorlagepflichten gemäß § 8 Abs. 3 SächsStatG verbunden, wäre jedoch eine vollständige Privatisierung (vgl. dazu ausführlich 4/5.7.3, ergänzend 5/5.7.5). In diesem Falle können in der Kurtaxe-Satzung jegliche Ausführungen zur Fremdenverkehrsförderungs-Statistik entfallen.

Ich habe gebeten, ergänzend in den Erläuterungen zur Muster-Satzung auf Folgendes hinzuweisen:

- Ein Durchschreibesatzverfahren darf nicht angewandt werden. Zum einen hätte es notwendig die Wirkung, den Unterschied zwischen der Freiwilligkeit der zur Durchführung der Fremdenverkehrsförderungs-Statistik zu machenden Angaben und der im Übrigen bestehenden Auskunftspflicht undeutlich werden zu lassen. Zum anderen müsste ein Durchschreibesatzverfahren zu Unklarheiten über den gänzlich unterschiedlichen Meldeweg führen, der einmal zur Meldebehörde und zur Kurtaxenstelle der Gemeinde, zum anderen, was die Statistik-Daten betrifft, zum örtlichen oder gemeinschaftlichen Fremdenverkehrsverein verläuft.
  Überdies: Geht man davon aus, dass die Kurtaxe, wie üblich, auf einer Stelle der Gemeinde entrichtet wird, sollten dort nicht gleichzeitig die Daten der Fremdenverkehrsförderungs-Statistik erhoben werden. Denn dann kämen diese zunächst, nicht vollständig anonym, in den Verfügungsbereich der Gemeinde, was, da diese keine kommunale Statistikstelle hat, überhaupt unzulässig wäre.

  Datenschutzgerecht wäre folgende Verfahrensweise: Getrennter Vordruck in den Räumen der Kurverwaltung, dort abzugeben im geschlossenen Umschlag, ersatzweise einzuwerfen in einen besonderen Briefkasten des örtlichen Fremdenverkehrsvereins. Es empfiehlt sich eine Ausgabe eines Erhebungsbogens mit der Gästekarte (§ 6 des Satzungsentwurfes), damit die Statistik nicht dadurch verfälscht wird, dass ein Gast viele Erhebungsbögen ausfüllt und abgibt (Frage der Eignung der Datenerhebung! Vgl. auch vorstehend unter 5.7.3).

- Weil gemäß § 2 Abs. 3 des Satzungsmusters kurtaxepflichtig auch Inhaber einer Nebenwohnung sein sollen, die demnach keinen Beherbergungsvertrag mit Dritten abschließen, scheidet die Möglichkeit, die Kurtaxe über die unterkunftgewährende Person einzuziehen, wohl aus, mit der Folge, dass diese Person auch als Erhebungs-

beauftragter für die Durchführung der Fremdenverkehrsförderungs-Statistik nicht in Frage kommt.

- Im oben erwähnten Falle der vollständigen Privatisierung der Fremdenverkehrsförderungs-Statistik ist der Fremdenverkehrsverein in seiner Vorgehensweise - innerhalb der Grenzen des für alle privaten Datenverarbeitungen geltenden dritten Abschnittes des BDSG - frei. Wichtig ist, dass die Erhebungsbögen so gestaltet werden, dass auch für den flüchtigen Betrachter klar ist, dass die Datenerhebung nicht durch die politische Gemeinde, sondern ausschließlich durch den - privaten - Fremdenverkehrsverein stattfindet.

  Eine - bei der Datenerhebung nicht erkennbare - Förderung des Fremdenverkehrsvereins durch die Kommune ist dieser unbenommen, d. h. macht die von diesem durchgeführte Fremdenverkehrsförderungs-Statistik nicht zu einer amtlichen.

Entgegen den mir gegenüber gemachten Ankündigungen ist bedauerlicherweise bis heute die Veröffentlichung einer verbesserten Fassung der Mustersatzung nicht veranlasst worden.
Auch hat bisher noch keine Gemeinde mir gemäß § 8 Abs. 3 SächsStatG den Entwurf einer Satzung vorgelegt, in der eine Fremdenverkehrsförderungs-Statistik angeordnet werden soll. Diese Pflicht besteht auch dann, wenn die Vorschrift, welche die Durchführung der Statistik anordnet, Teil einer im Übrigen nichtstatistikrechtlichen Satzung ist.

Vorsicht sollten sächsische Kurorte bei der Verwendung von Meldeschein-Vordrucken für Beherbergungsstätten nach nicht-sächsischem, z. B. baden-württembergischem, Vorbild walten lassen. Es sollte ihnen nicht so gehen wie dem sächsischen Kurort, der offenbar für viel Geld solche Vordruck-Sätze angeschafft hatte (und deren Benutzung - sprich Kauf - dann seinen Beherbergungsbetrieben aufzwingen wollte): Weil auf dem Gebiet des Statistikrechts ein erheblicher Unterschied zu Baden-Württemberg besteht, musste ich der Gemeinde mitteilen, dass sie diese Meldevordrucke, die überdies auch in melderechtlicher Hinsicht zu den Meldegesetzen anderer Länder, nicht aber zu dem Sachsens passten, nicht weiterverwenden darf.

5.7.5 Haben datenschutzrechtliche Fehler eines Mietspiegels zivilrechtliche Folgen?

Es hat sich inzwischen in den sächsischen Gemeinden herumgesprochen, dass die Sammlung und Auswertung von Mietvertragsdaten zum Zwecke der Erstellung eines Mietspiegels datenschutzrechtlichen, und d. h. inbesondere statistikrechtlichen, Regeln unterliegt; ich habe das ausführlich in 5/5.7.2 dargelegt (ergänzend 6/5.7.4).

So kann es nicht verwundern, dass in rechtlichen Auseinandersetzungen um Mieterhöhungsverlangen der eine oder andere Beteiligte auf den Gedanken gekommen ist, er könne gegen die Verwendung des örtlichen Mietspiegels in Erhöhungsverlangen auch rein datenschutzrechtliche Fehler des Zustandekommens des Mietspiegels geltend machen, also solche Fehler, die nicht Folge des Umstandes sind,

dass der Mietspiegel nicht den mietrechtlichen Bestimmungen, also dem MHRG, entspricht; letzteres führt ja auch zu einer datenschutzrechtlichen Fehlerhaftigkeit, weil die zur Erstellung des Mietspiegels stattfindende Verarbeitung personenbezogener Daten zur Erreichung des gesetzlich vorgegebenen Zweckes ungeeignet und daher rechtswidrig wäre.
Man könnte diese Überlegung daher auch folgendermaßen formulieren: Wenn mietrechtliche Fehler bei der Sammlung von Daten für Mietspiegel auf die datenschutzrechtliche Beurteilung durchschlagen, warum sollen dann nicht auch rein datenschutzrechtliche, also vor allem statistikrechtliche, Fehler der Datensammlung auf die zivilrechtliche Verwertbarkeit des betreffenden Mietspiegels durchschlagen? Folge wäre, dass ein solcher datenschutzrechtlich fehlerhaft zustandegekommener Mietspiegel als Begründungsmittel für ein wirksames Mieterhöhungsverlangen (§ 2 Abs. 2 Satz 2 MHRG) nicht taugte, so dass ein derartiges Mieterhöhungsverlangen unwirksam wäre, also das vorprozessuale Mieterhöhungsverfahren nicht in Gang zu setzen (oder dessen Nachholung im gerichtlichen Verfahren gemäß § 2 Abs. 3 Satz 2 MHRG nicht zu ermöglichen) vermöchte.

(Die davon zu unterscheidende Frage der Verwertbarkeit eines solchen Mietspiegels als Grundlage der gerichtlichen Feststellung der ortsüblichen Vergleichsmiete könnte sich zusätzlich nur dann stellen, wenn der gerichtlichen Entscheidung ein späterer Mietspiegel als derjenige zugrunde zu legen wäre, auf den sich das Erhöhungsverlangen gestützt hat; also wohl im Falle des Erscheinens des neuen Mietspiegels zwischen Zugang des Mieterhöhungsverlangens beim Mieter vor dem Zeitpunkt des § 2 Abs. 4 MHRG.)

Indes: Ob ein ausschließlich datenschutzrechtlich (statistikrechtlich) fehlerhaft zustandegekommener Mietspiegel einem zivilrechtlichen (mietrechtlichen) Verwertungsverbot unterliegt, lässt sich dem MHRG nicht ohne weiteres entnehmen, ist von den Zivilgerichten zu entscheiden und liegt gänzlich außerhalb meiner Zuständigkeit.

Meine Aufgabe, so muss ich alle derartigen Anfragen bescheiden, beschränkt sich darauf, sogenannte empirische Mietspiegel, d. h. Mietspiegel, die von der Gemeinde durch eine Befragung der Mieter erstellt werden, auf die Rechtmäßigkeit der Datenerhebung hin zu überprüfen. Stelle ich Verstöße gegen datenschutzrechtliche Vorschriften bei dieser Datenverarbeitung durch die Gemeinde fest, habe ich im Rahmen des § 26 SächsDSG die Aufgabe, die Gemeinde zu beanstanden. Zu beurteilen, welche mietrechtlichen Konsequenzen aus einem solchen Verstoß zu ziehen sind, fällt nicht in meine Zuständigkeit, sondern in diejenige der damit befassten Zivilgerichte.

5.7.6 Exemplarische Kommunalstatistik zur Bevölkerungsabwanderung

Eine ostsächsische Stadt wollte eine „Befragung Zugezogener und Fortgezogener“ durchführen. Wieder musste ich im Hinblick auf den Satzungsentwurf und den geplanten Fragebogen auf Folgendes hinweisen:
Statistiken dürfen nur zur Deckung eines objektiv bestehenden Informationsbedarfes durchgeführt, die Daten müssen benötigt werden, d. h. dienlich sein zur Aufgabener-

füllung (vgl. § 1 Abs. 1 Satz 1, § 6 Abs. 3 Satz 1, § 8 Abs. 2 Satz 1, § 9 Abs. 6 Satz 1 SächsStatG). Aufgabenerfüllung sind hier planerische Entscheidungen der Stadt - also Planungen innerhalb des Rahmens der Planungshoheit. Unter Planungshoheit ist das Recht der Gemeinde zu verstehen, in eigener Verantwortung die städtebauliche Entwicklung durch Bauleitpläne einschließlich der damit verbundenen finanziellen Entscheidungen zu ordnen sowie öffentliche und sonstige Einrichtungen zum Wohl der Einwohner zu schaffen.

Nach der Grundkonzeption der Satzung ging es darum, zur Erkenntnis der Gründe für die anhaltenden Wanderungsverluste, insbesondere die Struktur der abwandernden und zuziehenden Bevölkerung sowie die Wohnverhältnisse und Wohnbedürfnisse dieses Bevölkerungsteils in der Stadt festzustellen und diese Erkenntnisse für planerische Entscheidungen zu nutzen.
Viele der Erhebungsmerkmale waren dafür nicht geeignet bzw. nicht erforderlich, denn es war nicht nachvollziehbar, in welcher Weise sie den Informationsbedarf der Stadt decken könnten.

Dafür hier nur einige Beispiele:

- Die im Fragebogen vorgesehene Frage nach dem Verhältnis zu „Hausmitbewohnern/ Nachbarn“ ließ nicht erkennen, welchen Informationswert für die planerische Entscheidung sie haben könnte. Die Stadt hat nämlich auf dergleichen keinerlei Einfluss. Hinzu kommt: Ein schlechtes Verhältnis mit Nachbarn ist kein Grund, gleich nach außerhalb der Stadt zu ziehen (so klein ist sie nicht!). Es handelt sich daher um einen in seiner Eigenart für die Stadtverwaltung irrelevanten Grund, mit der Folge, dass diese nach dem Vorliegen gerade dieses Grundes nicht fragen darf: Die Frage wäre ungeeignet und daher rechtswidrig. (Außerdem war die Frage übrigens auch noch ungenau, da man in der Regel mehr als einen Nachbarn hat und das Verhältnis zu den mehreren Nachbarn, nach dem ja pauschal gefragt werden sollte, höchst unterschiedlich sein kann.)

- Ähnliches galt für die geplante Frage nach dem Umzugsgrund „Abriss oder Modernisierung“: Es ist selbstverständlich und bedarf keiner besonderen Erkenntnisse, dass Abriss oder (durchgreifende) Modernisierung zumindest zeitweilig zur Räumung der Wohnung und damit zum Umzug führen. Diese Umstände haben aber keinen Einfluss darauf, ob man in Zukunft nun gerade innerhalb oder außerhalb der Gemeinde wohnen will. Auf diesen Unterschied kam es der Stadt aber gerade an. Diese beiden Umzugsgründe waren daher also nur insofern für die planerischen Entscheidungen der Stadt von Belang, als sie gerade ohne Auswirkung auf diese Entscheidungen sind. Dasselbe gilt für die Umzugsgründe „Gründung eines neuen Haushaltes“ und „Vergrößerung oder Verkleinerung des Haushaltes“. Diese Gründe durften im Rahmen dieser amtlichen Statistik als solche, also in ihrer Unterschiedenheit als verschiedene Merkmalsausprägungen, gerade nicht erhoben werden; erhoben werden durfte nur, neben den zulässigen weil stadtplanungsrelevanten Umzugsgründen (Beispiel: „Suche oder Wechsel eines Arbeits- oder Ausbildungsplatzes“) das Vorliegen eines *sonstigen*, nämlich kommunalplanerisch irrelevanten Umzugsgrundes.

- Es gab aber auch den umgekehrten Fall, dass zu wenig genau gefragt werden sollte, weil nämlich höchst verschiedene Umzugs-Gründe unter einer Merkmalsausprägung zusammengefasst abgefragt werden sollten, mit der Folge, dass eine (gezielte) planerische Reaktion gar nicht möglich wäre (Beispiel: „Wohnung entsprach nicht mehr meinen Wünschen"). Die Datenerhebung wäre mangels Auffächerung der Antwortmöglichkeiten (in der Statistikersprache: Merkmalsausprägungen) ungeeignet gewesen.

- Diejenigen, die weggezogen waren, weil sie fern der Stadt einen Arbeitsplatz gefunden hatten, der ihnen zusagte, durften zur Wohnsituation nicht befragt werden. Denn ihre Wohnsituation konnte kein Grund bei der Entscheidung für den Wegzug aus der Stadt gewesen sein. Erhoben werden durfte also nur, dass jemand des besseren auswärtigen Arbeitsplatzes wegen weggezogen war.
  In der praktischen Durchführung bedeutete das, dass dieser Umstand als Filter-Merkmal abgefragt werden musste, welches im Falle der positiven Beantwortung zu einem Ende der Befragung führte.

Nach einem für beide Seiten ziemlich arbeitsaufwendigen Hin und Her ist hoffentlich am Ende eine einigermaßen vernünftige Statistik herausgekommen. Mit der linken Hand lässt sich so etwas nicht machen, und es reicht auch insbesondere nicht aus, die Erhebungen von Großstädten zum Vorbild zu nehmen (im vorliegenden Fall aus Nordrhein-Westfalen und Thüringen), man muss die Sache schon selber durchdenken. Schließlich: „Stadtforschung" und (amtliche) Kommunal-Statistik sind juristisch zwei verschiedene Welten.

5.8 Archivwesen

5.8.1 Weiterhin: Behinderung des Zugangs der zeitgeschichtlichen Forschung zu noch nicht archivierten Altdaten

In 6/5.8.4 habe ich ausführlich dargestellt, welche Konsequenzen sich für die Forschung daraus ergeben, dass Unterlagen aus der Zeit zwischen dem Ende des Zweiten Weltkrieges und der Wiedervereinigung trotz eindeutigen Willens des sächsischen Gesetzgebers nicht den Archiven angeboten werden. Die Forschung hat eben nach Archivrecht einen weitergehenden Zugang zu Unterlagen mit personenbezogenen Daten als nach Sächsischem Datenschutzgesetz, und sie soll ihn, was Altdaten betrifft, auch haben. Dieser erweiterte Zugang ist versperrt, werden die Unterlagen nicht den Archiven angeboten.

Die Auswirkungen dieser Praxis habe ich in meinem 6. TB an zwei Beispielen aus dem Bereich der Justizverwaltung veranschaulicht. In ihrer Stellungnahme dazu hat die Staatsregierung (LT-DS 2/10552, auf S. 13 zu Abschnitt 5.8.4) es abgelehnt, im Landtag den Entwurf einer Regelung einzubringen, welche bestimmt, dass auf Unterlagen, die unter § 4 Abs. 2 Satz 2 und 3 SächsArchivG fallen und noch nicht archiviert sind, die Regelungen des § 10 Abs. 1, Abs. 2 und Abs. 4 SächsArchivG entsprechend anzuwenden sind.

Für den Bereich der Justizverwaltung meint die Staatsregierung mit der *Verwaltungsvorschrift des Sächsischen Staatsministeriums der Justiz über die Aufbewahrung und Aussonderung von Unterlagen bei den ordentlichen Gerichten, Gerichten für Arbeitssachen, Staatsanwaltschaften und Justizvollzugsanstalten (VwV Aufbewahrung und Aussonderung - VwVAufAus) vom 12. Juni 1998 (Sächsisches Justizministerialblatt, S. 80)* das Nötige getan zu haben. Denn die VwV sorge mit dem Satz „die Unterlagen können dem zuständigen Archiv angeboten werden" dafür, dass bei Bedarf der forschungsfreundlichere Datenzugang nach Archivgesetz durch Archivierung eröffnet werden könne.

Sofern der ernsthafte Wille seitens des Staatsminsiteriums besteht, dem Anliegen des Sächsischen Archivgesetzes, die Erforschung der jüngeren Vergangenheit zu erleichtern, Rechnung zu tragen, sollte an der einschlägigen Stelle der Verwaltungsvorschrift für den Fall, dass ein Interesse der Forschung an Unterlagen erkennbar ist, die Anbietung im Weisungswege nicht nur freigestellt - was nur § 5 Abs. 6 SächsArchivG umsetzt -, sondern geboten werden. Dies hätte auch den Vorteil, das Ministerium von der Prüfung aller derartigen Einzelfälle zu entlasten.

Dies habe ich dem SMJus und dem als oberste Archivbehörde beteiligten SMI im Hinblick auf den mir zur Stellungnahme übersandten Entwurf einer Neufassung dieser Verwaltungsvorschrift (nunmehr veröffentlicht im Sächsischen Justizministerialblatt 1999, S. 28) gegenüber geltend gemacht - ohne Erfolg, wie man in Abschnitt D IV der genannten VwV nachlesen kann.
Abgesehen davon ersetzt eine solche VwV schon wegen ihres beschränkten Anwendungsbereiches eine gesetzliche Regelung nicht.

Nach wie vor halte ich daher meinen Vorschlag, eine gesetzliche Regelung zu schaffen, nach der auf Unterlagen, die unter § 4 Abs. 2 Satz 2 und 3 SächsArchivG fallen und noch nicht archiviert sind, die Regelungen des § 10 Abs. 1, Abs. 2 und Abs. 4 SächsArchivG entsprechend anzuwenden sind, für geeigneter, den vom sächsischen Archivgesetzgeber gewollten Datenzugang zu eröffnen.

Dass die VwVAufAus bisher nicht die nötige Abhilfe hat schaffen können, zeigt sich auch in der Praxis: Ein sächsisches Arbeitsgericht, welches angefragt hat, unter welchen Voraussetzungen eine Doktorandin Zugang zu von ihm aufbewahrten Akten aus Verfahren vor DDR-Arbeitsgerichten bekommen könne, habe ich auf die sich vor einer Archivierung ergebenden Schwierigkeiten hinweisen müssen (vgl. dazu unter 5.8.4), und daher habe ich auch in diesem Fall empfohlen, die Akten dem Staatsarchiv anzubieten: Dies müsste gemäß § 5 Abs. 6 SächsArchivG ohne weiteres auch vor Ablauf der Frist für die dem Gericht gebotene Aufbewahrung möglich sein. Und das Archiv könnte die Unterlagen übernehmen, ohne damit sich darauf festzulegen, diese bleibend, d. h. auf unabsehbare Zukunft aufbewahren zu müssen (vgl. § 8 Abs. 2 SächsArchivG).

Es wird sich herausstellen, ob jedenfalls im Falle dieses konkret angemeldeten Datenbedarfs für Forschungszwecke es zu der vom Gesetzgeber gewollten zügigen Anbietung von Altdaten gegenüber den Archiven kommt.

5.8.2 Benutzung von Archivgut zur Ermittlung der Anschrift eines IM?

Jemand hatte durch Einsichtnahme in seine Stasi-Unterlagen erfahren, dass er von einem IM bespitzelt worden war. Er wollte nun die jetzige Anschrift dieses IM ermitteln und wandte sich, vermutlich weil er an die alten Kreismeldestellen dachte, an das Kreisarchiv. Dieses wollte von mir wissen, ob es dem Antragsteller behilflich sein dürfe, weil der IM doch möglicherweise als Amtsträger gemäß § 10 Abs. 2 Satz 3 SächsArchivG nach Archivrecht insoweit keinen Schutz genieße.

Ich habe dem Kreisarchiv mitgeteilt, dass dem Antragsteller der Weg, die Anschrift über eine Benutzung des Archivgutes zu ermitteln, verschlossen bleibt, denn die dem Schutz des Persönlichkeitsrechtes dienenden Schutzfristen des § 10 Abs. 1 Satz 3 und 4 SächsArchivG sind noch nicht abgelaufen.
Zwar sind die genannten Schutzfristen auf Amtsträger in Ausübung ihrer Ämter nicht anwendbar; entsprechendes gilt für Mitarbeiter der in § 4 Abs. 2 und Abs. 3 SächsArchivG genannten Stellen (§ 10 Abs. 2 Satz 3 SächsArchivG). Jedoch greift § 10 Abs. 2 Satz 3 SächsArchivG hier nicht ein. Denn die Privatanschrift gehört nicht zur Amtsausübung und auch nicht zu deren DDR-Gegenstück, welches § 10 Abs. 2 Satz 3, 2. Halbsatz SächsArchivG erfasst. Darauf, ob ein IM unter den „Mitarbeiter"-Begriff des § 10 Abs. 2 Satz 3 SächsArchivG fällt, kam es daher entgegen der Vorstellung des Kreisarchivs gar nicht an.

Zusammengefasst: Die Privatanschrift eines Amtsträgers (oder eines Mitarbeiters i. S. d. § 10 Abs. 2 Satz 3, 2. Halbsatz SächsArchivG) ist ein Datum, das in keinem Zusammenhang mit seiner amtlichen Tätigkeit steht. Eröffnet der Staat Zugang zu diesem Datum, greift er in den Schutzbereich des Persönlichkeitsrechtes ein. Dies ist nur nach Maßgabe des § 10 SächsArchivG erlaubt.

Damit waren dem Stasi-Opfer aber keineswegs alle Möglichkeiten verbaut: Ihm steht die Melderegister-Auskunft nach § 32 SächsMG zu.

5.8.3 Benutzung von Archivgut zur Erarbeitung einer Ortschronik

Archivgut darf nur nach Ablauf der in § 10 SächsArchivG Satz 3 und 4 genannten Schutzfristen benutzt werden. Diese Schutzfristen sind mit 10 Jahren nach dem festgestellten Tod, ersatzweise 100 Jahre nach der Geburt, kürzer als nach dem Bundesarchivgesetz. Sie sollen einen weitgehenden Schutz des Persönlichkeitsrechts der Betroffenen gewährleisten. Soll die jüngere Vergangenheit chronikartig dargestellt werden, stoßen deshalb die Bearbeiter schnell an datenschutzrechtliche Grenzen, für die ich immer wieder einmal um Verständnis werben muss.

Das Gesetz erlaubt eine Verkürzung der Schutzfristen bei personenbezogenem Archivgut nur, wenn die Benutzung für ein bestimmtes Forschungsvorhaben erfolgt und schutzwürdige Belange der betroffenen Personen oder Dritter nicht beeinträchtigt werden oder das öffentliche Interesse an der Durchführung des Forschungsvorhabens die schutzwürdigen Belange erheblich überwiegt (§ 10 Abs. 4 Satz 2 SächsArchivG). Eine solche Verkürzung der Schutzfristen kommt bei der Bearbeitung einer Orts-

chronik nicht in Betracht, da diese nicht als Forschung einzustufen ist. Eine Chronik ist eine bloße Zusammenstellung des Stoffes, sie ist als bloße Aufbereitung von Quellen lediglich eine Vorstufe für die Gewinnung und Darstellung wissenschaftlicher Ergebnisse (die sich selbstverständlich auch auf einen örtlich begrenzten Bereich beschränken können). Darauf jedoch, also auf die wissenschaftliche Erforschung vergangener Sachverhalte, hebt § 10 Abs. 4 Satz 2 SächsArchivG ab.

Dieser Unterschied zwischen Chronik und wissenschaftlicher Untersuchung schlägt auch noch in einer anderen Hinsicht durch, nämlich gewissermaßen auf der zweiten und heikleren Stufe der Verarbeitung personenbezogener Daten bei der Benutzung von Archivgut, also bei der Veröffentlichung des Ergebnisses der Nutzung der Archivunterlagen: Eine Chronik lässt notwendig Einzelpersonen ungleich mehr in den Vordergrund treten als es wissenschaftliche Geschichtsschreibung tut. Eine chronikartige Darstellung erfüllt daher von vornherein kaum die Voraussetzung, von der das Gesetz in § 10 Abs. 4 Satz 2 SächsArchivG ausgeht, nämlich dass der Zugang zu den Daten für ein Vorhaben gewährt wird, dessen Eigenart es mit sich bringt, dass der schwerwiegendere Eingriff in das Persönlichkeitsrecht, mithin die Veröffentlichung personenbezogener Daten, hinter dem weniger schwerwiegenden, nämlich der Übermittlung an den Archivbenutzer (Forscher), quantitativ, also was die Menge personenbezogener Daten betrifft, erheblich zurückbleibt.

Damit ist aber nicht jede Nutzung personenbezogenen Archivgutes für chronikartige Darstellungen der jüngeren Vergangenheit ausgeschlossen: Der Ablauf der dem Schutz des Persönlichkeitsrechtes dienenden Schutzfristen des § 10 Abs. 1 Satz 2 und 4 SächsArchivG kann durch Einwilligung ersetzt werden. Und, was vielfach übersehen wird: Für Amtsträger gelten, soweit es um die Ausübung ihrer Ämter geht, die persönlichkeitsrechtschützenden Schutzfristen nicht (§ 10 Abs. 2 Satz 3, 1. Halbsatz SächsArchivG). Darunter fallen die Funktionsträger von NS-Organisationen ebenso wie aus der zweiten deutschen Diktatur, also die in § 10 Abs. 2 Satz 3, 2. Halbsatz i. V. m. § 4 Abs. 2 Satz 2 und 3 SächsArchivG genannten Personen.

5.8.4 Auswertung von Gerichtsakten durch Doktoranden

Manche Promotionsvorhaben auf dem Gebiet der Rechtswissenschaft kommen nicht ohne Auswertung von Gerichtsakten aus. Solche Akten befinden sich entweder noch bei den Gerichten, dann richtet sich mangels besonderer Vorschriften der Zugang zu ihnen nach allgemeinem Datenschutzrecht, oder sie wurden bereits archiviert, dann ist in Sachsen das Sächsische Archivgesetz anzuwenden.

Das Archivgesetz bietet im Gegensatz zum allgemeinen Datenschutzrecht einen erleichterten Zugang der Forschung - als eine solche sind Promotionsvorhaben anzusehen - zu solchen Unterlagen. Zwar gelten für Archivgut Schutzfristen, jedoch können diese für personenbezogenes Archivgut zugunsten eines bestimmten Forschungsvorhabens verkürzt werden (§ 10 Abs. 4 Satz 2 SächsArchivG).

Solange die Akten sich hingegen stattdessen in der Obhut der Justiz befinden, richtet sich der Zugang zu den in ihnen enthaltenen personenbezogenen Daten zu

Forschungszwecken ausschließlich nach § 12 Abs. 2 Nr. 4 SächsDSG i. V. m. § 15 Abs. 1 Nr. 2 oder aber i. V. m. § 13 Abs. 1 SächsDSG.
Dadurch ist der Zugang für die Forschung beträchtlich erschwert. Ich habe mich zu dieser Frage bereits eingehend in 6/5.8.4 geäußert.

Die Anwendung des Sächsischen Datenschutzgesetzes führt dazu, dass zunächst genau bestimmt werden muss, wer Empfänger der personenbezogenen Daten sein soll. Ist dies der Doktorand als Privatperson, so ist § 15 SächsDSG anzuwenden.
Schwierig ist es allerdings, die Voraussetzungen des § 15 Abs. 1 Nr. 2 i. V. m. Abs. 3 SächsDSG zu bejahen: Der Betroffene darf kein schutzwürdiges Interesse am Unterbleiben der Übermittlung haben; aus diesem Grund ist er vor der Übermittlung zu hören. Eine Einschränkung des Anhörungs-Gebotes sieht § 15 Abs. 3, 2. Halbsatz SächsDSG vor: Diese Ausnahmeregelung ist aber eng auszulegen (so im Ergebnis auch Ancôt, Kommentar zum Sächsischen Datenschutzgesetz, Rdnr. 5 zu § 15). Und zwar meines Erachtens deswegen, damit ein Wertungs-Unterschied gegenüber der entsprechenden Vorschrift des § 16 Abs. 3 Satz 2 BDSG vermieden wird; hier ist nicht jede Grundrechtsausübung, als welche sich ja auch namentlich die wissenschaftliche Betätigung eines Übermittlungsempfängers darstellt, als Ausnahmegrund gemeint.

Um eine Übermittlung an öffentliche Stellen, mit der Folge der Anwendung des § 13 SächsDSG, handelt es sich demgegenüber dann, wenn die Doktoranden aufgrund eines Beschäftigungsverhältnisses die Unterlagen für die Universität bzw. einer Organisationseinheit derselben einsehen sollen. Die Daten werden dann an die Hochschule zu Händen deren Bediensteter übermittelt. Dies setzt allerdings zusätzlich voraus, dass der Doktorand keine personenbezogenen Daten in Gestalt von Aufzeichnungen aus den Akten in seiner eigenen Wohnung aufbewahrt. Denn diese Wohnung kann nicht als Außenstelle der Universität angesehen werden, und durch Anerkennung einer Art „Heimarbeit“-Verhältnisses wären meiner Auffassung nach die Möglichkeiten, die § 13 SächsDSG bietet, überspannt.

Die Anonymisierung ist ein Ausweg, der sich immer bietet. Dem Doktoranden werden ausschließlich hinreichend anonymisierte Unterlagen, d. h. mit Schwärzungen versehene Ablichtungen, zur Verfügung gestellt. Dies ist allerdings mit einem ganz erheblichen Aufwand für das betreffende Gericht verbunden.

5.8.5 Datenschutz zugunsten Verstorbener in Anlehnung an Archivrecht

Eine sächsische Gemeinde wollte ein Verzeichnis der Gemeindebewohner zusammenstellen, die im Zweiten Weltkrieg gefallen oder vermisst sind.
Die von der Gemeinde beabsichtigte Datensammlung fiel größtenteils nicht unter datenschutzrechtliche Regelungen. Dies ergibt sich im Einzelnen aus Folgendem:

Träger des Grundrechts auf informationelle Selbstbestimmung sind ausschließlich Lebende. Allerdings gibt es in verschiedenen Einzelbereichen datenschutzrechtliche Regelungen auch zugunsten Verstorbener. Datenschutzrechtliche Spezialregelungen wie das Arzt-, das Statistik- und das Steuergeheimnis reichen über den Tod des

Betroffenen hinaus. Geschützt wird so das verfassungsrechtliche Persönlichkeitsrecht, insoweit es ausschließlich aus Art. 1 Abs. 1 GG (Menschenwürde) herzuleiten ist. Die zeitlichen Grenzen sind dabei schwer zu bestimmen (vgl. Simitis-Dammann, Rdnr. 17 zu § 3 BDSG).

Im vorliegenden Falle bot es sich an, sich an die dem Persönlichkeitsrechtsschutz dienenden Schutzfristen des Archivrechtes zu halten. Auch Archivrecht ist ja insoweit Datenschutzrecht. Nach § 10 Abs. 1 Satz 3 und 4 SächsArchivG sind dies zehn Jahre nach dem bekannten Todeszeitpunkt der betroffenen Person, ersatzweise hundert Jahre nach deren Geburt.

Selbst wenn man stattdessen die längeren Schutzfristen des Bundesarchivgesetzes (30 Jahre nach dem Tod, ersatzweise 110 Jahre nach der Geburt, § 5 Abs. 2 BArchG) zugrunde legt, sind diese Fristen für alle Erhebungsmerkmale, die sich unmittelbar auf den Gefallenen bzw. Vermissten beziehen, also etwa auch auf seine Wohnanschrift und seinen Dienstgrad und die Angabe, wann und wo er gefallen bzw. vermisst ist, bereits abgelaufen. Auch die allgemeine archivrechtliche Sperrfrist von 30 Jahren (§ 10 Abs. 1 Satz 1 SächsArchivG, § 5 Abs. 1 Satz 1 BArchG) ist seit der Rückkehr der letzten deutschen Kriegsgefangenen in den späten 50iger Jahren lange abgelaufen. Wer seitdem vermisst ist, kann unter dem Gesichtspunkt des Persönlichkeitsrechtsschutzes als verstorben gelten.

Demgegenüber durfte das geplante Merkmal „Anschrift der Angehörigen“ nur auf Einwilligungsgrundlage erhoben, gespeichert und durch die geplante Auslegung der Liste veröffentlicht werden. Denn gemeint waren hier offenbar lebende Personen, sei es nun mit oder ohne Namensnennung. Die bloße Anschriften-Angabe hätte ausgereicht, den Personenbezug herzustellen (vgl. § 3 Abs. 1 SächsDSG).

Vgl. auch unten 10.1.2.

5.9 Polizei

5.9.1 Automatisierte Dateien im Landeskriminalamt

Im Berichtsjahr legte mir das SMI einige vom LKA aktuell erstellte Errichtungsanordnungen für Fachdateien zur Stellungnahme vor. Die Errichtungsanordnung der Datei „Umweltkriminalität“ nahm ich zum Anlass, die Anwendung der Datei im LKA zu kontrollieren. Hierbei stellte sich zunächst heraus, dass das LKA diese Datei bereits seit dem Jahre 1993 nutzt, worin ein Verstoß gegen § 50 Abs. 2 Satz 2 SächsPolG liegt, denn nach dieser Vorschrift ist vor dem erstmaligen Einsatz von automatisierten Verfahren der Sächsische Datenschutzbeauftragte zu unterrichten. Die weitere Kontrolle der Datei ergab folgendes:

Differenzierte Löschungsfristen innerhalb der Datensätze für die einzelnen Datengruppen, wie z. B. für Geschädigten- oder Verdächtigtendaten, waren technisch nicht vorgesehen. Eine Ausnahme galt diesbezüglich nur für Beschuldigtendaten, da entge-

gen der im Entwurf der Errichtungsanordnung enthaltenen Vorgaben unter der Rubrik „Personen“ nur der Status „Beschuldigter“ aufgeführt war. Hieraus folgte, dass eine Überprüfung der Daten des betroffenen Personenkreises grundsätzlich nur indirekt über den einzelnen Vorgang möglich war und damit der vom Gesetzgeber in § 51 SächsPolG i. V. m. § 17 SächsDSG geregelte Auskunftsanspruch für alle Personengruppen außer bei Beschuldigten faktisch leer lief; eine differenzierte Datenpflege war somit nicht möglich.

Darüber hinaus war zu kritisieren, dass zwar eine Rückmeldung der Staatsanwaltschaft an die den Sachverhalt aufnehmende Polizeidienststelle erfolgte, jedoch keine Rückmeldung der Polizeidienststelle an die zentrale Datei im LKA vorgesehen war. Dies konnte in der Praxis zu dem datenschutzrechtlich unhaltbaren Ergebnis führen, dass ein ursprünglich im Rahmen eines Ermittlungsverfahrens Beschuldigter jahrelang in der Datei gespeichert bleibt, obwohl das Verfahren schon längst - z. B. nach § 170 Abs. 2 StPO - eingestellt worden ist.

Als weiteres Defizit der Datei musste ich feststellen, dass keine wirklich effiziente Zugriffskontrolle stattfand. Zwar wurde der Nutzer beim Systemstart aufgefordert, ein Passwort anzugeben. Bei diesem handelte es sich aber nur um das allgemeine Passwort des Behördenbediensteten und nicht um ein spezielles Passwort, dessen Eingabe speziell für die Nutzung der Datei „Umweltkriminalität“ erforderlich war. Folglich konnte - was durch eine entsprechende Demonstration bestätigt wurde - ein beliebiger Nutzer des LKA nach Eingabe seines Passworts direkt auf die Datei Zugriff nehmen. Der erst nach fünf Minuten Bearbeitung einsetzende Bildschirmschoner, der mit einem zusätzlichen Passwort abgelöst werden konnte, bot vor diesem Hintergrund keinen ausreichenden Schutz.

Wie die Kontrolle weiter ergab, wurden die vom Nutzer getätigten einzelnen Arbeitsschritte im Rechenzentrum des LKA nicht protokolliert. Eine Protokollierung fand nur hinsichtlich der Tatsache des Zugriffs auf die Datei an sich statt. Dies hatte zur Folge, dass z. B. die von einem Bearbeiter vollzogene Löschung eines Datensatzes oder eines Beschuldigtendatums später nicht mehr nachvollzogen werden konnte. Die einzelnen in der Datei vorgenommenen Arbeitsschritte waren somit nicht transparent.

Diese strukturellen Defizite automatisierter Datenverarbeitung im LKA musste ich auch bei der Kontrolle weiterer Dateien, so z. B. bei „Wirtschaftskriminalität“ und „Täterorientierte Recherche“, feststellen. Als Haupthindernis für den Einsatz rechtsverträglicher Anwendungen führte das LKA an, die eingesetzte Software, deren Hersteller nicht mehr existiere, ließe sich nachträglich nicht mehr verändern.

Angesichts der Zusicherung des SMI, die erkannten Missstände mittelfristig durch Einsatz neuer Technik zu beseitigen, habe ich von einer Beanstandung des Betriebs der automatisierten Verfahren abgesehen. Bei dieser Entscheidung habe ich auch berücksichtigen müssen, dass die (allerdings klar geregelte) Nutzung der in den Dateien enthaltenen Datenbestände für die polizeiliche Aufgabenerfüllung durchaus erforderlich ist.

5.9.2 Öffentlichkeitsfahndung im Internet

In 5/14.4 habe ich darüber berichtet, dass sich immer mehr sächsische Behörden des Internet bedienen. Wie ich unterdessen in Erfahrung bringen konnte, nutzt mittlerweile auch das Landeskriminalamt Sachsen das Internet, und zwar zur Fahndung nach Tatverdächtigen und Vermissten sowie zur Sachfahndung. Ich stehe dieser Nutzung grundsätzlich positiv gegenüber, da Polizei und Justiz sich nach meiner Ansicht zur Steigerung der Effektivität von Gefahrenabwehr und Strafverfolgung auch neuer Technologien bedienen müssen. Eine dieser zukunftsweisenden Neuerungen stellt das Internet dar, das die bisherigen Fahndungsformen um ein modernes, aktuelles und weitreichendes Instrument erweitert.

Eine solche Nutzung darf aber nur im Rahmen der rechtlichen Möglichkeiten erfolgen. Das Recht des Betroffenen auf informationelle Selbstbestimmung wird schon durch die öffentlichen Fahndungsmaßnahmen herkömmlicher Art, wie etwa die Nutzung von Fahndungsplakaten, Presse, Rundfunk und Fernsehen eingeschränkt. Die 51. Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat am 14./15 März 1996 in Hamburg Grundsätze für die öffentliche Fahndung im Strafverfahren aufgestellt, die prinzipiell auch für die Fahndung im Internet gelten. Die Konferenz hat dabei deutlich gemacht, dass nach den Grundsätzen des Bundesverfassungsgerichts im Volkszählungsurteil vom 15. Dezember 1983 für alle Maßnahmen der öffentlichen Fahndung nach Personen eine normenklare und dem Grundsatz der Verhältnismäßigkeit entsprechende gesetzliche Regelung notwendig ist.

Dies gilt nach meiner Überzeugung erst recht für die Fahndung im Internet, das mit den hergebrachten Medien, die für die Öffentlichkeitsfahndung genutzt werden, nicht gleichzusetzen ist, da es eine ungleich höhere Eingriffsintensität aufweist: Das Internet ist das größte Computernetz der Welt und überschreitet in vielerlei Hinsicht die Grenzen herkömmlicher Kommunikationsmittel. Es unterscheidet sich von anderen Speichermedien insbesondere durch die weltweite und jederzeit gegebene Abrufbarkeit der einmal zum Zweck der Verbreitung eingestellten Informationen. Diese Informationen sind nicht rückholbar und können beliebig kopiert werden. Durch die Veröffentlichung von Personenfahndungen im Internet wird es zudem möglich, dass Privatpersonen oder andere Institutionen eigene unautorisierte Personenfahndungen veröffentlichen, die durch ihre Gestaltung ein offizielles Aussehen erhalten. In diesem Zusammenhang ist auch nicht auszuschließen, dass Dritte die einmal erstellten Kopien von Fahndungsaufrufen der Strafverfolgungsbehörden bis hin zu beliebiger Verfälschung manipulieren. Zwar ist es in technischer Hinsicht durch kryptographische Verfahren möglich, unbefugte Änderungen für den Nutzer erkennbar zu machen. Diese Verfahren können aber nur wirken, wenn ausreichend sichere Verschlüsselungsalgorithmen verwendet werden, eine entsprechende Infrastruktur bereitsteht und eine konsequente Anwendung auch durch den Internet-Benutzer erfolgt. Diese Infrastruktur ist derzeit jedoch noch nicht überall vorhanden.

Aus diesen Gründen sollte vor dem Hintergrund des verfassungsrechtlichen Verhältnismäßigkeitsgebots vom Gesetzgeber nach meiner Auffassung klargestellt werden, dass das Internet nur unter bestimmten Voraussetzungen zu Zwecken der Öffent-

lichkeitsfahndung genutzt werden darf. So sollten Fahndungsaufrufe grundsätzlich nur dann in das Internet eingegeben werden dürfen, wenn konkrete Anhaltspunkte dafür vorliegen, dass es sich bei der gesuchten Person um einen auch international agierenden Straftäter handelt. Voraussetzung für eine Fahndung nach namentlich bekannten Tatverdächtigen bzw. Beschuldigten im Internet sollte zudem prinzipiell das Vorliegen eines Haft- oder Unterbringungsbefehls wegen einer schwerwiegenden Straftat sein.

Ich habe meine Auffassung dem SMI schriftlich mitgeteilt und angeregt, bis zur Schaffung einer bundeseinheitlichen gesetzlichen Regelung entsprechende Nutzungsrichtlinien in Sachsen zu erlassen, wie sie beispielsweise schon in Thüringen existieren und in Rheinland-Pfalz konkret geplant sind. Das SMI hat mir daraufhin zunächst versichert, dass es meine Anregungen aufnehmen und das LKA Sachsen mit der Erarbeitung einer Richtlinie beauftragen wolle.

Bedauerlicherweise hat mir das LKA Sachsen mitgeteilt, dass bezüglich der Öffentlichkeitsfahndung im Internet keine speziellen internen Vorschriften existierten und deren Erlass gegenwärtig auch nicht geplant sei. Daran anknüpfend lehnt auch die Staatsregierung die von mir gegebenen Empfehlungen nunmehr ab und verweist u. a. darauf, dass die Internet-Fahndung bereits jetzt in Anlage B zu den Richtlinien für das Strafverfahren und das Bußgeldverfahren geregelt sei und deshalb bis zum Erlass einer bundesgesetzlichen Regelung abgewartet werden könne. Im Übrigen ist die Staatsregierung der Ansicht, dass es nicht sachgerecht sei, die Öffentlichkeitsfahndung im Internet einzuschränken, da die für diese bestehenden Risiken im Grundsatz auch bei Fahndungsaufrufen in anderen Medien bestünden.

Ich kann diese Ansicht aus den genannten Gründen nicht teilen. Ganz abgesehen von dem Umstand, dass das Gesetzgebungsverfahren des Bundes in der neuen Legislaturperiode erst neu in Gang gesetzt werden muss und sein Ausgang ungewiss ist, sind die in den Richtlinien für das Strafverfahren und das Bußgeldverfahren genannten Publikationsorgane Presse, Rundfunk und Fernsehen hinsichtlich ihrer Breitenwirkung und Grundrechtsrelevanz nicht mit dem Internet zu vergleichen. Sie mit dem Internet auf eine Stufe zu stellen heißt, die besonderen Gefährdungspotentiale des Internet zu verkennen. Ich will insofern nur auf die Veröffentlichung des Starr-Berichts in der sog. Clinton/Lewinsky-Affäre erinnern. Hier wurde für jedermann deutlich, dass durch das Internet das Persönlichkeitsrecht der Betroffenen in ungleich stärkerer Weise beeinträchtigt werden kann, als dies mittels konventioneller Medien jemals möglich wäre. Ich werde mich daher auch in Zukunft dafür einsetzen, dass die Öffentlichkeitsfahndung im Internet im Freistaat Sachsen auf eine solide und praxisnahe Grundlage gestellt wird, die die maßgeblichen verfassungsrechtlichen Vorgaben berücksichtigt.

5.10 Verfassungsschutz

Mängel in der Aktenführung

Aus Anlass mehrerer Eingaben habe ich im Landesamt für Verfassungsschutz Sachsen die Aktenführung der dortigen Fachabteilungen kontrolliert. In einem Fall waren

in der Akte die einzelnen Arbeitsschritte nicht transparent dargestellt. So konnte wegen fehlenden Aktenvermerks nicht mehr nachvollzogen werden, welchen Inhalt eine Personenbefragung durch Bedienstete des Landesamtes hatte - ein gravierender Mangel auch im Hinblick auf die dadurch eingeschränkte aufsichtliche Kontrollmöglichkeit durch die Vorgesetzten.

Im geprüften Fall führte dies dazu, dass ich die Sachverhaltsdarstellung meines Petenten im Rahmen meiner datenschutzrechtlichen Kontrolle nicht verlässlich beurteilen konnte. Von einer Beanstandung habe ich jedoch abgesehen, weil die Amtsleitung meine Kritik sofort aufnahm und die Mitarbeiter schriftlich anwies, die relevanten Arbeitsschritte durch Vermerk in der Akte festzuhalten.

5.11 Landessystemkonzept / Landesnetz

In diesem Jahr nicht belegt.

5.12 Ausländerwesen

In diesem Jahr nicht belegt.

5.13 Wahlrecht

5.13.1 Einsichtnahme in öffentlich auszulegende Wählerverzeichnisse

Nach § 21 Abs. 3 BWO ist innerhalb der Auslegungsfrist (gemäß § 17 Abs. 1 Satz 2 BWG an den Werktagen vom zwanzigsten bis zum sechzehnten Tag vor der Wahl) das Anfertigen von Auszügen aus dem Wählerverzeichnis durch *Wahlberechtigte* zulässig, soweit dies im Zusammenhang mit der Prüfung des Wahlrechts einzelner bestimmter Personen steht. Die Auszüge dürfen nur für diesen Zweck verwendet und unbeteiligten Dritten nicht zugänglich gemacht werden.

Einer Stadtverwaltung, die mich fragte, ob sämtliche wahlberechtigten Bundesbürger oder nur die Wahlberechtigten der jeweiligen Gemeinde in das anlässlich der Bundestagswahl 1998 öffentlich auszulegende Wählerverzeichnis Einsicht nehmen dürfen, teilte ich - nach Erörterung der Thematik mit dem BfD und dem SMI - mit, dass der Gesetzgeber (anders als z. B. in § 18 Abs. 4 LWO) keinerlei Einschränkung bezüglich des einsichtnehmenden Personenkreises vorgesehen hat. So kann beispielsweise vor der Bundestagswahl ein wahlberechtigter Münchner zur Prüfung des Wahlrechts von Dresdner Bürgern in das Wählerverzeichnis der Stadt Dresden Einsicht nehmen und umgekehrt.

Die Datenschutzbeauftragten des Bundes und der Länder stellten schon vor Jahren die Bedeutung der wahlrechtlichen Bestimmungen über das öffentliche Auslegen von Wählerverzeichnissen - vorübergehend sogar mit einiger Aussicht auf Erfolg - in

Frage. Leider ruht dieses Thema zurzeit sanft. Wozu dient dieser Verwaltungsaufwand einer Datenveröffentlichung?

5.13.2 Gewinnung geeigneter Wahlhelfer für die Sächsische Kommunalwahl am 13. Juni 1999 und die Sächsische Landtagswahl am 19. September 1999

Verschiedene sächsische Behörden fragten, ob es zulässig sei, Beschäftigtendaten zum Zwecke der Bildung von Wahlvorständen an Bürgermeister zu übermitteln.

In 6/5.13 habe ich bezüglich der Bundestagswahl festgestellt, dass solche Datenübermittlungen mangels Rechtsgrundlage im Bundeswahlgesetz nur auf freiwilliger Basis erfolgen dürfen.

Landesrechtlich sieht dies jedoch anders aus. § 10 Abs. 2 KomWG besagt nämlich, dass die Körperschaften und sonstigen juristischen Personen des öffentlichen Rechts *verpflichtet* sind, dem Bürgermeister auf dessen Anforderung für die Durchführung der Wahl Angehörige ihrer Verwaltung zu benennen, *die zur Tätigkeit in den Wahlvorständen geeignet sind*. § 8 Abs. 6 SächsWahlG ergänzt diese Bestimmung aber um folgenden Zusatz:

„... wenn der nötige Bedarf weder durch Freiwillige noch durch die Gemeindeverwaltung gedeckt werden kann.“

Solche Datenübermittlungen erfolgen demnach prinzipiell ohne Wissen der Beschäftigten, was aber nach § 31 Abs. 1 SächsDSG zulässig ist, weil die Wahlgesetze dies ausdrücklich vorsehen. Die Verpflichtung, für die Tätigkeit in den Wahlvorständen nur *geeignete* Beschäftigte zu benennen, bedeutet nach meinem Dafürhalten nicht, dass der Behördenleiter in eine vertiefte Eignungsprüfung einzusteigen hat, z. B.
- ob der Betroffene in der anfordernden Gemeinde tatsächlich wahlberechtigt ist,
- ob der Betroffene aus familiären, beruflichen, gesundheitlichen Gründen gehindert ist, das Ehrenamt ordnungsgemäß auszuüben.

Vielmehr wird man sich bei der Auswahl der in Frage kommenden Beschäftigten von den für den Behördenleiter augenscheinlichen Kriterien wie
- Betroffener ist volljährig,
- Betroffener wohnt in der anfordernden Gemeinde,

leiten lassen müssen. Eine entsprechende Information jedes Betroffenen durch den Behördenleiter bzw. durch die Personalstelle, dass beabsichtigt sei, ihn der Gemeinde zu melden, würde ich begrüßen. Dadurch würde der Betroffene in die Lage versetzt, dem Behördenleiter/der Personalstelle Gründe zu nennen, ihn von vornherein nicht auf die Liste zu setzen. Die eigentliche Eignungsprüfung erfolgt sodann bei der Gemeinde durch Abgleich mit dem Melderegister und/oder dem Wählerverzeichnis.

Aus datenschutzrechtlicher Sicht halte ich es für unabdingbar, dass die Gemeinden die entsprechenden Daten der von den Behörden benannten Beschäftigten, die für eine Tätigkeit im Wahlvorstand nicht in Frage kommen (z. B. weil sie noch nicht

lange genug in der Gemeinde wohnen, weil sie in der Gemeinde nicht mit Hauptwohnung gemeldet und damit nicht wahlberechtigt sind, weil aus sonstigen Gründen das Wahlrecht ruht oder weil familiäre, berufliche, gesundheitliche oder sonstige wichtige Gründen gegen die Übernahme des Ehrenamtes sprechen), zuverlässig löschen.

Hierauf sollten die anfordernden Gemeinden hingewiesen werden.

5.14 Sonstiges

5.14.1 Controlling in der Vermessungsverwaltung

Die grundsätzliche inhaltliche und strukturelle Neugestaltung der Vermessungsverwaltung hat das SMI zum Anlass genommen, modellhaft für diesen Verwaltungszweig ein Controllingsystem zur prozessorientierten Aufgabensteuerung zu entwickeln.

Vornehmlich werden dabei Informationen über den zeitlichen Aufwand der Bearbeitung der Produkte, nicht-produktbezogener Tätigkeiten und von Projekten erfasst. Diese Daten dienen der Durchführung organisatorischer Maßnahmen, insbesondere der Personalplanung, dem Personaleinsatz sowie der Steuerung von Aufgaben.

Da das vorgesehene Verfahren durchaus zur Verhaltens- und Leistungskontrolle der Beschäftigten geeignet ist, hatte ich angeregt, in einer Dienstvereinbarung (§ 80 Abs. 3 Nr. 16 SächsPersVG) eine Nutzung der Daten zu anderen als Controllingzwecken ebenso auszuschließen wie jede Verknüpfung der im Controllingverfahren gewonnenen Daten mit anderen automatisiert verarbeiteten Beschäftigtendaten, beispielsweise aus der Zeiterfassung oder einem Personalinformationssystem.

Zu dem mir vorgelegten Entwurf einer Dienstvereinbarung sowie des Datenschutz- und Datensicherheitskonzeptes (gemäß § 9 SächsDSG) habe ich einige Konkretisierungen vorgeschlagen: Eindeutig ist z. B. festzuhalten, dass ausschließlich der Controller (oder sein Stellvertreter) die Daten seiner Dienststelle erfassen und auswerten darf.

Da es sich bei den zu verarbeitenden Daten um Beschäftigtendaten handelt, ist die Schutzwürdigkeit der personenbezogenen Daten besonders hoch, denn eine Zweckentfremdung der Daten (z. B. zur Leistungskontrolle) könnte für den Betroffenen eine erhebliche Beeinträchtigung nach sich ziehen. Deshalb sind auch die Anforderungen an ein Sicherheitskonzept, das die Maßnahmen zur Gewährleistung des Schutzes personenbezogener Daten gemäß § 9 Abs. 2 SächsDSG festlegt, hoch.

Im Datenschutz- und Datensicherheitskonzept wird festgelegt, welche Behördenebene welcher Benutzergruppe bzw. Zugriffsebene zugeordnet wird. Im Sicherheitskonzept wird festgelegt, wer welche Zugriffsrechte differenziert für wen (Benutzerprofile) vergibt. Festgelegt werden muss aber auch, wann diese durch wen widerrufen

oder gelöscht werden, was beispielsweise auch für den vorgesehenen Vertreter des jeweiligen Controllers gilt.

Es sind Festlegungen über die Auswertung von Protokollen zu treffen. Das Aufzeichnen von Protokolldaten ist eine Maßnahme, damit nachträglich überprüft und festgestellt werden kann, welche Daten zu welcher Zeit von wem eingegeben (Eingabekontrolle) worden sind. Protokolldaten sollen insbesondere die Anmeldung (Identifikation und Authentisierung) beim Server und Client sowie die Zugriffe auf Daten und Programme und insbesondere das Verändern sensibler personenbezogener Daten nachprüfbar machen. Außerdem sollen sie den Nachweis einer ordnungsgemäßen Datenverarbeitung erbringen. Die Protokollierung ist nur dann sinnvoll, wenn sie regelmäßig ausgewertet wird. Für das Controllingverfahren ist der Nachweis einer ordnungsgemäßen Datenverarbeitung eine unabdingbare Voraussetzung. Deshalb sind in das Sicherheitskonzept Regelungen zur Protokollierung aufzunehmen.

An der Weiterentwicklung insbesondere der Einführung der für die staatlichen Vermessungsbehörden geplanten Kosten- und Leistungsrechnung (KLR) lasse ich mich gemäß § 31 Abs. 7 SächsDSG beteiligen.

In diesem Zusammenhang aber auch eine kritische Anmerkung: Die Erfassung der Anzahl erledigter Produkte pro Zeiteinheit halte ich für eine „Milchmädchen-Rechnung“, wenn die Qualität der Arbeit (konkreter Schwierigkeitsgrad, Zuverlässigkeit des Ergebnisses, Rechtsmittel-Beständigkeit, Kundenzufriedenheit) des einzelnen Bearbeiters unberücksichtigt bleibt. Deshalb kann auf Dauer ein Controlling nur dann wirklich sinnvoll sein, wenn Rechtsgrundlagen für eine Leistungskontrolle geschaffen werden. Ihr wird sich gerade der öffentliche Dienst stellen müssen.

5.14.2 Verwendung von Gerichtsurteilen in Lehrveranstaltungen der Akademie für öffentliche Verwaltung des Freistaates Sachsen (AVS)

Teilnehmer eines Seminars der AVS machten mich auf einen datenschutzrechtlich bedeutsamen Sachverhalt aufmerksam: Während ihres Seminars zum Thema „Vertriebenenrecht“ hatte der Dozent mehrere Urteile von Verwaltungsgerichten den Teilnehmern zur Mitnahme ausgelegt. Die Namen der an den Gerichtsverfahren Beteiligten sowie dritter Personen waren nicht geschwärzt. Das Verhalten des Dozenten, das datenschutzrechtlich der AVS zuzurechnen ist, habe ich als Verstoß gegen das Sächsische Datenschutzgesetz bewertet und es gegenüber dem Staatsminster des Innern förmlich beanstandet. Ich habe dies wie folgt begründet:

Die rechtlichen Voraussetzungen für die Auslage der Urteile konnten im vorliegenden Falle ersichtlich nicht erfüllt werden. Denn zu Ausbildungszwecken dürfen nach § 12 Abs. 3 Satz 2 SächsDSG personenbezogene Daten durch öffentliche Stellen nur genutzt werden, wenn überwiegende schutzwürdige Interessen der Betroffenen nicht entgegenstehen. Bei dieser Abwägung ist insbesondere auch die Rechtsprechung des Sächsischen Verfassungsgerichtshofs zur Nutzung personenbezogener Daten zu Zwecken der Aus- und Fortbildung zu beachten. Nach dem Urteil des Sächsischen Verfassungsgerichtshofs zum Sächsischen Polizeigesetz vom 14. Mai 1996 gebietet

es Art. 33 SächsVerf, bei der Entscheidung über die Datennutzung zu Aus- und Fortbildungszwecken darauf zu achten, dass die berechtigten Interessen des Betroffenen an der Geheimhaltung seiner Daten regelmäßig überwiegen und nur ausnahmsweise zurücktreten müssen. Hieraus ergab sich für den vorliegenden Fall folgendes: Angesichts der Inhalte der ausgelegten Urteile, die sämtlich eine intensive begutachtende Beschreibung des familiären Umfelds und der intellektuellen Eigenschaften der am vertriebenenrechtlichen Aufnahmeverfahren Beteiligten enthielten, lag deren überwiegendes schutzwürdiges Interesse am Unterbleiben der Datennutzung nicht nur auf der Hand; vielmehr war die vom Dozenten vorgenommene Verbreitung von gerichtlichen Feststellungen zu Fähigkeits- und Kenntnisdefiziten der betroffenen Personen auch durchaus geeignet, diese zu diskriminieren.

Die Vermittlung von Wissen zum Vertriebenenrecht wäre ohne weiteres auch mit nicht personenbezogenen (oder pseudonymisierten) Urteilsauszügen zu erreichen gewesen. Im Rahmen der meiner Beanstandung vorausgegangenen Anhörung nach § 26 Abs. 1 SächsDSG vertrat die AVS die Auffassung, dass die Verwendung der ungeschwärzten Entscheidungsabschriften „aus fachlich-sachlichen Gründen“ geboten gewesen sei und akzeptierte den Einwand des zum Vorfall angehörten Dozenten, Urteile zur Vertriebenenanerkennung seien „tatsächlich nur ungeschwärzt nachvollziehbar“.

Dem habe ich in meiner Beanstandung energisch widersprochen, hieße dies doch, dass die Vermittlung juristischen Wissens nur noch einzelfallorientiert und nicht mehr in abstrakten Zusammenhängen gestaltet werden kann. Schließlich wäre auch die Verwendung von „echten“ Gerichtsentscheidungen im Rahmen der Lehrveranstaltungen durchaus möglich gewesen, wenn sich der Dozent der zumutbaren Mühe unterzogen hätte, die Entscheidungen zu pseudonymisieren. Die Anschaulichkeit der Lebenssachverhalte und deren vom Dozenten geforderte, didaktischen Zwecken dienende Subsumierbarkeit hätte somit in keiner Weise eingeschränkt werden müssen.

Weil der Dozent - wie seine Einlassung zum Sachverhalt anschaulich belegte - die erforderliche Einsicht in die einfachen rechtlichen Zusammenhänge der Nutzung personenbezogener Daten zu Ausbildungszwecken vermissen ließ, habe ich gegenüber dem SMI im Rahmen der nach § 26 Abs. 1 SächsDSG gebotenen Mängelbeseitigung angeregt, vom weiteren Einsatz des Dozenten an der AVS abzusehen. Ferner habe ich das SMI gebeten, für künftige Lehrveranstaltungen aufsichtlich zu gewährleisten, dass nur anonymisierte/pseudonymisierte Fallbeispiele Verwendung finden.

Das SMI hat sich meiner datenschutzrechtlichen Bewertung des Falles angeschlossen und auf meine Beanstandung sofort mit einem Katalog von Maßnahmen gegenüber der AVS reagiert:

1. Der Hinweis auf die Berücksichtigung datenschutzrechtlicher Belange bei der Gestaltung von Lehrveranstaltungen wird direkter Bestandteil des vom Dozenten zu unterzeichnenden Lehrvertrages.

2. Die von den Dozenten eingereichten Lehrgangsunterlagen sind von der AVS auf Datenschutzverstöße zu überprüfen. Hierbei kommt der persönlichen Kontrollpflicht des Direktors der AVS besondere Bedeutung zu.

3. Die AVS ist angewiesen, von der weiteren Zusammenarbeit mit dem in Rede stehenden Dozenten Abstand zu nehmen.

6 Finanzen

6.1 Führung von Fahrtenbüchern durch Ärzte für steuerliche Zwecke

In 6/6.4 und 6/6.5 habe ich mich ausführlich mit dem Zeugnisverweigerungsrecht der Ärzte in Steuerangelegenheiten befasst und insbesondere darauf hingewiesen, dass die Offenbarung des Patientennamens für steuerliche Zwecke wegen fehlender Rechtsgrundlage nicht verlangt werden kann.

Der BfD hat das BMF im Juli 1998 dementsprechend beanstandet.

Die Referatsleiter Abgabenordnung der obersten Finanzbehörden des Bundes und der Länder haben sich Anfang Dezember 1998 mit dem Thema befasst und - so teilte es mir das SMF mit - die Beanstandung des BfD gegenüber dem BMF als nicht berechtigt angesehen.

Die nach Ansicht der Datenschutzbeauftragten des Bundes und der Länder rechtswidrige Praxis wird demnach beibehalten. Falls es nicht doch noch zu einem Einlenken der Finanzbehörden kommt, kann eine Änderung durch Klagen betroffener Ärzte erreicht werden.

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

Ebenso wie die Veröffentlichungspraxis der Steuerberaterkammer des Freistaates Sachsen (vgl. oben unter Nr. 6.1) sind die Datenerhebungen der Finanzämter über Reiseteilnehmer aufgrund der entsprechenden Weisung der OFD Chemnitz vom 27. Juni 1996 ein datenschutzrechtlicher Dauerbrenner, wohl weil sich meine Rechtsauffassung grundlegend von der des SMF unterscheidet (vgl. 5/6.2 und 6/6.3).

Der vom SMF getragenen Weisung der OFD Chemnitz zufolge sollen die Namen und Anschriften der Reiseteilnehmer 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.

Ein Urteil des Finanzgerichts Düsseldorf vom 27. Juni 1996, Az.: S 2227-38-St31, ließ nun die Hoffnung in mir keimen, dass das SMF sich endlich auf das auch den

Steuerpflichtigen zustehende Grundrecht auf informationelle Selbstbestimmung besinnt. In dem Urteil heißt es u. a. nämlich, dass die Ermittlung von Namen und Anschriften der übrigen Reiseteilnehmer lediglich zu Kontrollmitteilungszwecken nicht gerechtfertigt sei.

Anders die Praxis. In einem von mir konkret untersuchten Fall forderte das Finanzamt ein Reisebüro auf, Namen und Anschriften der Reiseteilnehmer einer vom SMK angebotenen Israelreise zu nennen. Der Stellungnahme des Finanzamtes zufolge sollten die Daten *ausschließlich Kontrollmitteilungszwecken* dienen.

Ich habe dem SMF daher unter Übersendung des o. a. Urteils mitgeteilt, dass ich nach wie vor die Übermittlung der Namen und Anschriften von Reiseteilnehmern an deren Finanzämter zu Kontrollzwecken mangels Rechtsgrundlage für unzulässig halte. Die Anweisung der OFD Chemnitz vom 27. Juni 1996 an die Finanzämter, personenbezogene Kontrollmitteilungen zu versenden, stellt keine für solche Übermittlungen erforderliche Rechtsgrundlage dar. Ungeachtet dessen fehlt es an der Erforderlichkeit solcher personenbezogenen Übermittlungen. Im Urteil des Finanzgerichts Düsseldorf wird beispielsweise auf die Möglichkeit verwiesen, über die OFDen einen Kontrollhinweis an die Finanzämter mit der Maßgabe zu veranlassen, dass *für eine bestimmte Reise* Betriebsausgaben oder Werbungskosten nicht anerkannt wurden. Hierzu sind Namen und Anschriften sowohl des Steuerpflichtigen als auch der übrigen Reiseteilnehmer allerdings *nicht* erforderlich. Solche Hinweise bedürfen keiner Rechtsgrundlage, zumal sie keine personenbezogenen Daten beinhalten.

Grundsätzlich ist dem Urteil aber auch zu entnehmen, dass entsprechende Kontrollmitteilungen überhaupt nicht erforderlich sind, weil die Finanzämter aufgrund ihrer eigenen Prüfungskompetenz auf das Ergebnis der steuerlichen Prüfung der Abzugsfähigkeit durch ein anderes Finanzamt letztlich nicht angewiesen sind. Dies ist auch sinnvoll. Schließlich kann das Finanzamt, das die Kontrollmitteilung erhält, zu einer anderen steuerlichen Bewertung kommen, weil das übermittelte Ergebnis rechtswidrig war oder dem konkret zu besteuernden Fall völlig andere Voraussetzungen zugrunde lagen. Der Grundsatz der einheitlichen Besteuerung erlaubt es nicht, der Kontrollmitteilung folgend ebenso rechtswidrig zu entscheiden.

Es sollte nicht schwerfallen, die OFD-Verfügung vom 27. Juni 1996 entsprechend zu modifizieren. Das SMF hat mittlerweile signalisiert, in der OFD-Verfügung klarstellen zu lassen, dass die Anforderung von Teilnehmerverzeichnissen im Rahmen des § 93 AO nur dann möglich ist, wenn dies zur steuerlichen Bewertung *des Einzelfalles erforderlich* ist, also kein Wort mehr von „Kontrollmitteilungen“.

Die weitere Entwicklung behalte ich im Auge.

6.3 Informationszentrale für den Steuerfahndungsdienst (IZ-Steufa) in Wiesbaden

Durch Verwaltungsvereinbarung der Bundesländer wurde 1977 die IZ-Steufa in Wiesbaden errichtet. Die IZ-Steufa hat die Aufgabe, mittels einer Steuerstraftäter-

kartei Auskunft über Steuerstraftäter und Tätermerkmale zu geben. Sie nimmt Informationen der mit der Steuerfahndung und sonstigen mit der Führung von Ermittlungen in Steuerstrafsachen (Entscheidung in Steuerordnungswidrigkeiten) betrauten Dienststellen der Landesfinanzbehörden entgegen, wertet sie aus und gibt diesen Dienststellen Auskunft. Die Karteikarten werden nach zehn Jahren aussortiert und vernichtet. Die Verwaltungsvereinbarung wurde 1995 auf die neuen Bundesländer ausgedehnt.

Die IZ-Steufa betreibt nach Auffassung der Datenschutzbeauftragten des Bundes und der Länder Auftragsdatenverarbeitung für die einzelnen Bundesländer (Beschluss der 13. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 28. September 1982).

Dem SMF habe ich meinen datenschutzrechtlichen Standpunkt mitgeteilt:

Die sächsischen Finanzbehörden haben im Rahmen des § 7 SächsDSG als Auftraggeber sicherzustellen, dass die Daten nur so lange bei der IZ-Steufa gespeichert bleiben, wie es zur Aufgabenerfüllung der Finanzämter erforderlich ist (§ 19 Abs. 1 Nr. 2 SächsDSG). Nach meiner Kenntnis ist pauschal festgelegt, dass die einzelnen Karteikarten nach zehn Jahren auszusortieren sind. Darüber hinaus sei seit kurzem vorgesehen, dass der Betroffene nach einer Einstellung des Ermittlungsverfahrens über die Speicherung und darüber unterrichtet wird, dass er die sofortige Löschung der ihn betreffenden Daten *verlangen* könne.

Vorsorglich habe ich darauf hingewiesen, dass eine solche Regelung mit § 19 Abs. 1 Nr. 2 SächsDSG nicht vereinbar ist. Die Daten müssen von Amts wegen - also ohne „Verlangen“ des Betroffenen - gelöscht werden, wenn ihre Kenntnis für die Finanzverwaltung nicht mehr erforderlich ist.

Dieser Grundsatz lässt übrigens auch eine undifferenzierte Speicherungsdauer von zehn Jahren nicht zu. Vielmehr ist unter Beachtung des Verhältnismäßigkeitsgrundsatzes bei der Speicherungsdauer z. B. nach der Schwere der Tat, der verhängten Sanktion und einer denkbaren Wiederholungsgefahr zu unterscheiden. Solche Festlegungen hat aber nicht die IZ-Steufa zu treffen, sondern die auftraggebende Steuerverwaltung.

Ich habe das SMF gebeten, für eine den Anforderungen des § 19 Abs. 1 Nr. 2 SächsDSG entsprechende differenzierte Speicherungsdauerregelung zu sorgen und mich über die weitere Vorgehensweise zu unterrichten.

6.4 Veröffentlichung personenbezogener Daten bei Verurteilungen und strafbewehrten Unterlassungserklärungen im Kammerbrief der Steuerberaterkammer des Freistaates Sachsen

Seit 1996 plage ich mich damit ab, das SMF und die Steuerberaterkammer des Freistaates Sachsen von der Unzulässigkeit der personenbezogenen Veröffentlichungspraxis zu überzeugen (vgl. 5/6.6 und 6/6.2). Das Hin und Her gipfelte

letztendlich darin, dass die Steuerberaterkammer des Freistaates Sachsen unter Hinweis auf ein Urteil des Amtsgerichts Weißwasser, das sich mit Schadensersatzansprüchen eines Wettbewerbsstörers auseinandersetzte, im Juni 1998 die vorübergehend ausgesetzte Veröffentlichungspraxis (offenbar in Unkenntnis, dass ein Amtsgerichtsurteil eine fehlende Rechtsgrundlage nicht zu ersetzen vermag) wieder aufnahm. Meine förmliche Beanstandung der rechtswidrigen Veröffentlichungspraxis wurde mit dem Hinweis ignoriert, dass man *keinen Verstoß gegen Rechtsnormen sehe*, eine Ansicht, die übrigens auch die Bundessteuerberaterkammer in einem Schreiben von Anfang November 1998 an den BMF teilt.

Diese bizarr anmutende Rechtsauffassung zur Gesetzmäßigkeit der Verwaltung (Art. 20 Abs. 3 GG, Art. 3 Abs. 3 SächsVerf) veranlasste mich, die Steuerberaterkammer an folgende Grundsätze zu erinnern:

- Vorrang des Gesetzes = kein Handeln *gegen* das Gesetz,
- Vorbehalt des Gesetzes = kein Handeln *ohne* Gesetz.

Im vorangegangenen Schriftwechsel habe ich immer wieder herausgestellt, dass die Veröffentlichung in den Kammermitteilungen *ohne* ausreichende Rechtsgrundlage erfolgt und damit

1. gegen den Vorbehalt des Gesetzes und
2. gegen Art. 33 SächsVerf verstoßen wird, wonach das Recht auf informationelle Selbstbestimmung nur durch Gesetz oder aufgrund eines Gesetzes eingeschränkt werden darf.

Ein Eingriff in das Grundrecht ist demgemäß nur auf gesetzlicher Grundlage gestattet. Ist keine gesetzliche Befugnis ersichtlich, so darf die Veröffentlichung der Daten eben gerade *nicht* erfolgen. Oder, noch einfacher: Wir haben es mit einem verfassungsrechtlichen Verbot mit Erlaubnisvorbehalt zu tun. Fehlt diese Erlaubnis - wie ersichtlich - so ist jeder Umgang mit personenbezogenen Informationen rechtswidrig.

Verschiedene Steuerberaterkammern anderer Bundesländer haben daher aufgrund von Beanstandungen bzw. angedrohten Beanstandungen der dortigen Datenschutzbeauftragten die Veröffentlichungspraxis eingestellt (z. B. Berlin, Saarland, Schleswig-Holstein, Brandenburg, Niedersachsen). Einer Umfrage zufolge erfolgen die (rechtswidrigen) Veröffentlichungen in nur sieben Bundesländern.

Da sich die Steuerberaterkammer des Freistaates Sachsen - nicht zuletzt bestärkt durch das o. a. Schreiben der Bundessteuerberaterkammer - beharrlich weigert, die Veröffentlichungspraxis einzustellen, habe ich die Aufsichtsbehörde - das SMF - gebeten, den rechtswidrigen Zustand im Wege der Aufsicht zu beenden. Das SMF hat mir unter Hinweis auf ein Urteil des LG Meiningen vom 18.11.1998, 2 HKO 84/98, mitgeteilt, dass es nach nochmaliger Gegenüberstellung der im Rahmen des zu dieser Angelegenheit geführten umfangreichen Meinungsaustausches vertretenen Rechtsauffassungen und Abwägungen keine ausreichende Basis sieht, rechtsaufsichtliche Maßnahmen gegen die Steuerberaterkammer des Freistaates Sachsen zur Einstellung

ihrer Veröffentlichungspraxis zu ergreifen. Dies bedaure ich sehr, zumal das o. a. Urteil des LG Meiningen unrealistisch davon ausgeht, dass die Kammermitteilungen nur den Kammermitgliedern und keinen sonstigen Dritten zur Kenntnis gelangen.

Das Landgericht Meiningen hat als Prüfungsmaßstab ausschließlich § 1 UWG angelegt und datenschutzrechtliche Fragen im Rahmen des verhandelten Verfahrens außer Acht gelassen. Der konkrete Fall hätte Anlass sein müssen zu prüfen, inwieweit Datenschutzverstöße im Rahmen von § 1 UWG geltend gemacht werden können.

Auch soweit indirekte Bezüge bestehen, hat es das Gericht unterlassen, Datenschutzrecht zur Kenntnis zu nehmen. So wird die „kammerinterne“ Mitteilung nicht unter den Begriff „Veröffentlichung“ subsumiert, obwohl der Kreis der Mitteilungsempfänger eines Druckerzeugnisses erfahrungsgemäß nicht abgrenzbar ist. Dass es sich hierbei auf jeden Fall um eine Datenübermittlung aus dem öffentlichen in den privaten Bereich handelt, die nach dem jeweiligen Landesdatenschutzgesetz (in Sachsen z. B. § 15 SächsDSG) engen Voraussetzungen unterliegt, wird nicht erörtert. Offenbar ist vom Gericht auch nicht hinreichend gewürdigt worden, dass die Kammermitteilungen nicht nur den Kammermitgliedern, sondern sehr wohl auch anderen Privaten zur Kenntnis gelangen. Die Voraussetzungen des § 15 SächsDSG sind jedenfalls nicht erfüllt (vgl. 6/6.2). Das Gericht erörtert auch nicht ansatzweise die Frage, ob die „kammerinterne“ Datenübermittlung (die wie gesagt, auch anderen als Kammermitgliedern - auf welchem Weg auch immer - zugeht) geeignet ist, das erklärte Ziel, die Kammermitglieder vor unlauterem Wettbewerb zu schützen, zu erreichen.

Ebenso wenig wird die Frage der Erforderlichkeit und der Angemessenheit der Maßnahme im Hinblick auf das verfolgte Ziel erörtert. Dabei reicht es nicht aus, dass die Veröffentlichung diesem Ziel dienlich ist, denn eine Prangerwirkung ist ein sehr erheblicher Eingriff in das Persönlichkeitsrecht. Es wird lediglich festgestellt, dass die Steuerberaterkammer bei der Verfolgung von Wettbewerbsverstößen „auf die Kontrolle und Einflussnahme ihrer Mitglieder angewiesen“ sei. Inwieweit diese Unterstützung der Kammermitglieder durch die namentliche Benennung der Personen, die eine Unterlassungserklärung abgeben mussten, gefördert wird, wird nicht dargetan. In keinem Fall ist begründbar, dass diese Unterstützung eine namentliche Bekanntgabe an die Kammermitglieder (und letztlich an Außenstehende) voraussetzt.

Das Gericht erkennt zwar, dass Kammermitglieder die Bekanntgabe der Abmahnungen missbräuchlich für eigene Wettbewerbsvorteile und Geschäftszwecke verwenden. Dieser Aspekt wird von ihm aber datenschutzrechtlich nicht gewürdigt. Eine missbräuchliche Datennutzung stellt eine Zweckänderung dar, die nach dem für Private geltenden § 28 Abs. 4 BDSG engen Anforderungen unterliegt. Die Gefahr einer zweckwidrigen Datennutzung hat regelmäßig Auswirkungen auf die Rechtsmäßigkeit der Datenübermittlung. So fordert § 15 Abs. 1 Nr. 2 SächsDSG bei einer Datenübermittlung ausdrücklich die Berücksichtigung der schutzwürdigen Interessen des Betroffenen, die die Steuerberaterkammer regelmäßig gemäß § 15 Abs. 3 SächsDSG abfragen müsste.

Nicht zu vergessen ist auch die historische Entwicklung der Angelegenheit. Während die Steuerberaterkammer ihre Veröffentlichungspraxis zunächst mit der „analogen" Anwendung des § 23 Abs. 2 UWG zu rechtfertigen versuchte (vgl. 5/6.6), strapazierte man - nachdem eingesehen wurde, dass diese Bestimmung nicht einschlägig ist - in der Folgezeit Urteile des LG Kiel und des AG Weißwasser (beide nicht anwendbar) sowie den mehrheitlichen Beschluss der Berufsreferenten des Bundes und der Länder, der aber die fehlende gesetzliche Grundlage nicht zu ersetzen vermag. Auch das Schreiben der Bundessteuerberaterkammer vom 5. November 1998, Az.: H/K, an den Bundesminister der Finanzen ist nicht geeignet, die Veröffentlichungspraxis zu legitimieren (siehe oben).

In der Gesamtschau stellt sich mir die Rechtslage eindeutig dar. Ohne ausreichende Rechtsgrundlage sind die Veröffentlichungen durch die Steuerberaterkammer des Freistaates Sachsen nach wie vor rechtswidrig, so dass ich das SMF unter Hinweis auf § 25 Satz 1 SächsDSG nochmals gebeten habe, bei der Steuerberaterkammer des Freistaates Sachsen die von mir beanstandeten Veröffentlichungen im Wege der Rechtsaufsicht zu unterbinden.

6.5 Landeseinheitliche Fördermitteldatenbank

Es existieren unterschiedliche Quellen für Fördermittel (von der EU bis zur Kommune) genauso wie eine Vielzahl von Bewilligungs- und Bearbeitungsstellen. Gleiches gilt auch für die rechtlichen Grundlagen. Fördermittel werden aufgrund diverser Haushaltseinstellungen (EU, Bund, Land, Kommunen) ausgegeben. Auf Landesebene erfolgt die Veranlassung in einigen Fällen direkt durch spezialrechtliche Regelungen, in anderen Fällen nur durch die Einstellung im Haushaltsplan des Landes. Um eine wirksame Übersicht und ein geeignetes Controlling-Instrument zu bekommen, hat die Staatsregierung sich zum Ziel gesetzt, eine einheitliche landesumfassende Fördermitteldatenbank zu entwickeln. Die Datenbank wird bei der Staatskanzlei angesiedelt; in die technische Umsetzung ist das Statistische Landesamt einbezogen. Im Zuge der Bearbeitung eines jeden Fördermittelantrages sollen antragsbezogene Daten in die Datenbank eingespeist werden, so dass dann eine effektive landesweite Analyse aller Förderbereiche möglich ist. Daneben soll die Datenbank die Ausübung der Rechts- und Fachaufsicht unterstützen sowie eine Überprüfung ermöglichen, ob Anhaltspunkte für eine rechtswidrige Förderung vorliegen. Dann werden personenbezogene Daten durch eine Stelle verarbeitet, die nichts mit der eigentlichen Fördermittelverwaltung und Antragsbearbeitung zu tun hat. Bereits in 5/6.5 habe ich dafür eine bereichsspezifische gesetzliche Grundlage angemahnt. Diese ist mittlerweile von der Staatskanzlei erarbeitet worden und wird derzeit im Parlament behandelt.

Im Gesetzentwurf werden zwei Dinge geregelt: Zum einen die landeseinheitliche Fördermitteldatenbank und die Ressortdatenbanken, die ressortinterne Analyseinstrumente sind, und zum anderen die landeseinheitliche Fördermittelverwaltung, also die direkt für die Antragsbearbeitung eingesetzten Verfahren.

Die Bearbeitung der konkreten Fördervorhaben richtet sich nach spezialrechtlichen Regelungen oder nach § 44 der Sächsischen Haushaltsordnung. Art und Umfang der

Verarbeitung personenbezogener Daten bei der Fördermittelverwaltung werden durch diese Rechtsgrundlagen, soweit es in ihnen geregelt ist, bestimmt. Ansonsten gilt als Auffanggesetz das Sächsische Datenschutzgesetz. Bei der Prüfung, auf welcher rechtlichen Grundlage die Verarbeitung personenbezogener Daten in der Fördermittelverwaltung erfolgt, muss also immer der Einzelfall betrachtet werden. Eine generelle Regelung würde sich zum einen in Konkurrenz zu den spezialrechtlichen Regelungen setzen, zum anderen aber vor allem dem Bestimmtheitsgebot des Volkszählungsurteils widersprechen. Deshalb war in dem Gesetzentwurf aus datenschutzrechtlicher Sicht nur die Verarbeitung personenbezogener Daten für die Landeseinheitliche Fördermitteldatenbank und die Ressortdatenbanken zu regeln.

Der Gesetzentwurf erlaubt die Verarbeitung personenbezogener Daten für die o. g. Zwecke, wobei der konkrete Datensatz durch Rechtsverordnung festgelegt wird. Dies ist sinnvoll, da hier (im Gegensatz z. B. zum Meldewesen) kein festumrissener Datenkatalog existiert, der gesetzlich normiert werden kann, sondern eine Vielzahl von einzelnen Förderregelungen mit unterschiedlichen Datensätzen vorhanden ist, die wegen der laufenden Veränderung der Förderprogramme auch ständig geändert werden. Ferner werden Übermittlungsregelungen aufgestellt, sowohl von den fördermittelbearbeitenden Stellen zur Fördermitteldatenbank hin als auch für die Gegenrichtung im Falle einer rechtswidrigen Förderung. Für diese Übermittlungen ist der Einsatz automatisierter Abrufverfahren möglich, wobei die Staatsregierung die konkreten Einzelheiten ebenfalls durch Rechtsverordnung zu regeln hat. Eine spezielle Regelung im technischen Bereich findet sich nicht, so dass in diesem wie in allen nicht geregelten anderen Fällen das Sächsische Datenschutzgesetz als Auffanggesetz gilt. Die Frage, ob vor dem Hintergrund der rasanten Entwicklung der Informationstechnik ausreichende technische Sicherheitsvorkehrungen für den Betrieb der Datenbank getroffen werden, hat also eher in der Diskussion um die Novellierung des Sächsischen Datenschutzgesetzes ihren Platz (siehe unten 14.6).

An der Erarbeitung des Entwurfes war ich intensiv beteiligt. Die Staatskanzlei hat alle meine Anregungen aufgenommen. Die Zusammenarbeit war beispielgebend konstruktiv und ergebnisorientiert. Ich bin zuversichtlich, dass sich dies auch bei der noch kommenden Arbeit an den Rechtsverordnungen fortsetzen wird.

7 Kultus

7.1 Zuschüsse für Förderschulen in freier Trägerschaft

Die als Ersatzschulen genehmigten Schulen in freier Trägerschaft erhalten Zuschüsse vom Freistaat Sachsen. Einzelheiten regelt die Verordnung der Sächsischen Staatsregierung über die Gewährung von Zuschüssen für Schulen in freier Trägerschaft vom 16. Dezember 1997 (ZuschussVO).

Bei Förderschulen bemisst sich die Höhe des Zuschusses nicht nur nach einem festgelegten Satz pro Schüler (wie bei anderen Schularten), sondern auch nach den

tatsächlichen Personalkosten, allerdings pro Lehr- und Erziehungskraft höchstens bis zu dem Betrag, der sich bei Anwendung der im öffentlichen Dienst geltenden Tarifverträge ergeben würde. Dies erfordert eine Vergleichsberechnung. Deshalb hat der freie Träger dem zuständigen Oberschulamt das Personal und die entsprechende Vergütung zu melden (§ 2 Abs. 3 ZuschussVO).

Ein freier Schulträger hielt die vom Oberschulamt für diese Zwecke verwendeten Formblätter für nicht datenschutzgerecht und bat mich um Prüfung. Da ich ihm nur beipflichten konnte, habe ich die Bedenken an das SMK, das den Oberschulämtern die Vorgaben gemacht hatte, herangetragen.

Ich kritisiere, dass den Formblättern zufolge die Daten nicht wie in § 2 Abs. 3 ZuschussVO vorgesehen beim Träger, sondern personenbezogen bei den einzelnen Lehr- und Erziehungskräften zusammen mit einer Erklärung über die Richtigkeit der gemachten Angaben erhoben werden sollten. Künftig werden die Daten richtigerweise beim Träger erhoben, und zwar ohne Namensangabe der Beschäftigten. Ich konnte das SMK davon überzeugen, dass die Namen entbehrlich sind und Zweifelsfälle auch über Schlüsselnummern geklärt werden können, die der Träger vergibt.

Bei den für die Vergleichsberechnung benötigten Daten hat sich eine äußerst unbefriedigende Situation ergeben. Zwar wurden alle nicht erforderlichen Daten vom Vordruck gestrichen. Wie sich jedoch zeigte, fehlten für eine Vergleichsberechnung etliche Daten. Da § 15 Abs. 3 Satz 1 SächsFrTrSchulG eine „pfenniggenaue“ Berechnung auf tarifrechtlicher Basis vorsieht, kann auf die Daten nicht verzichtet werden. Nunmehr werden die zur Bezügeberechnung der Landesbediensteten verwendeten Formblätter, die sehr viel mehr Angaben erfordern als das ursprüngliche Formblatt, eingesetzt.

Ich habe inzwischen Gespräche mit dem SMK geführt und mich für eine pauschalierte Regelung eingesetzt. Dies würde nicht nur den Umfang der zu verarbeitenden personenbezogenen Daten erheblich reduzieren, sondern auch die Schulaufsichtsbehörden davon entlasten, sich mit der komplizierten Materie des Tarifrechts zu befassen.

7.2 Förderschulen - Schulbezeichnung, Gestaltung von Schülerausweisen

In Sachsen gibt es viele Förderschulen (§ 13 Abs. 1 Nr. 1-9 SchulG) folgender Typisierung:
1. Schulen für Blinde und Sehschwache
2. Schulen für Gehörlose und Schwerhörige
3. Schulen für geistig Behinderte
4. Schulen für Körperbehinderte (auch innere Organe)
5. Schulen für Lernbehinderte
6. Sprachheilschulen
7. Schulen für Erziehungshilfe
8. berufsbildende Schulen für Behinderte
9. Klinik- und Krankenhausschulen.

Nach § 2 Abs. 2 SOFS bereiten die Förderschulen u. a. ihre Schüler auf ein selbständiges Leben in der Gemeinschaft vor. Mit ihren Schülern und deren Erziehungsberechtigten halten sie einen besonders engen Kontakt.

Ob diesem Ziel durch die Bezeichnung der jeweiligen Förderschule (Schulbeschilderung, Briefkopf, Gestaltung des Dienstsiegels und der Schülerausweise) in der Öffentlichkeit gedient wird, habe ich gegenüber dem SMK kritisch in Frage gestellt. Man stelle sich nur vor, was Eltern oder Schüler erleiden müssen, wenn sie gegenüber Außenstehenden den Schultyp nennen müssen, um die Schule näher zu bezeichnen. Es werden dann mit dem Schüler Informationen verbunden, unter denen er unnötig leidet oder deretwegen er sich u. U. schämt.

Insbesondere habe ich darauf hingewiesen, dass sowohl die Schülerausweise der aus § 13 Abs. 1 Nr. 1-9 SchulG ersichtlichen Förderschulen als auch deren Dienstsiegel bei Vorlage eine nicht zu unterschätzende Prangerwirkung entfalten, die sich schwerlich mit Art. 14, 15 SächsVerf (Menschenwürde und Persönlichkeitsrecht) vereinbaren lässt. Beispielsweise läuft der Schüler einer *Schule für Erziehungshilfe*, der zwecks Inanspruchnahme eines ermäßigten Eintrittspreises seinen Schülerausweis vorzeigt, Gefahr, nicht zu einer Veranstaltung eingelassen zu werden (Furcht vor „Randale“). Über subjektive Empfindungen der Veranstalter bei Schülerausweisen i. S. v. § 13 Abs. 1, insbesondere der Nrn. 3, 4, 5, 6 und 8 SchulG braucht wohl nicht spekuliert zu werden.

Mein Anliegen ist es deshalb, im Interesse der betroffenen Schüler einen Weg zu finden, der die Beeinträchtigung ihrer Menschenwürde und ihres Persönlichkeitsrechts auf ein Minimum reduziert. Den Hinweis des SMK, dass *keine Pflicht* zur Beantragung eines Schülerausweises besteht, halte ich jedenfalls zur Lösung des Problems für nicht zielführend. Vielmehr habe ich Überlegungen angeregt, ob nicht anstelle der Bezeichnung des auf die Behinderung hinweisenden Schultyps ein neutraler (amtlicher) Name treten kann (z. B. „Oskar-von-Miller-Schule“, „Schule an der Mendelssohnallee“).

Dieser Vorschlag gewinnt insbesondere auch im Hinblick auf die Schulabschlusszeugnisse, die künftigen Bewerbungen stets beizufügen sind, an Bedeutung. Wenn mit dem Abschlusszeugnis eine normale Schulbildung endet, bedarf es in diesem Zeugnis keines Hinweises auf den Schultyp.

Das SMK hat sich meinem Anliegen nicht verschlossen und signalisiert, Lösungsvorschläge zur Minimierung der Prangerwirkung, insbesondere bei der Gestaltung von Schülerausweisen, erarbeiten zu wollen.

Aus meiner Sicht ist kein durchgreifender Grund ersichtlich, weshalb der Schultyp (Nr. 1 bis 9) nach außen beim Publikum in Erscheinung treten müsste. Im dienstlichen Verkehr mag dies nötig sein - aber eben nur dort.

7.3 Videomitschnitt von Unterrichtsstunden

Ich bin nach den Voraussetzungen gefragt worden, unter denen im Rahmen der praktischen Lehrerausbildung Videoaufzeichnungen vom Unterricht für eine spätere

Auswertung erstellt werden dürfen. Gedacht war dabei sowohl an Lehrfilme für eine längerfristige Nutzung als auch an Videos, die nach ihrer Auswertung unverzüglich gelöscht werden.

Die Rechtslage stellt sich wie folgt dar:

Die für den Schulbereich und die Lehrerausbildung geltenden Rechtsvorschriften enthalten keine Regelungen über Videoaufzeichnungen im Unterricht, so dass sich die Zulässigkeit nach dem Sächsischen Datenschutzgesetz richtet.

Videoaufzeichnungen sind eine spezielle Form der Datenerhebung. Gemäß § 11 Abs. 1 SächsDSG muss diese zur Aufgabenerfüllung der erhebenden Stelle *erforderlich* sein. Die Erforderlichkeit könnte in der Verbesserung der theoretischen Ausbildung durch den Einsatz dieses Mediums liegen.

Da die Betroffenen allerdings nicht verpflichtet sind, sich filmen zu lassen, sind Freiwilligkeit und schriftliche Einwilligung Voraussetzung; zu dieser Lösung zwingen auch die Vorschriften zum „Recht am eigenen Bild“ (§ 22 KunstUrhG). Beim Einholen der Einwilligung ist auf den Verwendungszweck der Daten, die Freiwilligkeit der Teilnahme sowie auf etwaige Folgen einer Verweigerung der Einwilligung hinzuweisen, wobei dem Betroffenen trotz Verweigerung keine Nachteile entstehen dürfen (§§ 4 Abs. 2 und 3, 11 Abs. 2 SächsDSG).

Die Umsetzung dürfte bei den betroffenen Lehramtsanwärtern, ihren Ausbildern sowie ggf. anwesenden Lehrern unproblematisch sein.

Bei Schülern stellt sich jedoch die Frage, *wer* die Einwilligung erteilen soll; denn die datenschutzrechtliche Einwilligung ist nicht von der bürgerlich-rechtlichen Geschäftsfähigkeit abhängig, sondern von der Einsichtsfähigkeit des Betroffenen. Diese wird bei normal entwickelten Kindern etwa ab dem 15. Lebensjahr angenommen. Ansonsten ist die Einwilligung zumindest eines Sorgeberechtigten erforderlich.

Wegen der „besonderen Qualität“ der per Video erhobenen Daten halte ich jedoch auch bei Schülerinnen und Schülern zwischen dem 15. und 18. Lebensjahr die zusätzliche Einwilligung eines Sorgeberechtigten für notwendig. Die „besondere Qualität“ liegt in dem Mehr an Informationen, die auch Rückschlüsse auf familiäre Verhältnisse zulassen. Im Gegensatz zum Gedächtnis zeichnet ein Video nicht nur das gesprochene Wort „wortwörtlich“ (einschließlich mundartlicher Merkmale wie z. B. Sächsisch, Bayerisch, Hochdeutsch) und jede Geste auf, sondern hält auch körperliche Merkmale (z. B. ethnische Zugehörigkeit, Behinderung), Kleidung (gepflegt/ungepflegt, teuer/billig) und Attribute einer bestimmten Gruppen- oder Religionszugehörigkeit (z. B. Kopftuch, rasierter Schädel, Piercing) auf Dauer verfügbar.

Beim Erstellen der Videos ist darauf zu achten, dass Personen, die nicht eingewilligt haben, nicht im Bild erscheinen. Zu Kontrollzwecken könnte das Video der Klasse vorgeführt werden.

Unter Nr. 16.2 ist die vom SMK inzwischen verbindlich vorgeschriebene Einwilligungserklärung abgedruckt, die auf einem Vorschlag von mir basiert.

7.4 Geschäftsmäßige Durchführung von Klassentreffen

Eine Agentur, die geschäftsmäßig Klassentreffen organisiert, beabsichtigte auch in Sachsen im Wege eines Adressmittlungsverfahrens Kontakt mit den an einem Klassentreffen interessierten ehemaligen Schülern aufzunehmen und fragte, ob gegen das Vorhaben datenschutzrechtliche Bedenken bestünden. Es sei vorgesehen, die Anschreiben den Schulen in frankierten Blankoumschlägen mit der Bitte zu übergeben, sie zu adressieren und zur Post zu geben. Es bliebe sodann den ehemaligen Schülern überlassen, Kontakt mit der Agentur aufzunehmen.

Da eine Weitergabe der Namen und früheren Anschriften von ehemaligen Schülern an die Agentur datenschutzrechtlich unzulässig ist, die Durchführung von Klassentreffen aber unterstützt werden sollte, habe ich das Adressmittlungsverfahren unter der Voraussetzung als zulässig erachtet, dass die Kuverts den *Absender der Schule* tragen, damit unzustellbare Briefe nicht an die Agentur zurückgehen. Auf diese Weise wird verhindert, dass die Agentur auf diesem Umweg die Daten dann doch erfahren hätte.

Die Schule hat die als unzustellbar zurückkommenden Briefe gemäß § 19 Abs. 1 Nr. 2 SächsDSG unverzüglich zu vernichten. Nachforschungen über den aktuellen Aufenthalt eines Betroffenen, z. B. bei Eltern oder Einwohnermeldeämtern, gehören nicht mehr zu ihrer Aufgabe.

7.5 Herausgabe von Klassenbüchern aus DDR-Zeiten an die Rehabilitierungsbehörde

Nach dem Verwaltungsrechtlichen Rehabilitierungsgesetz können Verwaltungsentscheidungen, die in der DDR zwischen dem 8. Mai 1945 und dem 2. Oktober 1990 getroffen wurden, auf Antrag aufgehoben werden, wenn sie zu einer beruflichen Benachteiligung geführt haben. Voraussetzung ist, dass die frühere Entscheidung mit den tragenden Grundsätzen eines Rechtsstaats unvereinbar ist. Erst nach dieser Feststellung der Rechtsstaatswidrigkeit bzw. Aufhebung der Entscheidung findet das Berufliche Rehabilitierungsgesetz zum Ausgleich der beruflichen Nachteile Anwendung. Für das Verfahren gelten gemäß § 13 Abs. 3 VwRehaG die Vorschriften des Verwaltungsverfahrensgesetzes.

In einem solchen Rehabilitierungsverfahren hatte ein Betroffener angegeben, wegen seiner Zugehörigkeit zu den Zeugen Jehovas beruflich behindert worden zu sein. So hätte er die gewünschte Lehre nicht machen können und heute keinen adäquaten Berufsabschluß. Die Rehabilitierungsbehörde hat ihm, obwohl Unterlagen fehlten, aus „Dringlichkeitsgründen“ einen vorläufigen Anerkennungsbescheid erteilt. Als die Reha-Behörde eine Einwilligungserklärung des Betroffenen verlangte, damit sie bei anderen Stellen Daten über ihn erheben konnte, stimmte er dem nicht zu.

Um die nun zweifelhaft erscheinenden Angaben zu überprüfen, forderte die Rehabilitierungsbehörde bei seiner ehemaligen Schule alte Klassenbücher an, ohne dies näher zu begründen. Die Schule war sich nicht sicher, ob sie zur Herausgabe verpflichtet ist, zumal Klassenbücher auch die Daten anderer Schüler enthalten.

Wie ich von der Rehabilitierungsbehörde erfahren habe, sollte anhand der Klassenbücher geprüft werden, ob möglicherweise unzureichende Leistungen oder „das Betragen" des Betroffenen der Grund dafür waren, dass ihm die Ausbildung verweigert wurde. Dazu war auch ein Vergleich mit den Leistungen der Mitschüler erforderlich.

Ich habe die Rehabilitierungsbehörde davon überzeugen können, dass in diesem Fall eine Auskunft der Schule über die Noten des Betroffenen, ggf. über ihn vorhandene Klassenbucheintragungen sowie über den Notendurchschnitt der Klasse völlig ausreicht. Der Behördenleiter hat mir zugesagt, künftig nur noch konkrete Auskunftsersuchen an die Schulen zu richten und allenfalls Auszüge (Kopien) aus dem Klassenbuch mit der Maßgabe anzufordern, dass die Daten Dritter unkenntlich zu machen sind.

7.6 Die schlechten Zensuren eines Schülers und die Öffentlichkeit

Eine Gruppe von Schülern, die auf dem Weg nach Hause die Straßenbahn benutzte, unterhielt sich - offenbar lautstark - über ihre Schule und benahm sich nicht unbedingt zur Freude der übrigen Fahrgäste. Da die Bahn voll besetzt war, hatten sie nicht bemerkt, dass eine ihrer Lehrerinnen in der Straßenbahn saß. Sie wies die Jugendlichen zurecht und nannte dabei die schlechten Zensuren eines Schülers. Dieser fühlte sich dadurch in der Öffentlichkeit bloßgestellt, berichtete seinen Eltern den Vorfall, diese wandten sich an mich.

Auch wenn ich viel Verständnis für eine Lehrerin habe, die sich in einem solchen Fall einmischt und sich zu einer unbedachten Äußerung hinreißen lässt, so bleibt es doch ein Verstoß gegen § 15 Abs. 1 SächsDSG. Dies habe ich dem Schulleiter mitgeteilt und ihn gebeten, dem Kollegium noch einmal die datenschutzrechtlichen Belange in Erinnerung zu rufen. Zwar ist jeder Lehrer gemäß § 6 SächsDSG auf das Datengeheimnis verpflichtet, was das bedeutet, gerät jedoch im Laufe der Zeit leicht in Vergessenheit. Der Schulleiter ist meiner Bitte nachgekommen.

Ein Gespräch zwischen den unmittelbar Beteiligten hat die Angelegenheit bereinigt.

8 Justiz

8.1 Neugestaltung des Insolvenzrechts

Am 1. Januar 1999 ist bundesweit die neue Insolvenzordnung in Kraft getreten, mit der der Gesetzgeber das Insolvenzrecht grundlegend neu gestaltet hat. Gleichzeitig wurden die Konkursordnung und die Vergleichsordnung aufgehoben. In § 305 Abs. 1 Nr. 1 der neuen Insolvenzordnung werden die Länder ermächtigt, durch Rechtsvor-

schriften die für die Schuldnerberatung im Vorfeld des gerichtlichen Verfahrens als geeignet angesehenen Stellen für ihren Bereich zu bestimmen.

Von dieser Möglichkeit hat der Freistaat Sachsen Gebrauch gemacht.

In meiner Stellungnahme zu dem Gesetzentwurf habe ich gegenüber dem SMS u. a. angeregt, die Schuldnerberatungsstellen als öffentliche Stellen im Sinne von § 2 Abs. 2 SächsDSG zu klassifizieren. Denn nur wenn diese Stellen den strengen Regeln des Sächsischen Datenschutzgesetzes unterfallen, ist im Bereich der Schuldnerberatung eine ordnungsgemäße Verarbeitung personenbezogener Daten gewährleistet. Eine derartige Regelung dient im Übrigen auch der effizienten Datenschutzkontrolle durch meine Dienststelle.

Das SMS hat diese Anregungen zwar nicht im Gesetz berücksichtigt, jedoch im Wesentlichen in der ebenfalls mittlerweile vorliegenden Verwaltungsvorschrift zum Ausführungsgesetz umgesetzt.

Dies halte ich für akzeptabel.

8.2 „Elektronische Gerichtstafel“ im Internet

Das SMJus plant eine „elektronische Gerichtstafel“: Mit Inkrafttreten der Insolvenzordnung am 1. Januar 1999 sollten personenbezogene Daten aus Eröffnungs- und Einstellungsbeschlüssen im Gesamtvollstreckungsverfahren in das Internet eingestellt werden.

Nach Auffassung des SMJus könnten damit zahlreiche Insolvenzen sächsischer Unternehmen verhindert, Befriedigungsaussichten von Gläubigern und Entschuldungsaussichten von Schuldnern verbessert werden. Zudem würden die Gerichte erheblich von Anfragen entlastet werden.

Nach konstruktiv verlaufenen Beratungen besteht zwischen dem SMJus und mir Einigkeit darin, dass nur personenbezogene Daten aus Eröffnungs- und Einstellungsbeschlüssen in dem von der Insolvenzordnung festgelegten Umfang per Internet zugänglich gemacht werden dürfen.

Die ursprünglich vom SMJus beabsichtigte Veröffentlichung weiterer Daten zur Quotenprognose und zur Verfahrensbeendigung wird nicht erfolgen, weil hierfür - auch nach Einschätzung des SMJus - keine gesetzliche Grundlage besteht.

Die technischen Vorarbeiten sind zurzeit noch nicht abgeschlossen.

8.3 Terminsliste im Verfahren auf Abgabe der eidesstattlichen Versicherung

Der Datenschutzbeauftragte eines anderen Bundeslandes hat mich darüber informiert, dass in seinem Zuständigkeitsbereich die vom Gericht zur Abgabe einer eidesstatt-

lichen Versicherung geladenen Schuldner in einer „Terminsliste“, die im Gerichtsgebäude aushängt, namentlich genannt werden. So erfahren auch unbeteiligte Dritte, welche Personen zu einer solchen Erklärung verpflichtet werden sollen. Wegen fehlender Erforderlichkeit halte ich diese namentliche Nennung der Schuldner für unzulässig.

Auf meine Anfrage hat mir das SMJus geantwortet, dass in sächsischen Gerichten nur Terminslisten verwendet werden, deren Inhalt sich auf die Angabe von Uhrzeit, Aktenzeichen und Raum beschränkt; die betroffenen Personen werden nicht genannt. Hiergegen habe ich keine datenschutzrechtlichen Bedenken.

8.4 Landesweite Zugriffsmöglichkeit auf EDV-geführtes Grundbuch?

Der Bürgermeister einer sächsischen Stadt unterrichtete mich über das Vorhaben seiner Stadtverwaltung, am automatisierten Grundbuchabrufverfahren nach § 133 Abs. 2 Grundbuchordnung (GBO), §§ 80 ff. Grundbuchverfügung (GBV) (vgl. 3/8.8) teilzunehmen. Hiernach hätte die Stadt grundsätzlich Zugriff auf alle in Sachsen in elektronischer Form geführte Grundbücher erhalten. Das ist deshalb schlimm, weil die Abteilung III des Grundbuchs wesentliche Finanz- und Vermögensdaten enthält. Die Mitteilung nahm ich zum Anlass, mit dem SMJus die Datenschutzvorkehrungen dieses Abrufverfahrens eingehend zu erörtern.

Danach besteht mit dem SMJus Einigkeit darin, dass beim elektronischen Abrufverfahren keine Vorabentscheidung über die Gewährung der Einsicht in das Grundbuch nach § 12 und § 12 c Abs. 1 Nr. 1 GBO durch den Urkundsbeamten der Geschäftsstelle möglich ist. Eine einzelfallbezogene Prüfung des berechtigten Interesses findet mithin nicht statt. Aufgrund der technischen Ausgestaltung des Verfahrens (Online-Zugang) ist ein Abruf von Daten aus dem Grundbuch auch dann möglich, wenn die abrufende Stelle kein berechtigtes Interesse am Abruf hat, sondern die Anforderung der Daten z. B. allein dem persönlichen Interesse eines Mitarbeiters dient. Hinzu kommt, dass wegen der landesweiten Verfügbarkeit der Grundbuchdaten der Abruf im Unterschied zur Einsicht in das Papiergrundbuch nicht auf die Grundbücher des jeweiligen Amtsgerichts beschränkt ist. Die Zugriffsmöglichkeit ist somit auch jenseits der Aufgabenzuständigkeit der Gebietskörperschaft gegeben.

Die die Ausgestaltung des Abrufverfahrens regelnde Grundbuchverfügung sieht deshalb als Ersatz einer missbrauchsverhindernden präventiven Entscheidung vor der Einsichtnahme in das Grundbuch die nachträgliche Überprüfung der Rechtmäßigkeit der Abrufe anhand der über diese anzufertigenden Protokolle nach § 83 GBV vor. Zuständig für die Durchführung dieser Kontrollen sind die für die Aufsicht über die abrufenden Stellen zuständigen Behörden. Bei den Abrufen durch die Kommunen wären hiernach die die allgemeine Rechtsaufsicht führenden Regierungspräsidien bzw. Landratsämter zuständig. Damit die vom Gesetzgeber vorgesehene Datenschutzkontrollmöglichkeit effektiv genutzt wird, ist es unerlässlich, dass die von § 83 GBV geforderte Stichprobenkontrolle auch tatsächlich durchgeführt wird. Bei Abrufen durch Kommunen ist eine Kontrolle auf das berechtigte Interesse am Abruf insbesondere dann angezeigt, wenn die Daten von Grundstücken aus außerhalb

oder eventuell weit entfernt gelegenen Grundbuchbezirken abgerufen werden. Die Kontrolle nach § 83 GBV ist die einzige Möglichkeit, datenschutzwidrige rechtsmissbräuchliche Abrufe ohne berechtigtes Interesse zu ermitteln und auf Dauer solche Abrufe zu verhindern. Ich begrüße daher die Absicht des SMJus, im Falle der Feststellung solcher Abrufe den Widerruf einer Genehmigung oder die Kündigung einer Verwaltungsvereinbarung nach § 133 Abs. 2 GBO in Erwägung zu ziehen.

Umso bedauerlicher ist es, dass aufgrund der zurzeit eingesetzten Technik das vom Gesetz gebotene Datenschutzniveau nicht eingehalten wird: So besteht keine programmtechnische Möglichkeit, die Einsicht externer Nutzer des maschinell geführten Grundbuches auf bestimmte Gemarkungen zu beschränken. Nach Auskunft des SMJus seien hierfür umfangreiche „kostenintensive“ Programmänderungen erforderlich, die nur in Zusammenarbeit mit dem landesübergreifenden Entwicklerverbund des Systems realisiert werden könnten. So lange diese mit einem „erheblichen organisatorischen Aufwand“ verbundenen Programmanpassungen nicht vorgenommen würden, bliebe nach Auffassung des SMJus nur die Möglichkeit, dass das Oberlandesgericht Dresden alle für die Prüfung der Abrufe zuständigen Stellen bei Übersendung der Abrufprotokolle zum Bericht auffordert.

Angesichts dieser erheblichen datenschutztechnischen Defizite werde ich mich auch weiterhin für eine Ausgestaltung des EDV-Grundbuchs einsetzen, die den Vorgaben der GBO und der GBV entspricht.

8.5 Vorkaufsrecht der Gemeinden

Wie ich bereits in 5/8.11 ausführte, halte ich bei der Beteiligung der Gemeinden zur Ausübung ihres gesetzlichen Vorkaufsrechts nach §§ 24 ff. BauGB ein zweistufiges Verfahren für geboten: So sollte in der ersten Stufe der Verkäufer bzw. der den Kaufvertrag beurkundende Notar der Gemeinde noch nicht den gesamten Kaufvertrag übermitteln, sondern lediglich Mindestangaben, die es der Gemeinde ermöglichen zu prüfen, ob ein Vorkaufsrecht besteht und ob sie an dessen Ausübung interessiert ist. Erst bei Interesse der Gemeinde wird ihr der vollständige Vertragsinhalt bekannt gegeben (siehe auch oben Nr. 5.5.7).

Die Notarkammer Sachsen teilte mir mit, dass die Anwendung eines so gestuften Verfahrens nicht immer möglich war, weil einige Gemeinden sogleich die Übermittlung des vollständigen Vertrags verlangten. Die Gemeinden hätten sich dabei auf eine Anweisung der Regierungspräsidien und Landkreise gestützt, sich von den Notaren stets den vollständigen Vertragstext übermitteln zu lassen.

Wie das SMI mir gegenüber erklärt hat, habe es gegen die Anwendung des gestuften Verfahrens keine Bedenken. So hätten weder das SMI noch die Rechtsaufsichtsbehörden (Regierungspräsidien und Landratsämter) den Gemeinden durch eine Anweisung vorgegeben, welche Daten sie zur Ausübung ihres gesetzlichen Vorkaufsrechts nach §§ 24 ff. BauGB und § 3 BauGB-Maßnahmegesetz von den Notaren abfordern sollen. Die Notarkammer Sachsen habe ich darüber informiert. Ich hoffe nun, dass die Gemeinden das von mir vorgeschlagene zweistufige Verfahren künftig akzeptieren.

8.6 Zur Zulässigkeit eines „Korruptionsregisters“

Durch Beschluss der Staatsregierung ist eine ressortübergreifende Anti-Korruption-Arbeitsgruppe eingerichtet worden, um geeignete Maßnahmen zur Bekämpfung und Vorbeugung von Korruption in der sächsischen Verwaltung zwischen den Ressorts abzustimmen.

Die Staatsministerien sind sich darin einig, dass zur Bekämpfung dieser Kriminalitätsart der Aufbau eines sog. Korruptionsregisters, in dem Verfehlungen und Vergabesperren von Gewerbetreibenden gespeichert werden sollen, anzustreben ist. Hierzu vertrete ich folgende Auffassung:

Gegen die Speicherung von Verfehlungen von Gewerbetreibenden in einem zentralen Korruptionsregister bestehen datenschutzrechtliche Bedenken, weil es zurzeit an einer einschlägigen gesetzlichen Grundlage hierfür fehlt. Nach dem Volkszählungsurteil des Bundesverfassungsgerichts vom 15. Dezember 1983 können Eingriffe in das Recht auf informationelle Selbstbestimmung zwar aus überwiegenden Gründen des Gemeinwohls zulässig sein, sie bedürfen jedoch einer gesetzlichen Grundlage, die normenklar und verhältnismäßig sein muss. Die Speicherung von Verfehlungen von Gewerbetreibenden in einem Korruptionsregister stellt einen ganz erheblichen Eingriff in das Persönlichkeitsrecht sowie in die Grundrechtsgüter freie Berufsausübung und Eigentum dar. Eingriffe in diese Rechte bedürfen daher einer bereichsspezifischen gesetzlichen Regelung. Das Sächsische Datenschutzgesetz als Auffanggesetz kommt angesichts der Eingriffstiefe der ins Auge gefassten Datenverarbeitung nicht in Betracht.

Die differenzierten Voraussetzungen einer Erhebung, Speicherung, Übermittlung und Löschung personen- und firmenbezogener Daten müssen in einem klaren Wortlaut gesetzlich gefasst werden, so dass für jedermann die Entscheidung im Einzelfall vorhersehbar ist und Rechtsschutz erlangt werden kann. Eine Entscheidung zur Verarbeitung personenbezogener Daten in derartigen Fällen dürfte als Verwaltungsakt bzw. als Realakt anzusehen sein, der in jedem Einzelfall Grundrechtsbezüge regelt und daher rechtsstaatliche Garantien hervorruft.

8.7 Versendung von Justizpost

Bei der Kontrolle einer Stadtverwaltung habe ich festgestellt, dass eine Vielzahl von Justizmitteilungen und sonstigen Schreiben von Staatsanwaltschaften und Gerichten, die an einzelne Ämter der Stadtverwaltung gerichtet waren (z. B. Jugendamt, Sozialamt), gesammelt in DIN A 4-Umschlägen allgemein an die „Stadtverwaltung“ adressiert waren. Dies hat zur Folge, dass diese Schreiben von den Mitarbeitern der zentralen Poststelle zur Kenntnis genommen und erst danach den Fachämtern zugeordnet wurden.

In meiner Stellungnahme gegenüber dem SMJus habe ich mitgeteilt, dass diese Verfahrensweise - soweit es sich um Justizmitteilungen im Sinne des Justizmitteilungsgesetzes (JuMiG) handelt - gegen § 18 Abs. 2 JuMiG verstößt. Hiernach

ist durch angemessene Vorkehrungen sicherzustellen, dass die mitzuteilenden Daten *unmittelbar* den beim Empfänger funktionell zuständigen Bediensteten erreichen. Für die übrige Justizpost liegt meines Erachtens ein Verstoß gegen § 9 Abs. 2 Nr. 2 SächsDSG vor, wonach zu verhindern ist, dass Datenträger unbefugt (in diesem Fall von Mitarbeitern der zentralen Poststelle) gelesen werden können.

Dieser rechtswidrige Zustand kann nur dadurch beseitigt werden, dass jedes Justizschreiben in einem *gesonderten Kuvert* an das jeweils zuständige *Fachamt* adressiert wird.

Weil ich davon ausgehe, dass hier kein Einzelfall vorliegt, habe ich das SMJus gebeten, den nachgeordneten Bereich entsprechend zu sensibilisieren. Im Herbst 1999 werde ich eine Justizbehörde (Gericht oder Staatsanwaltschaft) in diesem Bereich personenbezogener Datenverarbeitung kontrollieren.

8.8 Entwurf eines Gesetzes zur Reform des Verfahrens bei Zustellung im gerichtlichen Verfahren

Schriftstücke in gerichtlichen Verfahren wie Ladungen, Gerichtsurteile u. a. werden zugestellt nach Verfahren gemäß §§ 166 ff. ZPO. Häufig enthalten diese Schriftstücke schützenswerte personenbezogene Daten. Die Verärgerung der betroffenen Bürger - das zeigen Eingaben - ist groß, wenn ein solches Schriftstück bei der Zustellung in die falschen Hände gerät (z. B. Ehescheidungsurteile werden den Kindern oder Schwiegereltern ausgehändigt, Strafbescheide gegen Firmeninhaber erhalten deren Mitarbeiter, Gerichtsbescheide über Betreuungen gehen an Hausbewohner oder Nachbarn usw.).

Im sog. Zustellungsreformgesetz sollen endlich die bisherigen Verfahren modernisiert und vereinheitlicht werden. Zum Entwurf dieses Gesetzes habe ich gegenüber dem SMJus mit folgenden Überlegungen Stellung genommen:

Mit dieser Neufassung des Zustellungsverfahrens wächst das Risiko einer Verletzung des Grundrechts auf informationelle Selbstbestimmung nach Art. 33 SächsVerf. Die Flexibilisierung des Zustellungsverfahrens und seine Öffnung für moderne Datenübertragungstechnik darf - etwa aus Kostengründen - nicht die neuen Risiken für die Privatsphäre vernachlässigen. Der vorliegende Entwurf mindert nicht, sondern erhöht die Gefahr der immer wieder von Bürgern zu Recht beanstandeten Falschzustellungen aller Art. Im Interesse eines vorbeugenden Datenschutzes besteht bei dem vorliegenden Entwurf noch erheblicher Nachbesserungsbedarf.

Das latente Dilemma zwischen der Gewährleistung des Grundrechts auf informationelle Selbstbestimmung und dem Zwang zur Kosteneinsparung verlangt auch bei Zustellungsverfahren neue Überlegungen. Eine Risikoanalyse des Zustellungsverfahrens weist hierzu einen praktikablen Weg. Der Inhalt des zuzustellenden Schriftstücks hat hinsichtlich der Wahrung des Grundrechts auf informationelle Selbstbestimmung unterschiedliche, klassifizierbare Schutzwürdigkeit. So wäre daran zu denken, dass Schriftstücke, deren Fehlzustellung besonders gravierende

Beeinträchtigungen des betroffenen Bürgers zur Folge haben können (Beeinträchtigung des Ansehens, Kreditwürdigkeit etc.) von der absendenden Geschäftsstelle besonders gekennzeichnet werden (z. B. mit dem Zustellungsvermerk „eigenhändig“, „persönlich“). Bei dem Zustellungsvorgang muss danach strikt darauf geachtet werden, Ersatzzustellungen mit hohen Risiken von Falschzustellungen zu unterlassen. Entsprechende Regelungen können noch in den Gesetzesentwurf eingefügt werden.

Aus Gründen der künftigen Normenklarheit und Rechtssicherheit habe ich die Präzisierung des Gesetzesentwurfs an mehreren Stellen und Vorschläge zur Verringerung des Risikos von Falschzustellungen angeregt.

Die Nutzung moderner Datenübertragungstechnik für das Versenden, Übertragen und Empfangen von zuzustellenden Schriftstücken wäre ohne spezielle Schutzvorkehrungen (Verschlüsselung, digitale Signatur) ein unvertretbares Risiko (neu § 174 Abs. 2 ZPO). Die Nutzung z. B. der neuen Technik der elektronischen Post im Internet käme sogar einer weltweiten Veröffentlichung des betreffenden Schriftstücks gleich.

Um eine unwirksame Zustellung an einen beteiligten Prozesspartner zu vermeiden (neu § 179 Abs. 2 ZPO), müsste der mit der Zustellung Beauftragte Kenntnis haben über die Beteiligten des Rechtsstreits, sofern ihm nicht mitgeteilt wurde, wer als Zustellungsempfänger ausscheidet, er müsste also u. U. das Schriftstück öffnen. Eine bessere Möglichkeit für die Lösung dieses Problems durch besondere Kennzeichnung habe ich oben skizziert.

Zahlreiche Eingaben von Bügern kritisieren zu Recht das Aufbringen einer Geschäftsnummer (z. B. OWi) und der Gerichtsabteilung auf den Briefumschlag, wodurch auf den Inhalt geschlossen werden kann. Auch sollte künftig geregelt werden, dass der Absender nur das Gericht und nicht die jeweilige Gerichtsabteilung angibt (neu § 177 Abs. 1 ZPO).

Ich hoffe, dass meine gegenüber dem SMJus gemachten Anregungen im Interesse des Rechts auf informationelle Selbstbestimmung bei den Beratungen des Zustellungsreformgesetzes berücksichtigt werden.

8.9 Mitteilungen von Klagen, Vollstreckungsmaßnahmen u. Ä. an die Landesjustizverwaltung

Im Berichtszeitraum hatte ich mich erneut mit dem Vorhaben des SMJus zu befassen, mittels Verwaltungsvorschrift auf der Grundlage von § 36 a BRAO den Gerichten und Gerichtsvollziehern eine Pflicht aufzuerlegen, der Landesjustizverwaltung Sachverhalte aus der Berufs- und Lebensführung von Rechtsanwälten und Notaren mitzuteilen, die Anlass zu berufsrechtlichen Maßnahmen geben. Wie ich bereits in 4/8.5.2 dargelegt habe, kann dieses Ziel nicht mit dem Mittel der Verwaltungsvorschrift erreicht werden, weil nach dem Volkszählungsurteil des Bundesverfassungsgerichts Einschränkungen des Grundrechts auf informationelle Selbstbestimmung einer gesetzlichen Grundlage bedürfen. Gesetzlich geregelt ist durch § 36 a BRAO lediglich

die *Befugnis*, nach einer Interessenabwägung personenbezogene Informationen zu übermitteln; eine *Pflicht* zur Übermittlung wird durch diese Vorschrift ausdrücklich nicht normiert.

Nach eingehender Beratung des mir vorgelegten Entwurfs der Verwaltungsvorschrift nahm das SMJus im Hinblick auf die seinerzeit anstehende (inzwischen in Kraft gesetzte) Anordnung über Mitteilungen in Zivilsachen (MiZi) Abstand. Die Neufassung der MiZi weist leider in einem datenschutzrechtlich zentralen Punkt gravierende Defizite auf: Danach sollen - ebenso wie in dem vorbezeichneten Entwurf der sächsischen Verwaltungsvorschrift - sämtliche Forderungsklagen, die gegen einen Rechtsanwalt erhoben worden sind, den Rechtsanwaltskammern mitzuteilen sein. Dies führt dazu, dass entsprechende Datenübermittlungen vorgenommen werden, bevor ein Gericht festgestellt hat, dass die mit der jeweiligen Klage geltend gemachten Forderungen überhaupt begründet sind. Sollen etwa per se an die Eigenschaft als Beklagter sanktionsähnliche Rechtsfolgen gegen den Betroffenen geknüpft werden? Dies ist in der Rechtsordnung nicht nur unüblich, sondern verkennt auch in erheblichem Maße die Anforderungen an einen Rechtsstaat im Allgemeinen sowie Sinn und Zweck eines justizförmig ausgestalteten Gerichtsverfahrens im Besonderen:

Die Rechtsprechung ist die in einem besonders geregelten Verfahren zur letztverbindlichen Entscheidung führende rechtliche Beurteilung von Sachverhalten in Anwendung des geltenden Rechts durch ein unabhängiges Organ - den Richter. Die Feststellung, ob ein geltend gemachter zivilrechtlicher Anspruch besteht, obliegt ausschließlich der Justiz. Bevor diese Feststellung getroffen ist, gilt der betreffende Beklagte nach dem Rechtsstaatsprinzip als unbescholten bzw. im strafrechtlichen Sinne als unschuldig. Es ist deshalb auch folgerichtig, dass im Zivilprozess zwischen dem formalen Prozessführungsrecht und der materiellen Sachbefugnis unterschieden wird und die Eigenschaft als Beklagter zeitlich das Erkenntnisverfahren betrifft, also das Verfahren, in dem erst noch geklärt werden muss, ob die Klage überhaupt zu Recht erhoben worden ist. Eine staatlich angeordnete Verknüpfung der Tatsache der Klageerhebung mit negativen Folgen für den Beklagten wäre gerade im zivilrechtlichen Verfahren, wo im Gegensatz zum strafrechtlichen Verfahren vor Klageerhebung kein Ermittlungsverfahren durch eine sachlich unabhängige Instanz erfolgt, rechtswidrig. Dies berücksichtigt im Übrigen auch der als Ermächtigungsgrundlage anzusehende § 36 a Abs. 3 BRAO. Hiernach kommen nur solche personenbezogenen Informationen für eine Übermittlung in Frage, die für die Rücknahme oder den Widerruf einer Erlaubnis, Befreiung oder Zulassung eines Rechtsanwalts oder zur Einleitung eines rüge- oder anwaltsgerichtlichen Verfahrens von Bedeutung sein können. Mit dieser Formulierung wird auf §§ 7 und 14 BRAO Bezug genommen. Diese Normen knüpfen nach ihrem eindeutigen Wortlaut für die mit einem Rechtsstreit des Betroffenen verbundenen Sanktionen stets an eine gerichtliche Entscheidung an. Dies kommt besonders deutlich in §§ 7 Nr. 9 und 14 Abs. 2 Nr. 8 BRAO für die von den Landesjustizverwaltungen immer wieder besonders herausgestellte Konstellation eines im Vermögensverfall befindlichen Rechtsberaters zum Ausdruck. Die genannten Vorschriften verweisen nämlich auf § 915 ZPO, der die vom *Vollstreckungsgericht* zu koordinierende Aufnahme in das Schuldnerverzeichnis regelt. „Im Vermögensverfall befindlich“ ist der Betreffende eben erst dann und nicht schon

im Zeitpunkt einer materiell möglicherweise völlig unberechtigten Klageerhebung gegen ihn.

Ich bedaure, dass das SMJus diese vorstehenden Erwägungen nicht in das bundesweite Abstimmungsverfahren zur MiZi eingebracht hat.

8.10 Entwurf eines Gesetzes zur Regelung des Schutzes gefährdeter Zeugen

Straftäter mit besonders hoher krimineller Energie vermeiden weitgehend Spuren. Das Auffinden von Sachbeweisen ist daher für die Ermittlungsbehörden sehr schwierig. Deshalb kommt der Zeugenaussage besonders große Bedeutung bei der Bekämpfung schwerer Straftaten zu. Die für das Ermittlungsverfahren benötigten Informationen können vielfach nur von Personen gewonnen werden, die wegen ihrer persönlichen Nähe zu den Tätern genaue Kenntnisse über deren Tatbeteiligung sowie die Tatplanung und -ausführung haben. Bei diesem Personenkreis besteht jedoch die Gefahr, dass die Täter aufgrund der Aussage darauf schließen können, wer mit den Strafverfolgungsbehörden zusammenarbeitet. Sie werden daher bestrebt sein, weitere Zeugenaussagen zu verhindern und zu diesem Zweck Druck auf den Zeugen auszuüben. Diese Zeugen verdienen besonderen Schutz, den das Gesetz zur Regelung des Schutzes gefährdeter Zeugen bieten soll.

Aus datenschutzrechtlicher Sicht habe ich im Wesentlichen zu zwei Vorschriften des Gesetzentwurfs Stellung genommen:

Hinsichtlich der Aufgaben und Befugnisse der nach dem Gesetz einzurichtenden Zeugenschutzdienststelle war festgelegt, dass die im Zusammenhang mit dem Zeugenschutz geführten Akten von der Zeugenschutzdienststelle geführt werden, der Geheimhaltung unterliegen und nicht Bestandteil der Ermittlungsakte sind. Es blieb auch unter Berücksichtigung der Entwurfsbegründung unklar, ob und ggf. wer über die Mitarbeiter der Zeugenschutzdienststelle hinaus zu diesen Akten Zugang haben darf. Der Kreis der zugangsberechtigten Personen sollte nach meinem Dafürhalten wegen des zweifellos vorhandenen Geheimhaltungsbedürfnisses möglichst klein bleiben.

An anderer Stelle des Entwurfs war vorgesehen, dass die Zeugenschutzdienststelle von allen öffentlichen und nicht-öffentlichen Stellen unter bestimmten näher bezeichneten Voraussetzungen die Sperrung von Daten der Schutzpersonen verlangen kann. Diese Formulierung ließ offen, wer konkret unter den Begriff der öffentlichen Stelle im Sinne des Gesetzentwurfs zu subsumieren ist. Ob hierunter tatsächlich alle öffentlichen Stellen, also auch die Gerichte zu fassen sind, wurde weder aus dem Wortlaut noch aus der Begründung der Vorschrift deutlich. Es ist vor dem Hintergrund des verfassungsrechtlichen Bestimmtheitsgrundsatzes unerlässlich, dass der Begriff der öffentlichen Stelle definiert wird.

Das SMJus teilte meine Auffassung und hat zugesagt, meine Bedenken bei den Beratungen im Bundesrat einzubringen.

8.11 DNA-Analyse-Datei

Mit dem DNA-Identitätsfeststellungsgesetz vom 7. September 1998 (BGBl. I, S. 2646) hat der Bundesgesetzgeber festgelegt, ob und in welchen Grenzen die Erhebung, Speicherung und Nutzung der durch eine DNA-Analyse gewonnenen Untersuchungsergebnisse durch die Strafverfolgungsbehörden zulässig sind (vgl. die hierzu gefasste Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 17./18. April 1997, abgedruckt in 5/16.3.2).

In Umsetzung dieser gesetzlichen Regelungen hat das Bundeskriminalamt den Betrieb einer bundesweiten DNA-Analyse-Datei aufgenommen. So sehr ich diese Datei als Mittel effizienter Verbrechensbekämpfung akzeptiere, habe ich mich doch gegen eine Bestimmung der Errichtungsanordnung dieser Datei gewandt:

Danach sollen die Erhebung und die Speicherung von DNA-Identifizierungsmustern auch aufgrund der Einwilligung des Betroffenen ermöglicht werden. Damit erweitert die Errichtungsanordnung den vom Gesetz scharf konturierten Befugnisrahmen und umgeht die verfahrenssichernden Vorkehrungen des DNA-Identitätsfeststellungsgesetzes. So dürfen die Untersuchungen nach § 81 e StPO nur durch den Richter angeordnet werden (§ 81 f StPO), der gemäß § 81 g StPO eine negative Prognose hinsichtlich der betroffenen Person treffen muss. Eine solche negative Prognose durch den Richter kann nicht durch die Einwilligung des Betroffenen ersetzt werden. Im Übrigen kann nicht davon ausgegangen werden, dass der betroffene Personenkreis eine wirksame, nämlich völlig freiwillige Einwilligung für die Datenerhebung und -speicherung erteilt. Beschuldigte in Ermittlungsverfahren oder Inhaftierte etwa kurz vor der Haftentlassung werden häufig eine „Einwilligung“ erklären, um zu vermeiden, dass die Entscheidung über Hafterleichterung oder vorzeitige Haftentlassung zu ihren Ungunsten ausgeht. Darüber hinaus kann die wirklich freiwillige Willensentscheidung jederzeit widerrufen werden mit der Folge, dass die Daten in der Analysedatei zu löschen wären.

Zudem geht aus der Systematik der Strafprozeßordnung eindeutig hervor, dass gerade im Fall der DNA-Analyse eine „freiwillige Datenverarbeitung“ (einschließlich der Erhebung) nicht in Betracht kommt. Denn anders als in den sonstigen Vorschriften der §§ 81 ff. StPO erwähnt § 81 g StPO ausdrücklich *nicht* die Möglichkeit der auf Freiwilligkeit gegründeten Datenerhebung.

Im Übrigen bitte ich Folgendes zu bedenken:

Es kann nicht sein, dass der repressive Staat sich in die Abhängigkeit von freiwilligen Entscheidungen von Rechtsunterworfenen begibt. Von einer Gleichordnung, die jeder freiwilligen Entscheidung immanent ist, kann im vorliegenden Fall keine Rede sein.

Wesentlichstes Argument bleibt allerdings der Grundsatz der Gesetzmäßigkeit der Verwaltung: Denn Aufgaben und Befugnisse der Eingriffsverwaltung können durch die Konstruktion einer freiwilligen Einwilligung nicht erweitert, ergänzt oder sonst

verändert werden. Repressive Verwaltung vollzieht sich ausschließlich auf normenklarer gesetzlicher Grundlage.

In Besprechungen mit den Sächsischen Staatsministerien der Justiz und des Innern habe ich deutlich zum Ausdruck gebracht, dass die dem BKA vom Freistaat Sachsen zur Verfügung gestellten Datenbestände nur unter strenger Beachtung der gesetzlichen Voraussetzungen (Richterentscheidung) entstanden sein dürfen.

8.12 Kann die staatsanwaltschaftliche Ermittlungstätigkeit zur Befugniserweiterung von Verwaltungsbehörden führen?

Das Regierungspräsidium Dresden unterrichtete mich über folgenden Sachverhalt: Ein nordrhein-westfälisches Polizeipräsidium hatte von der Straßenverkehrsbehörde einer sächsischen Kreisstadt verlangt, dass diese sich von sämtlichen Personen, die einen Pkw Trabant vorübergehend stilllegen wollten, den Ausweis vorlegen lässt und die so erhobenen personenbezogenen Daten speichert. Diese Aufforderung, die im Rahmen der Ermittlungstätigkeit gegen eine international agierende Autoschieberbande erging, wurde durch eine Verfügung der für das Polizeipräsidium zuständigen nordrhein-westfälischen Staatsanwaltschaft bestärkt.

Das Regierungspräsidium Dresden meldete gegenüber dem Ersuchen des Polizeipräsidiums rechtliche Bedenken an, die von mir aus folgenden Gründen geteilt wurden:

Es gibt weder in der Straßenverkehrszulassungsordnung noch in anderen bereichsspezifischen Gesetzen eine Regelung, die es einer Zulassungsstelle erlauben würde, die Identität der Personen, die Fahrzeuge vorübergehend stilllegen wollen, durch Vorlage von Ausweispapieren festzustellen. Auch scheidet die Auffangvorschrift des § 11 Abs. 1 SächsDSG als Rechtsgrundlage für die Identitätsfeststellung im vorliegenden Fall aus, weil die angesonnene Datenerhebung nicht zur Erfüllung der Aufgabe der Zulassungsstelle erforderlich ist. Daher ist es der Zulassungsstelle auch nicht möglich, dem Polizeipräsidium über die Identität dieser Personen Auskunft aufgrund von § 161 StPO zu geben.

Es geht nicht darum, dass Behörden die bereits vorhandenen Daten an die Ermittlungsbehörden weitergibt, sondern ob sie zu diesem Zweck (eigentlich sachfremde) Daten erheben dürfen oder gar müssen.

§ 161 StPO ist keine Vorschrift, die die sachliche Zuständigkeit bzw. die Befugnisse von Behörden, die von einer Staatsanwaltschaft oder Polizeibehörde gemäß dieser Vorschrift um Auskunft gebeten werden, erweitert. Sie ermächtigt somit die um Auskunft gebetene Behörde nicht, eine Ermittlungen anzustellen, die nicht von der eigentlichen Aufgabe und den damit verbundenen Befugnissen der Behörde gedeckt sind. § 161 StPO ist daher nicht geeignet, die in § 163 b StPO geregelte Zuständigkeit für die Identitätsfeststellung im Rahmen der Strafverfolgung auf andere als die dort genannten Stellen auszudehnen. Die Verfügung der Staatsanwaltschaft gegenüber der Zulassungsstelle konnte somit nicht als Grundlage für die gewünschten Identitätsfeststellungen in Betracht kommen.

8.13 Begründet eine unzulässige Datenübermittlung aus dem Passregister ein Beweisverwertungsverbot?

Ein PKW-Fahrer beschwerte sich darüber, dass eine Passbehörde sein Passbild zum Vergleich mit einem bei einer Geschwindigkeitsüberschreitung entstandenen Lichtbild für eine Ordnungsbehörde zur Einsicht bereit gehalten hatte. Darin läge ein Verstoß gegen § 22 Abs. 2 Nr. 3 PaßG. Nach dieser Vorschrift dürfen Behörden aus dem Passregister u. a. Daten erhalten, wenn sie beim Betroffenen nur mit unverhältnismäßig hohem Aufwand erhoben werden können. Der Petent meinte, der (behauptete) Datenschutzverstoß begründe ein Verwertungsverbot des Lichtbilds im Ordnungswidrigkeitenverfahren; er müsse daher die verhängte Geldbuße nicht bezahlen.

Leider war es nicht mehr möglich, den Sachverhalt hinreichend aufzuklären. Zur Beurteilung der Frage des Verwertungsverbots war dies aber auch nicht notwendig, weil ein solches Verbot grundsätzlich bei Verstößen gegen § 22 Abs. 2 PaßG nicht besteht. Beweisverwertungsverbote sind im Ordnungswidrigkeitenverfahren nämlich nur dann gerechtfertigt, wenn nach einer Abwägung zwischen dem Interesse des Betroffenen und dem staatlichen Verfolgungsinteresse das Erstere überwiegt. Bei Sachverhalten wie dem vorliegenden ist dies aber nach gefestigter Rechtsprechung der Obergerichte nicht der Fall (vgl. Bay. ObLG, NJW 1998, S. 3656 ff. m. w. N.).

9 Wirtschaft und Arbeit

9.1 Straßenverkehrswesen

9.1.1 Ist eine amtlich anerkannte Begutachtungsstelle für die Fahreignung eine öffentliche Stelle im Sinne des Sächsischen Datenschutzgesetzes?

Im Berichtszeitraum habe ich die Aktenführung einer als Aktiengesellschaft organisierten amtlich anerkannten Begutachtungsstelle für die Fahreignung (MPU-Stelle) kontrolliert. Diese MPU-Stellen begutachten Fahrerlaubnisbewerber oder -inhaber, wenn der Fahrerlaubnisbehörde Tatsachen bekannt werden, die Zweifel an der Fahreignung der Betroffenen begründen. Wenn in einem solchen Fall die Fahrerlaubnisbehörde unter Beachtung des Grundsatzes der Verhältnismäßigkeit die Vorlage eines MPU-Gutachtens fordert, ist der Betroffene darauf angewiesen, eine amtlich anerkannte MPU-Stelle aufzusuchen, um die Eignungszweifel zu beseitigen (vgl. § 11 Abs. 3 Fahrerlaubnisverordnung, am 1. Januar 1999 in Kraft getreten). Lehnt er die Begutachtung ab, erhält er keine Fahrerlaubnis bzw. wird diese ihm entzogen.

Voraussetzung meiner Kontrolle war die Klärung der Rechtsfrage, ob die privatrechtlich organisierte MPU-Stelle überhaupt meiner auf den öffentlichen Bereich beschränkten Kontrollkompetenz unterliegt. Dies habe ich - unter Zustimmung der MPU-Stelle - aus folgenden Gründen bejaht:

Nach § 2 Abs. 2 SächsDSG gelten auch juristische Personen des privaten Rechts als öffentliche Stellen, soweit sie Aufgaben der öffentlichen Verwaltung wahrnehmen.

Nach meiner Auffassung ist das Erstellen von medizinisch-psychologischen Gutachten eine Aufgabe der öffentlichen Verwaltung, weil diese Tätigkeit Bestandteil des durch eine öffentlich-rechtliche Vorschrift zwingend vorgeschriebenen Verfahrens ist.

Außerdem spricht für diese Auffassung, dass ursprünglich bundesweit die Tätigkeit von MPU-Stellen *innerhalb* der Fahrerlaubnisbehörden geplant war. Lediglich aus Gründen der „Überlastung" sind die MPU-Stellen verselbständigt und ausgelagert worden. Es ist allgemein anerkannt, dass durch die Wahl der privatrechtlichen Organisationsformen die Aufgabe selbst nicht ihren öffentlichen Charakter als Verwaltungsaufgabe verliert, weil nicht sie, sondern nur die Organisation ihrer Wahrnehmung privatisiert wird (vgl. BGH, NJW 1998, S. 1874 ff.).

Die Kontrolle der Aktenführung der MPU-Stelle ergab, dass die datenschutzrechtlichen Anforderungen erfüllt waren.

9.1.2 Datenübermittlung der Kfz-Zulassungsstelle an die untere Abfallbehörde zum Vollzug der Altautoverordnung vom 4. Juli 1997 und des § 27 a StVZO

Seit 1. April 1998 hat der Halter eines Fahrzeugs, das endgültig aus dem Straßenverkehr gezogen werden soll, gemäß § 27 a StVZO der Kfz-Zulassungsstelle beim Abmelden des Fahrzeugs einen Verwertungsnachweis bzw. eine Verbleibserklärung vorzulegen. Die Kfz-Zulassungsstelle leitet diesen Nachweis dann der unteren Abfallbehörde zu. Ein Landratsamt, das sowohl Kfz-Zulassungsstelle als auch untere Abfallbehörde ist, wollte aus Gründen der Verwaltungsvereinfachung, dass der Abfallbehörde aus dem örtlichen Fahrzeugregister der Kfz-Zulassungsstelle über das hausinterne EDV-System Daten, die auf dem Verwertungsnachweis enthalten und auch im örtlichen Fahrzeugregister gespeichert sind (z. B. Angaben zum Fahrzeughalter und zum Fahrzeug), regelmäßig übermittelt werden.

Eine Datenübermittlung von einer öffentlichen Stelle zu einer anderen bedarf auch dann einer Rechtsgrundlage, wenn der Absender und Empfänger der Daten in einer Behörde („Bündelungsbehörde") organisatorisch zusammengefasst sind.

Die vorgesehene regelmäßige Datenübermittlung scheitert an den Voraussetzungen des § 35 Abs. 3 StVG. Diese Vorschrift regelt abschließend, unter welchen Voraussetzungen eine regelmäßige Datenübermittlung aus dem örtlichen Fahrzeugregister an andere öffentliche Stellen zulässig ist. Diese Voraussetzungen liegen aber bei der hier vorgesehenen Datenübermittlung nicht vor. Eine gesetzlich nicht vorgesehene Datenübermittlung aus dem örtlichen Fahrzeugregister, etwa aus verwaltungsökonomischen Gründen, ist unzulässig. Gemäß der Verordnung über die Entsorgung von Altautos und die Anpassung straßenverkehrsrechtlicher Vorschriften vom 4. Juli 1997 (BGBl. I S. 1666, 1674) sind die Formblätter Verwertungsnachweis/Verbleibserklärung maschinenlesbar zu gestalten, so dass sich bei Anschaffung der entsprechenden EDV-Technik die angestrebte Verwaltungsvereinfachung realisieren ließe.

9.1.3 Ausstattung der Polizeifahrzeuge der sächsischen Polizei mit dem UDS - Unfalldatenschreiber (Black Box)

Wie ich der Presse entnehmen konnte, will das SMI die Polizeifahrzeuge der sächsischen Polizei mit der sogenannten „Black Box“ ausstatten. Es handelt sich hier um einen Unfalldatenschreiber (UDS), der bestimmte Betriebsvorgänge eines Fahrzeugs aufzeichnet und bei einem Unfall automatisch speichert (30 Sekunden vor dem Unfallereignis bis 15 Sekunden danach). Damit lässt sich der Unfallhergang im Wesentlichen nachvollziehen. Da sich mit diesem Unfalldatenschreiber auch das Fahrverhalten des Fahrzeugführers des Dienstkraftfahrzeugs zum Unfallzeitpunkt nachvollziehen lässt, handelt es sich um eine automatisierte Verarbeitung von Beschäftigtendaten, die zur Verhaltenskontrolle des Fahrzeugführers geeignet ist. Gemäß § 31 Abs. 7 SächsDSG ist daher vor Einführung des UDS die Beteiligung des Sächsischen Datenschutzbeauftragten erforderlich.

Dem Presseartikel war zu entnehmen, dass im Rahmen eines Pilotversuchs zunächst Fahrzeuge eines Polizeireviers der Polizeidirektion Dresden mit UDS ausgestattet wurden. Meine vorgeschriebene Beteiligung erfolgte erst nach Aufforderung. Nachdem mir durch das SMI die Wirkungsweise des UDS und die mit dessen Einführung verbundenen Auswirkungen auf die Betroffenen erläutert wurden, habe ich dem Verfahren zugestimmt, zumal der Pilotversuch gezeigt hat, dass die Unfallhäufigkeit in dem Polizeirevier erheblich zurückgegangen ist. Es galt bei meiner Beurteilung des Verfahrens auch zu bedenken, dass der UDS bei einem Verkehrsunfall nicht nur den Fahrzeugführer des Polizeifahrzeugs belastende, sondern auch ihn entlastende Umstände aufzeigt.

Ich stehe daher der Ausstattung der Polizeifahrzeuge des Freistaates Sachsen mit UDS positiv gegenüber.

9.1.4 Bedeutung von Vorstrafen für die Fahreignungsprüfung

Anlässlich der Kontrolle einer Führerscheinstelle habe ich die Frage grundsätzlich bejaht, ob zur Prüfung der Fahreignung Vorstrafen berücksichtigt werden dürfen:

§ 9 StVZO *verpflichtet* Fahrerlaubnisbehörden sogar, bei der Eignungsprüfung zu ermitteln, ob Bedenken gegen den Führerscheinbewerber wegen schwerer oder wiederholter Vergehen gegen Strafgesetze bestehen. Die Verwaltungsbehörde wird daher in aller Regel von dem Betroffenen die Vorlage eines Führungszeugnisses verlangen (vgl. § 8 Abs. 3 StVZO).

Ein Verwertungsverbot ergibt sich jedoch für Verurteilungen, die im Strafregister getilgt worden sind oder hätten getilgt werden müssen (z. B. nach Ablauf gesetzlich festgeleger Tilgungsfristen). Dies folgt unmittelbar aus § 51 BZRG. Danach dürfen bei Tilgungreife dem Betroffenen Tat und Verurteilung im Rechtsverkehr nicht mehr vorgehalten und nicht zu seinem Nachteil verwertet werden. Die Formulierung: „im Rechtsverkehr“ erfasst alle Rechtsverhältnisse, insbesondere auch Verwaltungsverfahren wie das Fahrerlaubnisverfahren.

9.2 Gewerberecht

In diesem Jahr nicht belegt.

9.3 Industrie- und Handelskammern; Handwerkskammern

9.3.1 Datenabgleichverfahren zwischen den Industrie- und Handelskammern, Handwerkskammern und der Arbeitsverwaltung

Im Berichtszeitraum erfuhr ich von Vereinbarungen zwischen der Arbeitsverwaltung und den Industrie- und Handelskammern/Handwerkskammern über ein Datenabgleichverfahren, die das Ziel haben, Lehrstellen effizienter anbieten und besetzen zu können. So heißt es beispielsweise in einer solchen Vereinbarung:

„*Zur Verbesserung der Transparenz auf dem Ausbildungsmarkt gleichen Arbeitsämter und Kammern regelmäßig die Daten über noch nicht vermittelte Bewerber/innen und unbesetzte Ausbildungsstellen bei den Arbeitsämtern mit den eingetragenen Ausbildungsverhältnissen bei den Kammern ab.*“

Trotz großem Verständnis für die allenthalben bestehende prekäre Lehrstellensituation musste ich feststellen, dass die Datenabgleiche ohne die dafür erforderliche Rechtsgrundlage erfolgen. Sämtliche bundesweit von den Kammern nacheinander und abwechselnd angeführten Bestimmungen (u. a. §§ 35 ff. SGB III, §§ 341 ff. SGB III, § 402 Abs. 1 Satz 1 Nr. 2 SGB III, § 28 Abs. 2 HandwO) sowie Hinweise auf das IHK-G, das Berufsbildungsgesetz und die allgemeinen Datenschutzgesetze legitimieren nicht zu solchen Datenabgleichen.

Hinzu kommt, dass die Fachleute bei näherem Hinsehen festgestellt haben, dass durch den Abgleich allenfalls 1 bis 2 Prozent durch Mehrfachbewerbungen blockierte Ausbildungsplätze ermittelt wurden. Im Übrigen zeigt sich wiederum, dass mit bürokratischen Mitteln der - im Einzelfall durchaus verständliche - Umstand, dass junge Leute, denen eine Lehrstelle zugesagt ist, sich durch weitere Bewerbungen verbessern wollen, nicht abgebaut werden kann. Die Sache scheint noch nicht durchdacht zu sein: Was soll der Aufwand des Datenabgleichs bewirken?

Der BfD erwägt, in seinem Zuständigkeitsbereich die Bundesanstalt für Arbeit für den Fall weiterer rechtswidriger Datenabgleiche förmlich zu beanstanden. Ich habe das SMWA gebeten, zur Vermeidung einer förmlichen Beanstandung meinerseits die Kammern auf die Rechtswidrigkeit der Datenabgleiche hinzuweisen und sicherzustellen, dass es zu keinen unzulässigen Datenübermittlungen an die Arbeitsverwaltung mehr kommt.

Die Angelegenheit ist noch im Fluss.

9.3.2 Bekanntgabe von Prüfungsergebnissen an den Ausbildungsbetrieb

Die Datenschutzbeauftragten befassten sich schon vor Jahren mit der Frage der Zulässigkeit der Weitergabe von Prüfungsergebnissen an den Ausbildungsbetrieb.

Angeregt wurde u. a., im BBiG eine normenklare Regelung zu schaffen (vgl. 4/9.3.3).

Von mir zunächst völlig unbemerkt wurde das Problem mit dem Zweiten Gesetz zur Änderung der Handwerksordnung (HandwO) und anderer handwerksrechtlicher Vorschriften vom 25. März 1998 (BGBl. I S. 596), wenn auch nicht voll zufriedenstellend, gelöst.

So wurden § 31 Abs. 2 HandwO sowie § 41 BBiG folgende Sätze angefügt, die seit 1. April 1998 gelten:

„Dem Ausbildenden werden auf dessen Verlangen die Ergebnisse der Zwischen- und Abschlussprüfung übermittelt."

Der Begründung dieser Änderungen zufolge wird die Weitergabe dieser Daten deshalb gerechtfertigt, *weil der Ausbildungsbetrieb Kenntnis von „seinen" Ausbildungsergebnissen erhalten muss.*

Daraus schließe ich, dass nicht das komplette Ergebnis der Zwischen- und Abschlussprüfung mitgeteilt werden darf, sondern nur die betriebsbezogenen Ausbildungsergebnisse, nicht also z. B. Noten der Fächer Religion, Sport, Deutsch. Solche Fächer allgemeinbildender Natur geben dem Ausbildungsbetrieb nämlich keine Hinweise auf die Qualität „seiner" betrieblichen Ausbildung.

Ich habe das SMWA gebeten, die Industrie- und Handelskammern, die Handwerkskammern und die Ausbildungsbetriebe entsprechend zu unterrichten.

9.4 Offene Vermögensfragen

In diesem Jahr nicht belegt.

9.5 Sonstiges

In diesem Jahr nicht belegt.

10 Soziales und Gesundheit

10.1 Gesundheitswesen

10.1.1 Staatsvertrag über das Gemeinsame Krebsregister

Mit Gesetz vom 6. November 1998 (GVBl. S. 594) hat der Sächsische Landtag dem am 21. November 1997 unterzeichneten Staatsvertrag über das Gemeinsame Krebsregister der sechs östlichen Bundesländer zugestimmt. Das Zustimmungsgesetz hebt einige Regelungen des Sächsischen Ausführungsgesetzes zum Krebsregistergesetz

(SächsKRGAG) zu Gunsten entsprechender Regelungen des Staatsvertrages auf. In der Sache ändert sich in Sachsen die Rechtslage hiermit nur unwesentlich. Meinen von mir im Schlussabsatz von 5/10.1.1 erläuterten Bemühungen ist der Erfolg versagt geblieben - hoffentlich verwirklichen sich die damit vom SMS eingegangenen juristischen Risiken für Sachsen nicht.

Anderer Handlungsbedarf bleibt:
Nach Untersuchungen des GKR (Vortrag seiner Leiterin, Dr. Eisinger, am 24. März 1999 in Dresden auf dem „2. Workshop Krebsregister" der Deutschen Krebsgesellschaft e. V.) verteilt sich der Vollständigkeitsgrad der Meldungen zum GKR für die Jahre 1995 bis 1997 Folgendermaßen:

Sachsen	78 %
Brandenburg	70 %
Mecklenburg-Vorpommern	60 %
Thüringen	35 %
Sachsen-Anhalt	25 %
Berlin	15 %

Sachsen hat die widerspruchsunabhängige Meldepflicht immerhin seit Juli 1993, Mecklenburg-Vorpommern hat sie erst seit dem 1. Juli 1998, die anderen beteiligten Länder haben ein bloßes widerspruchsabhängiges Melderecht (mit Informationsverpflichtungen), also die Standardregelung des GKR.

Das erlaubt zwei Feststellungen: Sachsen hat noch nicht die nötige Melderate von 95 v. H. (vgl. 4/10.1.1). Brandenburg hat ohne Meldepflicht einen nicht wesentlich geringeren Meldevollständigkeitsgrad erreicht als Sachsen.
Außerdem ist nach den Erkenntnissen des GKR die Quote der Widersprüche Betroffener (gegen Meldungen durch ihre Ärzte) sehr gering.

Daraus folgt: In Sachsen müssen rasch die fehlenden 15 Prozent noch geschafft werden, damit die gesetzlich angeordnete Datensammlung nachhaltig geeignet und damit auch nachhaltig rechtmäßig wird bzw. bleibt. Die (widerspruchsunabhängige) Meldepflicht allein bringt noch nicht den nötigen Erfolg. Es müssen ergänzende Maßnahmen getroffen werden. Möglicherweise kann man insoweit von Brandenburg lernen. Vermutlich muss man unter anderem die Erfüllung der Meldepflicht den Ärzten finanziell besser honorieren, gerade weil es keine Sanktionen bei Nichterfüllung der Meldepflicht gibt.

10.1.2 Örtliche Sammlungen von Altdaten über Krebserkrankungen

(1) Die in 2/10.1.5 genannten Datensammlungen gibt es, wie sich herausgestellt hat, zum Teil immer noch. An der Rechtslage hat sich nicht etwa dadurch etwas geändert, dass nunmehr das Krebsregistergesetz des Bundes vom 4. November 1994, ergänzt durch das Sächsische Ausführungsgesetz dazu (SächsKRGAG, vgl. 5/10.1.1) und durch den Staatsvertrag über das Gemeinsame Krebsregister der östlichen Bundesländer mitsamt dem dazu gehörenden Gesetz (vorstehend 10.1.1) die maßgebende, nämlich vorrangige und abschließende Spezialregelung darstellt.

Neue Gesichtspunkte dazu sind allerdings im Zusammenhang mit einer Untersuchung zu Tage getreten, welche ein privates Forschungsunternehmen im Auftrag der Bundesanstalt für Arbeitsschutz und Arbeitsmedizin unter Beteiligung des Bundesamtes für Strahlenschutz und des Hauptverbandes der Gewerblichen Berufsgenossenschaften sowie des Deutschen Krebsforschungszentrums Heidelberg, einer Stiftung des öffentlichen Rechtes, zur Bestimmung der Risikofaktoren durchführt, die bei WISMUT-Bergarbeitern Lungenkrebs und Leukämie verursacht haben. Diesen Forschungsgegenständen kommt wegen der Arbeitsbedingungen, die im WISMUT-Uranbergbau geherrscht haben, große Bedeutung zu. Der Bundesgesetzgeber hat eigens Sonderregelungen für die Nutzung der Datenbestände des „Gesundheitswesens Wismut“ zu Forschungszwecken geschaffen, vgl. BGBl. I 1997, S. 972.

(2) Soweit es sich um die Doppel der Meldungen zum „Nationalen Krebsregister beim Zentralinstitut für Krebsforschung bei der Akademie der Wissenschaften der DDR“ (NKR) handelt, richtet sich der Zugang zu diesen Daten ausschließlich nach Krebsregisterrecht, also nach § 8 KRG. Das bedeutet: Das Forschungsunternehmen muss sich die Daten beim Gemeinsamen Krebsregister der sechs östlichen Bundesländer in Berlin besorgen. Stellen im Freistaat Sachsen dürfen Daten aus diesen Unterlagen daher nicht zur Verfügung stellen.

(3) Dies gilt auch insoweit, als diese Meldungen (d. h. die sich noch in Sachsen befindenden Doppel) Eintragungen zum Rauchverhalten sowie solche Eintragungen zur beruflichen Tätigkeit des Patienten enthalten, die über das Erhebungsprogramm des § 2 Abs. 2 Nr. 5 KRG hinausgehen. (Das Rauchen wird zur Überraschung des Laien nach geltendem Krebsregisterrecht nicht erfasst; die Erweiterung des Erhebungsprogrammes gemäß Art. 3 Abs. 1 des GKR-Staatsvertrages, als Nachfolgeregelung des § 2 SächsKRGAG, wirkt sich hier nicht aus.) Dies folgt aus der Datenverarbeitungserlaubnis des Art. 6 GKR-Staatsvertrag (Vorgängerregelung: § 5 Abs. 1 SächsKRGAG). Diese Vorschrift, die sich im Rahmen der Öffnungsklausel des § 13 Abs. 4 KRG hält, erlaubt die Verarbeitung, insbesondere auch Nutzung, von zu DDR-Zeiten gemeldeten Daten auch insoweit, als diese über das derzeit gültige Erhebungsprogramm hinausgehen.

Die Sperrwirkung, die das KRG zusammen mit dem SächsKRGAG und dem GKR-Staatsvertrag entfaltet, erfasst also auch insbesondere diejenigen Meldungen aus DDR-Zeiten, welche die - für das Forschungsvorhaben besonders wichtigen - Angaben zum Rauchverhalten enthalten.

(4) Anderes gilt, soweit die betroffenen Personen nachweislich bereits vor 10 Jahren verstorben oder bereits vor mehr als 100 Jahren geboren sind. Folgt man der in § 10 Abs. 1 Satz 3 SächsArchivG zum Ausdruck kommenden Grenzziehung für das Grundrecht auf informationelle Selbstbestimmung, oder - richtiger gesagt - für die datenschutzrechtliche Ausstrahlung des verfassungsrechtlichen Persönlichkeitsrechtes (näher dazu oben unter 5.8.5), dürfen Daten aus Unterlagen dieses Personenkreises auch ohne rechtliche Erlaubnis gespeichert und übermittelt werden.
Allerdings sind die Gesundheitsämter nicht zuständig für die Speicherung solcher ausschließlich historische Gesundheitszustände wiedergebenden Unterlagen. Sofern

diese Unterlagen - z. B. für die Forschung! - von bleibendem Wert sind, ist ihre Aufbewahrung Aufgabe ausschließlich der Archivbehörde, nicht einer anderen Behörde.

Es bleibt also dabei: Meldungen zum NKR dürfen nicht im Gesundheitsamt aufbewahrt werden.

Die Grenzen der datenschutzrechtlichen Ausstrahlung des verfassungsrechtlichen Persönlichkeitsrechtes werden - so muss man das Gesetz wohl verstehen - in § 11 KRG allerdings weit hinausgeschoben, wenn diese Regelung gebietet, die verschlüsselten Identitätsdaten 50 Jahre nach dem Tod oder spätestens 130 nach der Geburt des Patienten zu löschen, was gemäß Art. 6 Abs. 1 Satz 2, Abs. 3 GKR-Staatsvertrag (Vorgängerregelung § 5 SächsKRGAG) auch für die Daten aus DDR-Zeiten Geltung beanspruchen dürfte. Dies ist eine bemerkenswerte Ausweitung des Persönlichkeitsschutzes für diese speziellen Daten gegenüber dem allgemeinen Archivrecht, die man im Hinblick auf die besondere Bedeutung dieser in Teilen Sachsens und Thüringens angefallenen Gesundheitsdaten vielleicht noch einmal überdenken sollte.

(5) Abweichendes gegenüber (1) und (2) gilt für diejenigen Doppel der Meldungen zum NKR, die Bestandteil von Krankenakten aus Einrichtungen des staatlichen Gesundheitswesens der DDR sind: Diese Unterlagen fallen unter das Gebot des § 5 Abs. 2 SächsArchivG, sie dem zuständigen staatlichen Archiv anzubieten, ersatzweise gemäß § 13 Abs. 1, Abs. 3 Satz 1 SächsArchivG dem Kreisarchiv (Stadtarchiv), mit der damit verbundenen Speicherungserlaubnis des § 5 Abs. 5 Satz 1 SächsArchivG.
Eine Entfernung des Doppels der Meldungen zum NKR aus dieser Patientenakte ist nicht geboten, ja sie wäre auch nicht erlaubt: Insoweit setzt sich das Gebot der Bearbeitung des Archivguts *nach archivwissenschaftlichen Erkenntnissen* (vgl. § 8 Abs. 1 SächsArchivG), nämlich unter Wahrung des Entstehungs- und Überlieferungszusammenhanges, gegenüber der Sperrwirkung des KRG durch. Ungefähr demselben Gesichtspunkt trägt das allgemeine Datenschutzrecht in § 19 Abs. 2, § 20 Abs. 2 SächsDSG, was personenbezogene Daten in Aktenbestandteilen betrifft, Rechnung.

Allerdings gibt es keine Rechtsgrundlage dafür, dass diese Patientenunterlagen aus der Zeit vor der Wiedervereinigung vom Gesundheitsamt aufbewahrt werden. Erst recht darf das Gesundheitsamt keinen Zugang zu diesen Daten gewähren, auch nicht unter Anwendung der Datenzugangsregeln des Sächsischen Archivgesetzes. Vielmehr müssen die Unterlagen in der genannten Weise dem zuständigen Archiv angeboten werden.
Erst nach einer Archivierung - im Rechtssinne! - darf das private Forschungsunternehmen Zugang zu den in diesen Unterlagen enthaltenen Daten im Freistaat Sachsen erhalten, also eben seitens der dann zuständigen Archivbehörde.

(6) Soweit die Patienten nicht bereits 10 Jahre verstorben bzw. vor mehr als 100 Jahren geboren sind, darf das betreffende Archiv dem Forschungsunternehmen die benötigten Daten zur Verfügung stellen gemäß § 10 Abs. 4 Satz 2 SächsArchivG. Dies ist eine Befugnis im Sinne von § 203 Abs. 1 StGB im Hinblick auf das

Arztgeheimnis. Sofern über § 5 Abs. 7, 2. Halbsatz SächsArchivG auch das Sächsische Krankenhausgesetz anwendbar sein sollte, wäre die Übermittlung der Patientendaten durch das Archiv an das Forschungsunternehmen von § 34 Abs. 3 Nr. 1 SächsKHG gedeckt.

(7) In beiden Fällen des Datenzuganges für das Forschungsunternehmen, also sowohl beim GKR als auch ggf. beim Sächsischen Staatsarchiv oder beim kommunalen Archiv, muss die Arbeit, die Unterlagen zu den vom Forschungsunternehmen mit Namen, evtl. Anschrift und Geburtsdatum, bezeichneten Personen herauszusuchen, vom Personal derjenigen Stelle geleistet werden, welche die Unterlagen aufbewahrt. Die betreffenden öffentlichen Stellen dürfen diese Arbeit nicht Dritten, also z. B. Beschäftigten des Forschungsunternehmens, überlassen. Das führte zu unnötigen und damit unzulässigen Datenübermittlungen. Dafür, mit derartigen Arbeiten solche wichtigen Forschungsvorhaben zu ermöglichen, gibt es die betreffenden Stellen mit ihrer Aufgabe, Sammlungen personenbezogener Daten zu verwalten.

(8) Praktisches Ergebnis ist es insbesondere, dass es den Gesundheitsämtern nicht erlaubt ist, einschlägige Unterlagen aufzubewahren, außer für die in § 5 Abs. 4 SächsArchivG vorgesehene Frist, und, und zwar auch während dieser Frist, Zugang zu den in den Unterlagen enthaltenen Daten zu gewähren, was namentlich auch für die Verwendung zu Forschungszwecken gilt.
Insoweit die Unterlagen nicht vernichtet werden müssen, wie vorstehend dargestellt, ist das Forschungsvorhaben behindert, solange die Archivierung durch eine zuständige Archivbehörde nicht stattgefunden hat. Bis dahin sind die Daten weiterhin gesperrt zu halten. Soweit die Datensammlungen nicht in die Obhut der Archivverwaltung übernommen werden, sind sie zuverlässig zu vernichten.

Das Schweigen von SMS und SMI auf meine Forderungen werte ich als Zustimmung.

10.1.3 Dienstanweisung für den Datenschutz im Maßregelvollzug fertig gestellt

In 4/10.1.10 hatte ich über Defizite im Maßregelvollzug beim Umgang mit Daten psychisch kranker Straftäter berichtet und auf die Notwendigkeit einer Dienstanweisung hingewiesen. Das SMS hat den Hinweis aufgegriffen und zum 1. Januar 1999 die Dienstanweisung „Datenschutz im Maßregelvollzug“ erlassen (s. a. 5/10.1.1 und 6/10.1.3). Nach meiner Kenntnis gibt es im übrigen Bundesgebiet noch keine solchen Regelungen.

Der nunmehr vorliegenden Verwaltungsvorschrift sind mehrere Entwürfe vorausgegangen, zu denen ich mündlich und schriftlich eingehend Stellung genommen habe, ebenso das SMI und SMJus. Außerdem hat das SMS die Meinung eines externen, in Fragen des Maßregelvollzugs bundesweit anerkannten Experten eingeholt. Auch seine wertvollen Vorschläge wurden in die Dienstanweisung eingearbeitet.

Die größte Schwierigkeit bei der Umsetzung des Vorhabens bereitete das Fehlen bereichsspezifischer Rechtsvorschriften, die berücksichtigen, dass es sich bei dem Betroffenen um einen Patienten *und* Straftäter handelt, und dass das Krankenhaus bei Durchführung des Maßregelvollzugs *auch* als Strafvollzugsbehörde tätig wird.

So findet z. B. das Sächsische Krankenhausgesetz, das in §§ 33 und 34 detaillierte Verarbeitungsvorschriften für Patientendaten enthält, im Maßregelvollzug keine Anwendung, obwohl dies sicher sinnvoll wäre. Auch über §§ 25, 26 SächsPsychKG (Recht auf Besuch, Postverkehr) lässt sich nur ein kleiner Teil der Gesamtproblematik lösen. Deshalb muss subsidiär immer wieder auf das Sächsische Datenschutzgesetz zurückgegriffen werden. Dies ist insofern problematisch, als die Ärzte im Maßregelvollzug und deren berufsmäßig tätige Gehilfen gemäß § 203 Abs. 1 Nr. 1 und Abs. 3 StGB schweigepflichtig sind und sich aus dem Sächsischen Datenschutzgesetz keine Offenbarungsbefugnisse ableiten lassen, weil die in diesem Auffanggesetz enthaltenen allgemeinen Übermittlungs- und Nutzungsvorschriften nicht speziell genug sind. Folglich muss stets das sog. „Zwei-Schranken-Prinzip“ beachtet werden, wenn Patientendaten verarbeitet werden. „Zwei-Schranken-Prinzip“ bedeutet, dass die Daten nur weitergegeben werden dürfen, wenn die Übermittlung datenschutzrechtlich zulässig ist *und* eine Offenbarungsbefugnis (Rechtsgüterabwägung, gesetzliche Mitteilungspflicht bzw. -erlaubnis, Einwilligung) besteht.

Bisher hat der Sächsische Verordnungsgeber von der Ermächtigung in § 42 Abs. 3 SächsPsychKG keinen Gebrauch gemacht. Ob dies die Problematik entschärfen könnte, sollte diskutiert werden.

10.1.4 Wartung und Fernwartung von Datenverarbeitungsanlagen im medizinischen Krankenhausbereich

In 6/10.1.1 habe ich noch die Ansicht vertreten, dass Wartung/Fernwartung von Datenverarbeitungsanlagen im medizinischen Krankenhausbereich *Auftragsdatenverarbeitung* i. S. v. § 33 Abs. 10 SächsKHG sei, eine Auffassung, die allerdings vom SMI nicht geteilt wurde.

Nach neuerlicher Würdigung bin auch ich zu dem Ergebnis gelangt, dass Wartung/Fernwartung keine Auftragsdatenverarbeitung sein kann, da sie sich nicht auf den *Informationsgehalt* von Datenfeldern bezieht, sondern auf eine ausschließlich (rein technisch gesehen) funktionierende Datenverarbeitung ausgerichtet ist. Das Interesse des Wartungspersonals konzentriert sich ausschließlich darauf, Fehler an Hard- und Software zu beheben. Selbst wenn zur Fehlerbeseitigung im Einzelfall (ausnahmsweise) Patientendaten zur Verfügung gestellt werden müssten, ist die damit verbundene „Offenbarung“ an das Wartungspersonal kein Datenverarbeitungsschritt, sondern eine *unabdingbare Nebenfolge*, die wohl in Kauf genommen werden muss.

Gleichwohl darf die Frage der Zulässigkeit der Offenbarung von Patientendaten im Zuge der Wartung/Fernwartung nicht vernachlässigt werden. Ich könnte mir vorstellen, dass im Interesse klarer Verhältnisse für Patienten und Krankenhäuser durch einen entsprechenden Passus im Krankenhaus-Aufnahmevertrag unmissverständlich darauf hingewiesen wird, dass es in Ausnahmesituationen im Falle der Wartung/Fernwartung zu einer Offenbarung der Patientendaten kommen kann und dass der Patient dies mit seiner Unterschrift unter den Vertrag ausdrücklich anerkennt. Schließlich - auch darauf sollte hingewiesen werden - liegt es zuvörderst im Interesse

des Patienten, dass die ihn betreffenden Daten nicht verfälscht, verstümmelt oder unlesbar werden oder gar unwiederbringlich verloren gehen.

Dadurch könnten auch die mit der Fremdwartung verbundenen strafrechtlichen Risiken für die Krankenhäuser minimiert werden. Voraussetzung dafür, dass den Patienten eine solche Klausel zur Fremdwartung im Aufnahmevertrag zugemutet werden kann, ist jedoch, dass die Offenbarung von Patientendaten an die Wartungsfirma auf das unumgängliche Maß eingeschränkt wird. D. h., dass in der Praxis alle technischen und organisatorischen Sicherungsmöglichkeiten zu aktivieren sind, damit Patientendaten nur dann zur Kenntnis des Wartungspersonals gelangen, wenn mit vertretbarem Aufwand keine andere Lösung möglich ist.

Die Wartung und vor allem die Fernwartung sind auf eine vertragliche Grundlage zu stellen, in der das Wartungsunternehmen explizit zur Verschwiegenheit verpflichtet wird. Für Zuwiderhandlungen sind *empfindliche* Vertragsstrafen vorzusehen. Die Unternehmen müssen Erklärungen über die Zuverlässigkeit ihres Wartungspersonals abgeben. Unter Umständen empfiehlt es sich, Führungszeugnisse nach dem BZRG zu verlangen.

Die externen Mitarbeiter müssen der Klinik oder dem Krankenhaus namentlich benannt werden. Dieser Personenkreis soll aber überschaubar bleiben und möglichst wenig wechseln.

Schließlich sollte die Wartung und Fernwartung nur dann durchgeführt werden, wenn sichergestellt ist, dass ausreichender eigener Sachverstand für die Beurteilung der externen Aktivitäten vorhanden ist.

Für alle Wartungs- und Fernwartungsaktivitäten ist ein Logbuch zu führen, aus dem der Grund der Wartung, der Zeitpunkt und die die Wartung durchführende Person sowie die Wartungsaktivitäten, insbesondere ob auf den Echtdatenbestand zugegriffen werden musste, erkennbar sein müssen.

Um den sächsischen Krankenhäusern über das SMS ein abgestimmtes Konzept für das „handling“ der Wartung/Fernwartung an die Hand geben zu können, habe ich meine Vorstellungen zu den technischen und organisatorischen Erfordernissen zunächst der Sächsischen Landesärztekammer, der Sächsischen Landeszahnärztekammer und der Krankenhausgesellschaft Sachsen mitgeteilt und um Ergänzungs- und Verbesserungsvorschläge gebeten.

Die Angelegenheit ist als „Dauerbrenner“ noch nicht abgeschlossen.

10.1.5 Behandlung von Patientenunterlagen nach Auflösung der „staatlichen Arztpraxen“ der DDR

In kleineren Gemeinden der DDR, in denen es keine Poliklinik gab, waren „staatliche Arztpraxen“ für den Gesundheitsschutz der Bürger eingerichtet worden. Sofern diese

„staatlichen Arztpraxen“ nach der Wende aufgelöst wurden, gelangten die Patientenunterlagen manchmal in die Obhut der Gemeinde, ein Zustand, der sich mit der ärztlichen Berufsordnung und der ärztlichen Schweigepflicht nicht vereinbaren lässt. § 10 Abs. 4 Berufsordnung schreibt nämlich u. a. vor, dass Patientenunterlagen bei Aufgabe einer Arztpraxis in „gehörige“ Obhut gegeben werden müssen. Diese Berufsordnung hat den größtmöglichen Schutz zu sichern, denn das Arzt-Patientengeheimnis ist ein hohes Schutzgut. Irgendeine amtliche Obhut reicht also keinesfalls aus. Nach meinem Dafürhalten hätten die Patientenunterlagen deshalb zur Wahrung des Patientengeheimnisses entweder von den Gesundheitsämtern übernommen oder im Hinblick auf § 5 SächsArchivG dem Kommunalarchiv angeboten werden müssen. Eine Aufbewahrung durch (Hilfs-)Personen, die nicht dem Arztgeheimnis unterliegen, ist immer dann nicht „gehörig“, wenn z. B. eine ärztliche Obhut im Gesundheitsamt zur Verfügung steht.

In einem konkreten Fall habe ich dafür gesorgt, dass die Patientenunterlagen einer aufgelösten Arztpraxis dem Zugriff durch gemeindliches Personal entzogen wurden, indem sie in die Obhut des Gesundheitsamtes gelangten.

Das von mir unterrichtete SMS hat daraufhin dem Gesundheitsamt, das unter enormer Raumnot litt, folgende Verfahrensweise vorgeschlagen:

1. Mit Einwilligung der Patienten dürfen deren Patientenakten an den nun behandelnden Arzt übergeben werden.

2. Alle anderen Patientenakten (die also nicht zur Weiterbehandlung benötigt werden) sollten an das Kreisarchiv des Landratsamtes übergeben werden (was ich im Hinblick auf §§ 5, 6 SächsArchivG für zulässig halte).

10.1.6 Anfertigung von Personalausweis-Kopien bei der Patientenaufnahme

Ein Petent, der sich zur Notfallbehandlung in ein Krankenhaus begeben musste und seine Chipkarte nicht dabei hatte, teilte mir mit, dass sein Personalausweis kopiert worden sei. Nach seinem Veständnis hätte es ausgereicht, wenn das Krankenhaus die benötigten Daten seinem Ausweis entnommen hätte.

Dem habe ich zugestimmt; denn gemäß § 33 Abs. 2 Nr. 1 SächsKHG dürfen Patientendaten nur erhoben, verarbeitet und gespeichert werden, soweit dies im Rahmen des Behandlungsverhältnisses *erforderlich* ist. Außer Namen, Anschrift und Geburtsdatum des Patienten besteht kein Erfordernis an der Kenntnis weiterer Daten aus dem Personalausweis.

Ich habe das Krankenhaus gebeten, diese Praxis einzustellen.

Der Verwaltungsleiter des Krankenhauses hat versichert, das Vorkommnis sei ein Einzelfall gewesen. Gleichwohl habe er die Kliniken per Rundschreiben über die Einhaltung datenschutzrechtlicher Erfordernisse informiert.

10.1.7 Auskünfte über Psychiatriepatienten zur Prüfung von Schadensersatzansprüchen

Ein psychisch kranker Patient in einem Landeskrankenhaus hatte eine Mitarbeiterin so schwer verletzt, dass sie längere Zeit arbeitsunfähig war. Das LfF prüfte daraufhin, ob der Patient gemäß § 38 BAT-O für die dem Freistaat Sachsen entstandenen Dienstausfallkosten schadensersatzpflichtig gemacht werden konnte. Im Zuge dieser Prüfung bat es das Krankenhaus „im Wege der Amtshilfe“ um Mitteilung über die Zurechnungsfähigkeit des Patienten. Offensichtlich war dem LfF - wie übrigens vielen anderen sächsischen Behörden - immer noch nicht bekannt, dass personenbezogene, erst recht ärztliche Daten nur unter ganz bestimmten datenschutzrechtlichen Voraussetzungen übermittelt werden dürfen, also amtshilfefest geschützt sind (vgl. BVerfGE 65, S. 46).

Das Krankenhaus hatte zu recht Zweifel an der Rechtmäßigkeit des „Amtshilfeersuchens“. Ich teilte ihm mit, dass § 33 Abs. 3 Nr. 1 bis 8 SächsKHG abschließend regelt, in welchen Fällen die Daten eines Patienten *ohne dessen Einwilligung* an Personen oder Stellen außerhalb des Krankenhauses übermittelt werden dürfen. Da hier keine der in den Nummern 1 bis 8 genannten Voraussetzungen zutraf, durfte das Krankenhaus die Auskunft nur mit Einwilligung des Patienten geben. Zwar stand dieser unter Betreuung; zur Abgabe einer Einwilligungserklärung war er jedoch in der Lage.

10.1.8 Melderechtliche Auskunft von Krankenhäusern bei telefonischen Anfragen von Polizeibehörden über Patienten

Krankenhäuser stehen häufig vor der Frage, ob und unter welchen Voraussetzungen sie der Polizei Auskunft (auch telefonisch) über Patienten geben dürfen. § 33 Abs. 3 Nr. 8 SächsKHG erlaubt u. a. die Übermittlung von Patientendaten an Personen oder Stellen außerhalb des Krankenhauses, wenn sie in einem anderen Gesetz geregelt ist.

Ein solches Gesetz ist das Sächsische Meldegesetz. Gemäß § 20 Abs. 2 Satz 1 SächsMG ist jedes Krankenhaus verpflichtet, aufgenommene Patienten unverzüglich in ein Verzeichnis einzutragen, und zwar mit Namen und Anschrift, Geburtsdatum und Staatsangehörigkeit sowie Aufnahme- und Entlassungsdatum (§ 20 Abs. 3 SächsMG). Aus diesem Verzeichnis kann eine Polizeidienststelle Auskunft verlangen, soweit dies nach ihrer Feststellung zur Abwehr einer *erheblichen und gegenwärtigen* Gefahr, zur Strafverfolgung oder zur Aufklärung des Schicksals von Vermissten oder Unfallopfern *im Einzelfall* erforderlich ist (§ 20 Abs. 4 SächsMG). Die Verantwortung, dass diese Voraussetzungen vorliegen, trägt die Polizei.

Die Art des Auskunftsverfahrens ist nicht geregelt, so dass grundsätzlich auch telefonische Auskünfte möglich sind. Dabei muss jedoch besonders sorgfältig vorgegangen werden; denn die „Schwachstelle“ ist die Identitätsfeststellung des Anrufers. Es muss gewährleistet sein, dass die Daten des Patienten tatsächlich an die anfragende Polizeidienststelle, und dort an den befugten Beamten, übermittelt werden. Das Krankenhauspersonal hat sich demnach zu vergewissern, dass der Anrufer tatsächlich dem auskunftsberechtigten Personenkreis zuzurechnen ist.

Als Maßnahme hat sich z. B. die Vereinbarung von Kennwörtern bewährt. Datenschutzrechtlich bestehen keine Bedenken, sie auch für einen längeren Zeitraum im Voraus festzulegen. In diesem Fall sind sie jedoch verschlossen und besonders gesichert aufzubewahren und den befugten Personen kurzfristig bekannt zu geben, bevor das aktuelle Kennwort die Gültigkeit verliert.

Um klare Verantwortlichkeiten zu schaffen, sollten der Verwaltungsleiter des Krankenhauses und der Leiter der Polizeidienststelle die Kennwörter vereinbaren. Dabei ist die Zahl der Beschäftigten, die sie zur Kenntnis erhält, so klein wie möglich zu halten. In überschaubaren Verhältnissen ist es aber auch möglich, über längere Zeit Kontakt zu pflegen und sich dann an der Stimme zu erkennen.

Zu betonen bleibt, dass sich die Auskünfte auf *Einzelfälle* beschränken müssen.

10.1.9 Aufzeichnung und Auswertung von Telefonaten im Rettungswesen

Ein Petent, der zur Notfallbehandlung seiner Frau den Rettungsdienst angerufen hatte, teilte mir mit, die Rettungsleitstelle hätte die in diesem Zusammenhang geführten Telefonate auf Band mitgeschnitten. Der Gesprächstext sei später einem Notarzt als Beweismittel für eine gegen ihn gerichtete Klage zur Verfügung gestellt worden. Der Petent fragte, ob das Aufzeichnen von Telefonaten zulässig und die Übermittlung der Gesprächsdaten rechtmäßig gewesen sei.

Ich habe dem Träger der Rettungsleitstelle (Landratsamt) und dem Petenten mitgeteilt, dass datenschutzrechtlich keine Bedenken bestehen, wenn im Rettungswesen Gespräche mitgeschnitten werden. Dies sei zum einen für die Durchführung der Rettungseinsätze selbst erforderlich, zum anderen diene es dem Nachweis, dass der Rettungseinsatz ordnungsgemäß abgelaufen ist (§ 28 Abs. 1 Nr. 1 und 3 SächsRettDG).

Die Übermittlung des Gesprächstextes an den Notarzt war jedoch unzulässig; denn der abschließende Charakter des § 28 Abs. 1 Nr. 1 bis 4 SächsRettDG lässt sie nur für folgende Zwecke zu:

1. die Durchführung des Einsatzes,
2. die unmittelbar anschließende Versorgung des Patienten,
3. den Nachweis der ordnungsgemäßen Durchführung eines Einsatzes,
4. der Abwicklung eines Beförderungsauftrages, insbesondere die Abrechnung.

Keiner dieser Erlaubnistatbestände war hier erfüllt.

10.1.10 Veröffentlichung personenbezogener Daten bei Verlust von Arztausweisen im Ärzteblatt Sachsen

In 4/5.1.27 habe ich auf die datenschutzrechtliche Problematik bei Veröffentlichung personenbezogener Daten im SächsABl. bei Verlust von *Dienst*ausweisen hingewiesen. Das führte schließlich zur Einstellung der Veröffentlichungspraxis.

Der Sächsischen Landesärztekammer, die den Verlust von Arztausweisen personenbezogen im Ärzteblatt Sachsen veröffentlichte, habe ich Folgendes mitgeteilt:

Nach § 4 Abs. 1 SächsDSG dürfen sächsische öffentliche Stellen personenbezogene Daten nur verarbeiten, wenn es das Sächsische Datenschutzgesetz oder eine andere Rechtsvorschrift erlaubt oder soweit der Betroffene eingewilligt hat. Ohne ausreichende Rechtsgrundlage oder bei fehlender Einwilligung ist die Veröffentlichung personenbezogener Daten demnach unzulässig (siehe auch Art. 33 SächsVerf).

Ich habe um Mitteilung gebeten, ob diese Grundsätze bei der personenbezogenen Veröffentlichung der Arztausweisverluste im Ärzteblatt Sachsen ausreichend berücksichtigt wurden und angeregt, eine Lösung ohne Namensnennung zu finden.

Die Sächsische Landesärztekammer hat mitgeteilt, dass der Verlust der Arztausweise mit Namensnennung veröffentlicht wird, um Missbrauch zu vermeiden. Beispielsweise könnten Personen, die in den Besitz eines abhanden gekommenen Arztausweises gelangt sind, verschreibungspflichtige Arzneimittel erwerben.

Nach meiner Einschätzung ist die Veröffentlichung von Arztausweisverlusten im Ärzteblatt Sachsen nicht geeignet, einen solchen Missbrauch zu verhindern.

Zum einen wird das Ärzteblatt Sachsen in erster Linie nur von sächsischen Ärzten gelesen und nicht von den Apothekern. Selbst wenn es von den Apothekern gelesen würde, müssten diese die veröffentlichten Ausweisverluste auch speichern und mit vorgelegten Arztausweisen vergleichen, wenn der Erwerb von verschreibungspflichtigen Medikamenten durch Unbefugte wirksam verhindert werden soll.

Zum anderen kann eine Person, die in den Besitz eines abhanden gekommenen Arztausweises gelangt ist, sehr wohl in anderen Bundesländern aktiv werden, weil dort die Veröffentlichungen im Ärzteblatt Sachsen nicht bekannt sein dürften.

Nach meinem Dafürhalten wäre das einzige wirksame Mittel, unbefugten Medikamentenerwerb zu verhindern eine Liste/Datei über alle bundesweit abhanden gekommenen Arztausweise, die allen Apotheken im Bundesgebiet als Kontrollinstrument mit der Maßgabe zur Verfügung gestellt werden müsste, vorgelegte Arztausweise entsprechend abzugleichen.

Da mir Bestrebungen in dieser Richtung nicht bekannt sind, sollten die Apotheker motiviert werden, sich *generell* bei Medikamentenerwerb durch Ärzte neben dem Arztausweis (der im Übrigen mit einem Lichtbild versehen ist) *auch den Personalausweis* vorlegen zu lassen. So heißt es auch in einem mir vorliegenden Arztausweismuster: „*Nur gültig in Verbindung mit einem amtlichen Personalausweis oder Reisepaß.*“

Einer personenbezogenen Veröffentlichung von abhanden gekommenen Arztausweisen im Ärzteblatt Sachsen bedarf es jedenfalls nicht. Die Sächsische Landesärzte-

kammer hat inzwischen signalisiert, künftig auf entsprechende Veröffentlichungen verzichten zu wollen.

10.1.11 Herausgabe von Patientenakten, Epikrisen, OP-Berichten bei Verdacht eines unnatürlichen Todes

Ein Krankenhaus teilte mir mit, dass Polizeibeamte bei Verdacht eines unnatürlichen Todes die Herausgabe von Patientenunterlagen verlangen würden. Durch das forsche Auftreten der Beamten und gelegentlich auch durch Androhung der Beschlagnahme der Akten seien verunsicherte Ärzte bereit, die geforderten Unterlagen herauszugeben, nachdem zunächst in den Todesbescheinigungen (§ 14 SächsBestG) nachgesehen wurde, ob eine nichtnatürliche Todesursache vorlag.

Das Herausgabebegehren ist im Hinblick auf §§ 97 Abs. 2 Satz 2, 98 Abs. 1 StPO und § 27 SächsPolG sowie nach § 33 Abs. 3 SächsKHG problematisch. Andererseits darf nach meinem Dafürhalten die Aufklärung einer durch strafbare Handlung herbeigeführten Todesursache durch Verweigerung der Herausgabe von einschlägigen Patientenunterlagen nicht unmöglich gemacht werden.

Das SMI und SMS bat ich um Stellungnahme, nach welchen Kriterien aus dortiger Sicht Krankenhausärzte im Falle eines nichtnatürlichen Todes Patientenunterlagen an die Polizei herausgeben dürfen.

Das SMS kommt in seiner Stellungnahme zum Ergebnis, dass weder § 14 SächsBestG noch § 33 Abs. 3 SächsKHG eine Herausgabe von Patientenunterlagen an die Polizei zulassen. Allenfalls käme eine *Beschlagnahme* der Patientenunterlagen dann in Betracht, wenn

1. der Arzt selbst einer Straftat verdächtigt wird,
2. das Interesse an der Aufklärung der Straftat gegenüber dem datenschutzrechtlichen Schutz des verstorbenen Patienten überwiegt und
3. der verstorbene Patient den Arzt von seiner Schweigepflicht entbunden hat oder dies seinem mutmaßlichen Willen entsprochen hätte.

Die Stellungnahme des SMI steht noch aus.

10.1.12 Bestattungswesen und medizinische Forschung

Anlässlich zweier Forschungsvorhaben war ich mit mehreren Fragestellungen, die das Sächsische Bestattungsgesetz (SächsBestG) aufwirft, befasst:

1. Zum einen ging es darum, dass Mitarbeiter einer sächsischen Universität zur Durchführung ihres Forschungsvorhabens Einsicht in Todesbescheinigungen nehmen wollten. Zur Erleichterung der Einsichtnahme sollten die betreffenden Gesundheitsämter der Universität Kopien der Todesbescheinigungen zusenden.
   § 14 SächsBestG regelt, wann und wie eine Todesbescheinigung auszustellen ist, wer ein Exemplar derselben aufzubewahren hat und unter welchen Voraussetzun-

gen eine Einsichtnahme in die Todesbescheinigungen zu gewähren ist bzw. Auskünfte daraus zu erteilen sind: Gemäß § 14 Abs. 5 Satz 3 Nr. 2 SächsBestG können die Gesundheitsämter auf Antrag Einsicht in die Todesbescheinigung gewähren oder Auskünfte daraus erteilen, wenn Hochschulen oder andere mit wissenschaftlicher Forschung befasste Stellen die Angaben für ein wissenschaftliches Vorhaben benötigen und wenn dem wissenschaftlichen Interesse an der Durchführung des Forschungsvorhabens größeres Gewicht als den Belangen des Verstorbenen oder seiner Hinterbliebenen beizumessen ist. In dem von mir zu prüfenden Fall war von einem überwiegenden Interesse an der Durchführung des Forschungsvorhabens auszugehen.
Was nun die Erleichterung der Einsichtnahme durch Übersendung von Kopien der Todesbescheinigungen betraf, bin ich zu dem Ergebnis gekommen, dass die Befugnis des Gesundheitsamtes, Einsicht in die Todesbescheinigung zu gewähren oder Auskünfte daraus zu erteilen, auch die Erlaubnis umfasst, Kopien anzufertigen und zu übersenden. Ein sachlicher Grund, die Einsicht dadurch zu erschweren, dass die Datenübermittlung auf Einsichtnahme an Ort und Stelle oder Auskunft ohne Benutzung der Fotokopiertechnik beschränkt werden sollte, ist nicht ersichtlich. Insbesondere kann auch aus § 14 Abs. 5 Satz 2 SächsBestG kein Umkehrschluss gezogen werden. Diese Regelung bestimmt, dass eine Kopie der Todesbescheinigung dem Gesundheitsamt des letzten Hauptwohnortes übermittelt werden kann. Dass damit die Übermittlung von Kopien an andere Stellen oder Privatpersonen, die zur Einsichtnahme berechtigt sind, ausgeschlossen werden sollte, ist weder dem Gesetzestext noch der Gesetzbegründung zu entnehmen. Auch die Auslegung nach Sinn und Zweck der Regelung lässt eine solche Schlussfolgerung nicht zu.

2. Eine weitere sächsische Universität hat vor, im Rahmen eines Forschungsvorhabens ihre Mitarbeiter an Obduktionen teilnehmen zu lassen und bei der Obduktion Lichtbilder anzufertigen.
Ich bin zu dem Ergebnis gekommen, dass die Teilnahme eines Forschers an einer Obduktion, die aus einem der in § 15 Abs. 1 Nr. 1-3 SächsBestG genannten Gründe, also nicht zu Forschungszwecken, durchgeführt wird, zulässig ist, wenn die Voraussetzungen des § 15 Abs. 1 Nr. 4 SächsBestG vorliegen und der die Obduktion durchführende Arzt mit einer Teilnahme einverstanden ist:
Zwar sieht das Sächsische Bestattungsgesetz eine Teilnahme Dritter, die die Obduktion nicht durchführen, seien diese Dritten auch Ärzte oder sogar Fachärzte für Pathologie oder für Rechtsmedizin, an der Obduktion nicht vor. Die Strafprozessordnung, die neben dem Sächsischen Bestattungsgesetz Regelungen zur Durchführung einer Obduktion enthält, sieht zwar eine Teilnahme Dritter vor, jedoch nicht die eines Forschers, sondern die der Staatsanwaltschaft bzw. des die Obduktion anordnenden Richters. Aus diesen Regelungen lässt sich gleichwohl nicht schließen, dass als teilnehmende Dritte lediglich die Staatsanwaltschaft bzw. der anordnende Richter in Betracht kommen. Das folgt im Wege eines Erst-recht-Schlusses aus § 15 Abs. 1 Nr. 4 SächsBestG:

Ein Forscher darf eine Obduktion durchführen, wenn die Voraussetzungen des § 15 Abs. 1 Nr. 4 SächsBestG erfüllt sind. Ist er aber berechtigt, selbst eine

Obduktion durchzuführen, kann ihm eine bloße Teilnahme an einer Obduktion nicht verwehrt werden, es sei denn, der die Obduktion Durchführende hat Einwände, denn bei einer bloßen Teilnahme sind nicht nur die Interessen des Verstorbenen bzw. der die Totenfürsorge wahrnehmenden Angehörigen zu berücksichtigen, sondern auch die Interessen des die Obduktion durchführenden Arztes an einer ungestörten und unbeobachteten Tätigkeit.

Zur Anfertigung von Lichtbildern bei der Obduktion:

Das Sächsische Bestattungsgesetz bestimmt, dass eine Todesbescheinigung und bei Durchführung einer Obduktion ein Obduktionsschein auszustellen sind (§ 14 Abs. 1 Satz 1, § 15 Abs. 5 SächsBestG). Welchen Inhalt die beiden Bescheinigungen haben müssen und dürfen, ergibt sich aus § 14 Abs. 2 und § 15 Abs. 5 SächsBestG i. V. m. der Anlage. Lichtbilder werden nicht erwähnt. Für die Anfertigung von Lichtbildern fehlt es an einer gesetzlichen Rechtsgrundlage.
Lichtbilder anzufertigen wäre aber dann zulässig, wenn der Verstorbene zu Lebzeiten eingewilligt hat oder, sofern von ihm eine Erklärung hierzu nicht vorliegt, nunmehr der nach § 10 Abs. 1 SächsBestG verantwortliche Angehörige zugestimmt hat. Die Lichtbilder werden dann nicht Bestandteil des Obduktionsscheines, sondern dürfen nur für den Zweck verwendet werden, auf den sich die Zustimmung des Verstorbenen bzw. des verantwortlichen Angehörigen bezieht.

10.1.13 Zur sog. Leukämie-Studie Rossendorf des SMS

Im Februar 1997 hat das SMS von einer Studie mit dem Titel „Vergleichende Analyse der räumlichen und zeitlichen Verteilung von Krebserkrankungsfällen in Gebieten mit hoher natürlicher Strahlenbelastung im Vergleich zur Umgebung des Zentralinstitutes für Kernforschung (ZfK) Rossendorf“ eine „Kurzfassung zum Forschungsbericht“ veröffentlicht. Diese Kurzfassung konnte jeder Interessierte beim Ministerium anfordern.
Die Untersuchung hatte schon vor ihrer Fertigstellung 1996 den Landtag und die Öffentlichkeit lebhaft beschäftigt. Zu Fragen des Zuganges des privaten Forschungsunternehmens zu Melderegister-, Totenschein- und Archivdaten hat man mich seinerzeit zu Rate gezogen.

Nach Veröffentlichung des genannten Kurzberichtes wurde in der überregionalen Presse und auch vor der Enquéte-Kommission des Deutschen Bundestages zur „Überwindung der Folgen der SED-Diktatur im Prozeß der Deutschen Einheit“ der Vorwurf erhoben, das SMS halte zu Unrecht Teile der Untersuchung geheim. Ein Urheber solcher Vorwürfe beschwerte sich bei mir, weil das Ministerium ihm die Einsicht in Teile der Untersuchung unberechtigt unter Berufung auf den Datenschutz verweigert habe.

Ich habe daraufhin mir die dem Petenten bis dahin vorenthaltenen Teile der Untersuchung angesehen. Es stellte sich heraus, dass Petent und SMS zum Teil aneinander vorbeigeredet hatten, so dass 158 bisher verweigerte - personenbezugsfreie - Seiten zugänglich gemacht werden durften. Für 59 Seiten galt dies allerdings nicht: Sie

enthielten Daten, die mit wenig Zusatzwissen Rückschlüsse auf eine bestimmte Person zulassen. Diese Daten betreffen keineswegs nur die Umgebung Rossendorfs, sondern viele Orte in Sachsen, eben das ganze zum Vergleich herangezogene Gebiet. Zur Veranschaulichung habe ich dem Petenten einige Auszüge aus den Tabellen in anonymisierter Form zugesandt.

Ergebnis und Verfahrensweise haben beide Seiten zufriedengestellt.

Was die auch seitdem noch nicht verstummte Kritik an der wissenschaftlichen Richtigkeit der Untersuchung betrifft - im Februar 1999 konnte man von einem vom SMS veranstalteten Kolloquium dazu in der Presse lesen -, habe ich dem Petenten erläutert, dass für eine wissenschaftliche Untersuchung des Wertes der Studie durchaus auch die ihm vorenthaltenen personenbezogenen Daten zur Verfügung stünden, die in dem Forschungsbericht enthalten sind und wie sie ja in den eigentlichen 'Quellen' den Urhebern der Studie zur Verfügung gestanden haben (vgl. § 12 Abs. 2 Nr. 4 SächsDSG); dass dies jedoch nur für einen ausgewiesenen Fachleuten förmlich übertragenen Untersuchungsauftrag (Begutachtung des Forschungsberichtes) gelten könne, nicht für die kritische Lektüre eines interessierten epidemiologischen Laien.

10.2 Sozialwesen

10.2.1 Vermittlung von Arbeitswilligen zur Aufbauarbeit in Bosnien

Nach seinem Besuch in Bosnien war der Presse zu entnehmen, dass der Herr Ministerpräsident die Idee hatte, arbeitslose Fachkräfte zur Aufbauhilfe nach Bosnien zu entsenden. Dass sich daraus ein datenschutzrechtliches Problem entwickeln könnte, hätte ich nicht erwartet. Erst eine Anfrage der SK macht mich problembewusst.

Zahlreiche Interessenten haben sich aufgrund der hoffnungsfrohen Presseveröffentlichungen für die Aufbauhilfe in Bosnien sowohl bei der Arbeitsverwaltung als auch unmittelbar bei der SK beworben. Ein Auskunftsersuchen der SK über die bei der Arbeitsverwaltung registrierten Bewerberdaten sei unter Hinweis auf den „Datenschutz" abgelehnt worden. Die SK fragte, ob die ablehnende Haltung der Arbeitsverwaltung rechtens sei.

Da es sich bei den in Arbeitsämtern gespeicherten Informationen um Sozialdaten handelt, die dem Sozialgeheimnis (§ 35 SGB I) unterliegen, war die Auskunftsverweigerung rechtmäßig, denn §§ 68 ff. SGB X lassen die Übermittlungen von Sozialdaten an die SK nicht zu. Denn es gehört nicht zu den gesetzlichen Aufgaben der SK, Arbeitsvermittlung (im weitesten Sinne) zu betreiben (wegen des Grundsatzes der Gesetzmäßigkeit der Verwaltung bedürfte es im Verhältnis zum einzelnen Bürger nämlich einer gesetzlichen Aufgaben - oder Befugnisübertragung).

Deshalb habe ich der SK vorgeschlagen, die bei ihr eingegangenen Bewerbungen komplett an die Arbeitsverwaltung abzugeben, damit das Arbeitsamt (in allgemeiner, nicht mehr personenbezogener Kooperation mit der SK) die weiteren Maßnahmen ergreift.

Außerdem habe ich darum gebeten, die betroffenen Bewerber über die Abgabe ihrer Bewerbungsunterlagen an die Arbeitsverwaltung schriftlich zu informieren.

Wie die SK mir telefonisch versicherte, sei beabsichtigt, meine Vorschläge umzusetzen.

Ich bat, mich über die weitere Vorgehensweise zu informieren.

10.2.2 Auskünfte aus Gesundheitsunterlagen ehemaliger Volkspolizisten

Der Ärztliche Dienst der Polizei verwaltet u. a. auch die Gesundheitsakten ehemaliger Volkspolizisten. Aus diesen verlangte das Referat „Sonderversorgung" des Polizeipräsidiums Dresden Auskunft über die Krankheitstage eines Betroffenen zur Überführung der Ansprüche und Anwartschaften aus Zusatz- und Sonderversorgungssystemen der DDR in die Rentenversicherung. Der Ärztliche Dienst verweigerte dies unter Berufung auf die ärztliche Schweigepflicht; zu Unrecht, wie ich meine. Denn gemäß § 8 Abs. 1 Satz 1 AAÜG hat der vor der Überführung der Ansprüche und Anwartschaften zuständige Versorgungsträger (dies sind nach Artikel 13 EinigVtr die neuen Bundesländer als Rechtsnachfolger der DDR, also auch der Freistaat Sachsen) dem für die Feststellung der Leistungen zuständigen Träger der Rentenversicherung, hier der BfA, die Daten mitzuteilen, die zur Durchführung der Versicherung und der Feststellung der Leistungen aus der Rentenversicherung erforderlich sind. Diese Aufgabe hat die Staatsregierung dem Referat „Sonderversorgung" beim Polizeipräsidium Dresden übertragen. Allerdings verfügt dieses Referat nicht in jedem Fall selbst über sämtliche der notwendigen Daten.

Kann ein Versorgungsträger die Daten nicht den eigenen Unterlagen entnehmen, ist er gemäß § 8 Abs. 1 Satz 4 AAÜG berechtigt, sie *auch von Dritten* anzufordern. Diese sind gemäß § 8 Abs. 1 Satz 5 AAÜG verpflichtet, Auskunft zu erteilen und auf Verlangen die Unterlagen vorzulegen, aus denen die entscheidungserheblichen Tatsachen hervorgehen. Da der Gesetzgeber keine Ausnahmen vorgesehen hat, gilt die Verpflichtung uneingeschränkt, also auch für solche Dritte, die zu dem in § 203 StGB bezeichneten Personenkreis gehören, also grundsätzlich einer besonderen Schweigepflicht unterliegen. Insoweit handelt es sich um eine gesetzliche Mitteilungspflicht, die zur Offenbarung von Daten befugt.

Ob der polizeiärztliche Dienst im Verhältnis zum Referat „Sonderversorgung" Dritter ist, konnte offen bleiben; denn wenn der Gesetzgeber dem Versorgungsträger das Recht einräumt, die Daten *auch* von Außenstehenden anzufordern, darf er dies erst recht im eigenen Bereich.

10.2.3 Darf das Jugendamt Namenslisten als Verwendungsnachweis über bewilligte Zuwendungen anfordern?

Die Jugendämter unterstützen im Rahmen der verfügbaren Haushaltsmittel u. a. die Jugendarbeit freier Träger, die diese i. S. v. § 11 Abs. 3 Nr. 1 SGB VIII wahrnehmen. Ein Jugendamt verlangte als Nachweis über die Verwendung der bewilligten Zuwen-

dungen Listen mit den Namen und Adressen der Teilnehmer bestimmter Veranstaltungen.

Da der freie Träger lediglich die Auflage hatte, einen Sachbericht über die Anzahl der Teilnehmer, Altersstruktur und soziale Lage der betreuten Kinder zu erstatten, weigerte er sich, dem Jugendamt darüber hinaus die Teilnehmerlisten auszuhändigen und bat mich, die Rechtslage zu prüfen.

Die in den Teilnehmerlisten enthaltenen Daten sind gemäß § 67 SGB X Sozialdaten. Gemäß § 67 a SGB X dürfen sie nur erhoben werden, wenn ihre Kenntnis zur Aufgabenerfüllung erforderlich ist. Die namentliche Kenntnis der Teilnehmer im Zusammenhang mit Verwendungsnachweisen über bewilligte Zuwendungen ist für das Jugendamt nicht erforderlich, da der Nachweis auch in anonymisierter Form (z. B. Anzahl der Teilnehmer) erbracht werden kann. Sofern Zweifel an den Angaben des Zuwendungsempfängers bestehen, hätte ich keine Bedenken, wenn das Jugendamt Einsicht in Teilnehmerlisten verlangt. Dabei ist jedoch zu bedenken, dass niemand verpflichtet ist, sich in eine ausliegende Teilnehmerliste einzutragen.

Künftig wird das Jugendamt im Zusammenhang mit Verwendungsnachweisen grundsätzlich keine Teilnehmerlisten mehr verlangen.

10.2.4 Übermittlung personenbezogener Daten durch den Landeswohlfahrtsverband an Dritte

Für einen Sozialhilfeempfänger war ein Betreuer bestellt worden, der neben anderem die Vermögensangelegenheiten des Betreuten wahrzunehmen hat. Als der Betreute Miterbe eines Nachlasses wurde, ist dann für diesen Teilbereich der Vermögenssorge, nämlich die Vertretung des Betreuten in seiner Stellung als Miterbe des Nachlasses, ein Ergänzungsbetreuer bestellt worden.
Der Landeswohlfahrtsverband als überörtlicher Träger der Sozialhilfe hat daraufhin dem Ergänzungsbetreuer den an den Betreuer als Vertreter des Sozialhilfeempfängers in Vermögensangelegenheiten gerichteten Sozialhilfebescheid insgesamt zur Kenntnisnahme übermittelt.

Diese Übermittlung war rechtswidrig.
Gemäß § 67 b Abs. 1 SGB X sind die Verarbeitung von Sozialdaten und deren Nutzung nur zulässig, soweit die nachfolgenden Vorschriften oder eine andere Rechtsvorschrift in diesem Gesetzbuch es erlauben oder anordnen oder soweit der Betroffene eingewilligt hat.
Eine Einwilligung war nicht erklärt worden.
Als Erlaubnisvorschrift kam § 69 Abs. 1 Nr. 1 SGB X in Betracht. Dessen Voraussetzungen waren jedoch nicht erfüllt:
Nach § 69 Abs. 1 Nr. 1 SGB X ist eine Übermittlung von Sozialdaten zulässig, soweit sie erforderlich ist für die Erfüllung einer gesetzlichen Aufgabe der übermittelnden Stelle nach diesem Gesetzbuch. Übermittelnde Stelle war hier der Landeswohlfahrtsverband. Er hat den Sozialhilfebescheid dem Ergänzungsbetreuer „als Ergänzungsbetreuer“ zur Kenntnisnahme übermittelt, also als Vertreter des Sozialhil-

feempfängers in Vermögensangelegenheiten. Damit sollte dem Ergänzungsbetreuer die für die Wahrnehmung von Vermögensangelegenheiten bedeutsame Tatsache mitgeteilt werden, dass der Betreute Sozialhilfe bezieht. Bedeutsam ist die Tatsache deshalb, weil dem Sozialhilfeempfänger Mitwirkungspflichten gemäß den §§ 60 bis 67 SGB I obliegen. Nach § 60 Abs. 1 Nr. 1 SGB I hat derjenige, der Sozialleistungen beantragt, alle Tatsachen anzugeben, die für die Leistung erheblich sind. Auskunftspflichtig gemäß § 60 Abs. 1 Nr. 1 SGB I ist anstelle des Betreuten der Ergänzungsbetreuer, soweit sich die Auskunftspflicht auf Vermögen bezieht, das zum Nachlass gehört. Die Auskunftspflicht besteht gegenüber dem Landeswohlfahrtsverband, der gemäß § 28 BSHG i. V. m. § 27 Abs. 1 Nr. 6 und Abs. 2, §§ 39 ff. BSHG i. V. m. § 43 Satz 2 BSHG die Aufgabe hat, die Anspruchsberechtigten und den Umfang der Hilfeleistung zu bestimmen, der u. a. von der Höhe des Vermögens des Hilfesuchenden abhängig ist.
Der Landeswohlfahrtsverband hätte also dem Ergänzungsbetreuer zur Begründung eines Auskunftsverlangens mitteilen dürfen, dass der Betreute Sozialhilfe bezieht. In einem solchen Fall ist jedoch ausreichend, allein die Tatsache des Sozialhilfebezuges mitzuteilen, nicht den gesamten Inhalt des Sozialhilfebescheides. Hier wurde jedoch ohne ersichtlichen Anlass der gesamte Sozialhilfebescheid in Abschrift übermittelt.

Der Landeswohlfahrtsverband hat mir zugesichert, sich zu bemühen, solche Versehen in Zukunft zu vermeiden.

10.3 Lebensmittelüberwachung und Veterinärwesen

10.3.1 Übermittlung der Daten landwirtschaftlicher Selbstvermarkter an Handwerkskammern?

In meiner 4/10.3.1 erwähnten Stellungnahme gegenüber dem SMWA habe ich eine Übermittlung der Namen und Anschriften der dort gekennzeichneten Selbstvermarkter von den Lebensmittelüberwachungs- und Veterinärämtern (LÜVÄ) an die Landratsämter als die zur Verfolgung von Ordnungswidrigkeiten nach dem Gesetz zur Bekämpfung der Schwarzarbeit zuständigen Verwaltungsbehörden für zulässig erklärt.

Dieses Schreiben ist von den Handwerkskammern missverstanden worden. Sie haben unter Bezugnahme auf mein Schreiben die LÜVÄ um Übermittlung ebendieser Daten ersucht. Dies sollte, so wurde erklärt, zu dem Zweck erfolgen, zu überprüfen, ob die Selbstvermarkter ihren sich aus der Handwerksordnung ergebenden Verpflichtungen (Anzeigepflichten nach § 16 Abs. 2 und § 18 Abs. 1 HandwO) nachkämen; falls nicht, müsse dies als Ordnungswidrigkeit (§ 118 Abs. 1 Nr. 1 HandwO) verfolgt werden.

Die Handwerkskammern sind jedoch für die Verfolgung von Ordnungswidrigkeiten, auch für solche nach der Handwerksordnung oder der Gewerbeordnung, nicht zuständig. Daher wäre eine Übermittlung an sie, die zum Zweck der Verfolgung von Ordnungswidrigkeiten erfolgte, unzulässig.

Die Betriebsdaten stattdessen verdachtsunabhängig an die zuständige Ordnungswidrigkeitenbehörde zu übermitteln wäre ebenfalls nicht erlaubt, weil dafür eine Rechtsgrundlage fehlt.

Aufgrund meiner ersten dahingehenden Stellungnahme hat das SMWA in Erfahrung gebracht, dass die anderen Bundesländer einheitlich die Meinung vertreten, dass eine Datenübermittlung der von den sächsischen Handwerkskammern gewünschten Art rechtswidrig wäre. Der in dieser Frage vom BMWi zu Rate gezogene BfD hat dabei zu Recht darauf hingewiesen, dass vielfach nicht der in § 3 Abs. 2 HandwO vorausgesetzte Umfang an handwerksmäßiger Herstellung erreicht wird. Für die Einfügung einer Übermittlungserlaubnis in die Handwerksordnung, vergleichbar der Regelung in § 17 Abs. 4, sehe ich mit dem BfD kein Bedürfnis. Wenn ein Bauer einem Metzger oder Bäcker ernstlich Konkurrenz macht, wird der örtliche Handwerker genau wissen, welcher Landwirt das ist.

Angesichts dessen hat das SMWA die sächsischen Handwerkskammern unterrichtet, dass die von ihnen gewünschte Datenübermittlung unzulässig wäre.

10.3.2 Vermeidung von 'Vollzugsdefiziten' durch die Fachaufsicht - ohne zentrale Datensammlung

Ein Regierungspräsidium wollte in seiner Eigenschaft als höhere Lebensmittelüberwachungsbehörde (§ 1 Abs. 2 Nr. 2 SächsAGLMBG) eine hinreichend dichte Kontrolle der Erfüllung bestimmter lebensmittelrechtlicher Pflichten bewirken, die im Zusammenhang mit der Herstellung von Speisen in Großküchen und im Transport der Erzeugnisse zur Essenausgabestellen, etwa in Betrieben und Schulen, zu beachten sind: Für die Zeit zwischen Fertigstellung der Speisen und ihrer Ausgabe an die Essenteilnehmer gilt eine Höchstgrenze, bei der Essenausgabe muss eine Mindesttemperatur eingehalten werden.

Vermeiden wollte das RP ein 'Vollzugsdefizit' bei den unteren Lebensmittelüberwachungsbehörden insbesondere in denjenigen Fällen, in denen die Betriebsstätte des Speisenherstellers in dem örtlichen Zuständigkeitsbereich einer anderen unteren Lebensmittelüberwachungsbehörde (Landkreis oder kreisfreie Stadt) lag als die Essenausgabestelle.
Was die Überprüfung der Ausgabefrist betraf, ging es um eine Überprüfung der Richtigkeit der in den Begleitpapieren enthaltenen Angabe über den genauen Herstellungszeitpunkt. Was die Einhaltung der Mindesttemperatur bei der Anlieferung der Speisen an der Essenausgabestelle anging, kam es darauf an, Speisenhersteller-Betriebe, bei denen häufiger Verstöße bei der Anlieferung festzustellen waren, in Erfahrung zu bringen, gezielt die Ursachen zu ermitteln und die Fehlerquellen auszuschalten.

Dies wollte das RP dadurch erreichen, dass es die unteren Lebensmittelüberwachungsbehörden anwies, ihm als höherer Lebensmittelüberwachungsbehörde betriebsbezogene Mitteilungen zu machen, wenn sie feststellten, dass die Mindest-

temperatur unterschritten oder die Ausgabefrist überschritten war oder dass die Angabe über den Herstellungszeitpunkt fehlte oder aber nicht plausibel war.

Ein derartiges Vorgehen wäre unzulässig, und zwar aus zweierlei Gründen.

Zum einen: Das RP dürfte, und zwar auch in Gestalt des Erhebens, Speicherns, Nutzens und möglicherweise auch Übermittelns betriebsbezogener Daten - nur tätig werden, soweit es als höhere Lebensmittelüberwachungsbehörde für die Ausführung des Lebensmittelrechtes zuständig ist. (Dass diese Daten personenbezogen im Sinne von § 3 Abs. 1 SächsDSG sind, versteht sich von selbst: Betriebe gehören meist bestimmten Menschen, zumindest werden sie von bestimmten Menschen geleitet.)

Die umfassendste Betätigungsweise, zu welcher die höhere Lebensmittelüberwachungsbehörde befugt sein kann, ist die volle Übernahme der unmittelbaren Zuständigkeit, welche unter den Voraussetzungen des sog. Selbsteintrittes zulässig ist, der für die Lebensmittelüberwachungsbehörden in § 2 Abs. 5 SächsAGLMBG geregelt ist. Diese nur für den Ausnahmefall begründete Befugnis setzt voraus, dass die betreffende Aufgabe - also im vorliegenden Fall die Überwachung der Einhaltung von Höchstfristen und Mindesttemperaturen auf dem Weg zwischen Speisenhersteller und Essenausgabestelle - „sachgerecht nur einheitlich wahrgenommen werden kann“.
Dabei muss dieses Einheitlichkeitserfordernis selbstverständlich über die Gleichförmigkeit der Gesetzesanwendung hinausgehen, denn diese ist ja ohnehin ganz allgemein geboten. Dies schließt sogar auch die Einheitlichkeit der Ermessensausübung ein. Ermessensausübungsrichtlinien sollen von der Fachaufsichtsbehörde ja gerade im Wege allgemeiner Verwaltungsvorschriften gegeben werden, sie sollen aber nicht dadurch überflüssig gemacht werden können, dass die höhere Behörde im Wege des Selbsteintrittes selbst tätig wird.
Diese Auslegung von § 2 Abs. 5 SächsAGLMBG wird zumindest durch Art. 84 Abs. 1, Art. 85 Abs. 3 SächsVerf geboten.
Geht es - wie es offenbar vorliegend der Fall war - weniger um die Vermeidung uneinheitlicher Vollzugspraxis bzw. Rechtsanwendung, sondern darum, eine genügend intensive Vollzugstätigkeit herbeizuführen, sind die Voraussetzungen des Selbsteintrittes gemäß § 2 Abs. 5 SächsAGLMBG von vornherein nicht erfüllt.
Damit blieben nur die Befugnisse übrig, welche dem RP als höherer Lebensmittelüberwachungsbehörde kraft Rechts- und Fachaufsicht zustanden.

Das Instrumentarium der Rechts- und Fachaufsicht ermöglichte nach meiner Überzeugung dem RP als höherer Lebensmittelüberwachungsbehörde die gewünschte Intensivierung des Verwaltungsvollzuges:
Zunächst dürfte es ohne zusätzliche Datenverarbeitung, insbesondere Datenübermittlung, äußerst wirksam sein, wenn die örtliche für die Essenausgabestelle zuständige untere Lebensmittelüberwachungsbehörde gemäß § 10 Abs. 4 SächsAGLMBG im Falle einer Speisentemperaturunterschreitung die betreffenden Erzeugnisse sicherstellt oder beschlagnahmt. Dasselbe gilt für den Fall einer sich bereits aus den Unterlagen ergebenden Überschreitung der höchstzulässigen Anlieferungsfrist.

Für Fälle der fehlenden oder nicht plausiblen Angabe des Herstellungszeitpunktes empfiehlt sich dann die Übermittlung von der örtlich für die Essenausgabe zuständigen Stelle an die örtlich für die Betriebsstätte des Speisenherstellers zuständige untere Lebensmittelüberwachungsbehörde. Diese Übermittlung wird durch § 12 Abs. 2, Abs. 1 Satz 1 SächsAGLMBG erlaubt, die strengeren Anforderungen des § 13 Abs. 1 Nr. 1 SächsDSG wären ebenfalls erfüllt. Genauso erlaubt wäre die Übermittlung über die Grenzen der Regierungsbezirke und auch über die Grenze zu benachbarten Bundesländer hinweg.

Um, darüber hinaus, für die als erforderlich erachtete Intensität der Kontrollen durch die untere Lebensmittelüberwachungsbehörden zu sorgen, bietet es sich an, dass das RP zunächst Berichtspflichten einführt, die durch statistische, also nicht auf den einzelnen Betrieb bezogene Angaben zu erfüllen sind.
Hinzu kommen können dann konkrete betriebsbezogene Berichtspflichten - etwa mit Aktenvorlage -, die an bestimmte Fall-Merkmale anknüpfen, so etwa daran, dass innerhalb eines bestimmten Zeitraums ein bestimmter Speisehersteller-Betrieb mit einer bestimmten Anzahl oder einem bestimmten Ausmaß an Verstößen auffällig geworden ist.

Der andere Grund, weswegen das geplante Vorgehen unzulässig wäre, ist folgender: Die recht weit gefasste besondere Datenübermittlungsregelung des § 12 Abs. 2, wohl aber auch des § 12 Abs. 1 Satz 1 SächsAGLMBG ist, zumal bei verfassungskonformer Auslegung, beschränkt auf das für die - wirkungsvolle - Aufgabenerfüllung Erforderliche. Sinn dieser Datenübermittlungserlaubnis ist nicht, die Grenzen, die für die Rechts- und Fachaufsicht bzw. für den Selbsteintritt gelten, zu verschieben. Und es ist, wie wohl vorstehend hat gezeigt werden können, möglich, den gewünschten Zweck einer hinreichenden Kontroll- und Vollzugsdichte auch in der höheren Lebensmittelüberwachungsbehörde ohne eine in der übergeordneten Behörde stattfindende zentrale Datensammlung zu erreichen.
Damit ist der Datenschutz ebenso gewahrt wie die verfassungsrechtlich garantierte Rechtsstellung der Gemeinden als Träger öffentlicher Aufgaben.

SMS und SMI haben, ebenso wie SLT und SSG, gegen meine Rechtsauffassung keine Einwände erhoben.

10.4 Rehabilitierungsgesetze; Vertriebenenzuwendungsgesetz

Darf die Behörde zu Beweiszwecken den DDR-Sozialversicherungsausweis vollständig kopieren?

Anlass zur Beschäftigung mit dieser Frage war das von den zuständigen Behörden geübte Verfahren bei der Durchführung des Vertriebenenzuwendungsgesetzes (VertrZuwG), dem ‘Ersatz’ für einen Teilbereich des sog. *Lastenausgleichs*, der nach dem Zweiten Weltkrieg in Westdeutschland durchgeführt worden ist.
Nach § 2 VertrZuwG ist Voraussetzung für die einmalige Zuwendung an Vertriebene, dass sie nach der Vertreibung ihren ständigen Wohnsitz im Beitrittsgebiet vor dem

3. Oktober 1990 genommen und ihn dort bis zu diesem Zeitpunkt ohne Unterbrechung innegehabt haben; das dient der Vermeidung doppelter Leistungsgewährung. Außerdem erhalten gemäß § 2 Abs. 2 VertrZuwG solche Vertriebenen die Zuwendung nicht, die vor oder nach Ende des Zweiten Weltkrieges einem totalitären System erheblich Vorschub geleistet oder durch ihr Verhalten gegen die Grundsätze der Menschlichkeit oder der Rechtsstaatlichkeit verstoßen haben; dieser Ausschlusstatbestand hat starke Ähnlichkeit mit entsprechenden Regelungen der beiden SED-Unrechtsbereinigungsgesetze, vgl. dazu zuletzt 4/10.4.2.

Die zuständigen Behörden (Sozialämter) ziehen zum Nachweis der Tatbestandsvoraussetzungen sowie zur Überprüfung des Vorliegens von Ausschlussgründen das Arbeits- und Sozialversicherungsbuch der DDR heran. Des Weiteren wird eine Einwohnermeldeauskunft eingeholt.
Als Nachweis des „ständigen Wohnsitzes im Beitrittsgebiet“ dient die Einwohnermeldeauskunft. Sind die Melderegister nicht vollständig erhalten, kann der Nachweis des ständigen Wohnsitzes auch dem Sozialversicherungsausweis entnommen werden. Das Vorliegen von Ausschlussgründen nach § 2 Abs. 2 VertrZuwG lässt sich nur über eine Einsichtnahme in das Arbeits- und Sozialversicherungsbuch überprüfen. Das Arbeits- und Sozialversicherungsbuch der DDR gliedert sich in zwei Teile, einmal den Sozialversicherungsausweis, in dem die Beschäftigungsverhältnisse festgehalten wurden (Art und Dauer des Arbeitsverhältnisses), zum anderen das Arbeitsbuch, in dem der Ausbildungsgang und Parteifunktionen festgehalten wurden. Ob der Ausschlussgrund „einem totalitärem System erheblich Vorschub leisten“ vorliegt, kann anhand bestimmter Beschäftigungsverhältnisse (z. B. Polizei, K 1, MfS) festgestellt werden. Als Orientierung dient die Verwaltungsvorschrift der Sächsischen Staatsregierung zur Prüfung der persönlichen Eignung im Beamtenverhältnis (SächsABl. 1994, S. 41).

Bisher hatten die Behörden bei der Bearbeitung von Anträgen auf Gewährung einer Zuwendung das gesamte Arbeits- und Sozialversicherungsbuch kopiert und zu den Akten genommen.
Diese Vorgehensweise war nicht datenschutzgerecht. Zwar benötigt eine Verwaltungsbehörde für jeden Einzelfall, der ihr zur Bearbeitung vorgelegen hat oder vorliegt, Unterlagen, anhand deren sich der Verfahrensgang nachvollziehen lässt: Zum einen zur weiteren Bearbeitung, zum anderen zum Nachweis eines ordnungsgemäßen Verlaufes des Verwaltungsverfahrens. Mit der Aufbewahrung von Unterlagen, die personenbezogene Daten enthalten, wird jedoch in das Recht auf informationelle Selbstbestimmung eingegriffen. Damit dieser Grundrechtseingriff sich im Rahmen des Verhältnismäßigen hält, dürfen Unterlagen nur im erforderlichen Umfang angelegt und aufbewahrt werden, d. h. nur in dem Umfang, der für ein ordnungsgemäßes Verwaltungsverfahren nötig ist.

Konkret bedeutet das:
Im Rahmen der Entscheidung über die Gewährung einer einmaligen Zuwendung für Vertriebene ist eine Einsichtnahme in das Arbeits- und Sozialversicherungsbuch der DDR zur Überprüfung der Tatbestandsvoraussetzungen und des Vorliegens von Ausschlussgründen erforderlich. Der jeweilige Bearbeiter des Antrages auf Gewäh-

rung einer Zuwendung darf also die Vorlegung des Arbeits- und Sozialversicherungsbuches vom Antragsteller verlangen und es zur Überprüfung der Angaben durchsehen. Begründen die Angaben im Antrag oder im Arbeits- und Sozialversicherungsbuch den Verdacht, es liege ein Ausschlussgrund im Sinne des § 2 Abs. 2 VertrZuwG vor, darf der Bearbeiter Ablichtungen der entsprechenden Passagen des Arbeits- und Sozialversicherungsbuches anfertigen. Dasselbe gilt, soweit der Nachweis des ständigen Wohnsitzes im Beitrittsgebiet aus dem Melderegister nicht hat geführt werden können.
Das reicht aus, damit die Behörde eine ausreichende Entscheidungsgrundlage in Händen hat und nachweisen kann, auf welche Tatsachenfeststellungen die Entscheidung gegründet worden ist. Nicht erforderlich ist hingegen, das gesamte Sozialversicherungsbuch zu kopieren, lediglich um nachzuweisen, dass eine solche vollständige Überprüfung stattgefunden hat. Dazu reicht nämlich der Vermerk aus: „SV-Ausweis hat vorgelegen“/Datum/Unterschrift. Stattdessen könnte auch das Deckblatt kopiert und zu dem Vorgang genommen werden.

Über dies Ergebnis konnte in angenehmer Zusammenarbeit mit dem SMI rasch Einigkeit erzielt werden, zumal der Bund als Geldgeber die Kopie des SV-Ausweises zu Zwecken finanzieller Revision nicht verlangt und wohl auch nicht verlangen dürfte. Das Ministerium hat einen entsprechenden Erlass an die unteren Eingliederungsbehörden gerichtet, in dem diese neue Verfahrensweise angewiesen wird, die im Übrigen auch Kosten sparen dürfte und die Akten von Ballast frei hält.
In dem Erlass wird auch bestimmt, was die Behörde mit denjenigen Ablichtungen zu machen hat, die nach der bisherigen Verfahrensweise angefertigt wurden. Soweit sie nicht zum Nachweis anspruchs- oder ausschlussbegründender Tatsachen benötigt werden, hat die Behörde die Kopien dem Antragsteller auf Verlangen zurückzusenden.

11 Landwirtschaft, Ernährung und Forsten

§ 70 Abs. 3 LwAnpG: Rechtsstandpunkt gerichtlich bestätigt

Die 6/11 geäußerte Gewissheit, dass das SML in der mit ihm abgesprochenen Weise bekanntmachen werde, welche nach § 70 Abs. 3 LwAnpG angefertigten Prüfberichte existieren und dass ihr Inhalt betroffenen ehemaligen LPG-Mitgliedern zur Verfügung steht, war begründet. Dem Landwirtschafts- und dem Innenausschuss des Sächsischen Landtages konnte ich nicht nur, wie angekündigt, die Erledigung der Angelegenheit mitteilen, sondern auch von dem Echo berichten, welches die Bekanntmachungen der Landwirtschaftsverwaltung bei Betroffenen und in Fachkreisen hervorgerufen hat.

Neben dem Dank betroffener ehemaliger LPG-Mitglieder hat es freilich auch den Versuch eines an der Umwandlung einer LPG Beteiligten gegeben, die Offenlegung der Prüfergebnisse, namentlich der ihm seinerzeit für seine Tätigkeit gezahlten Entgelte, gerichtlich untersagen zu lassen.

Der Versuch ist vor dem VG Dresden gescheitert (Beschluss vom 20. November 1998 - 1 K 3007/98). Im Ergebnis, wenn auch nicht in der Begründung, hat das Gericht meinen Rechtsstandpunkt bestätigt. Dadurch hat es zugleich entschieden, dass das Persönlichkeitsrecht der durch eine solche Bekanntgabe von Daten betroffenen Geschäftsführer und in ähnlicher Weise an den Vorgängen Beteiligten an die ehemaligen LPG-Mitglieder (und deren Rechtsnachfolger) der Offenlegung der Prüfergebnisse nicht entgegensteht.

Die Aussichten, dass die sächsische Praxis auch in dem einen oder anderen der übrigen neuen Bundesländer Schule machen wird, dürften damit gestiegen sein.

12 Umwelt und Landesentwicklung

Übertragung der Überwachung der Standorte von Abfallbehältern auf Private (Outsourcing im Ordnungswidrigkeitenbereich)

Abfallbehälter werden von manchen Hausbewohnern oder Nachbarn nicht ordnungsgemäß gefüllt, vielmehr werfen diese ihren Müll zwecks Kostenersparnis oder aus Bequemlichkeit neben die Abfallbehälter.

Eine Stadt wollte über die Einleitung von Ordnungswidrigkeitenverfahren gegen diese Verhaltensweise vorgehen. Mit der Feststellung des für das Ordnungswidrigkeitenverfahren relevanten Sachverhaltes wollte sie einen Privaten, nämlich ein Detektivunternehmen, beauftragen. Wohnanlagen, an denen solche Müllablagerungen am häufigsten vorkommen, sollten überwacht und dabei sollten zu Beweissicherungszwecken entsprechende Vorgänge aus dem Auto heraus gefilmt werden.

Ich habe der Stadt mitgeteilt, dass ich eine solche Übertragung hoheitlicher Befugnisse, nämlich der Verfolgung von Ordnungswidrigkeiten, auf Private für unzulässig erachte. Diese rechtliche Beurteilung ergibt sich im Einzelnen aus Folgendem:

Zuständig für die Verfolgung von Ordnungswidrigkeiten ist die Verwaltungsbehörde (§ 35 OWiG), in diesem Fall also die untere Abfallbehörde nach § 17 Abs. 3 i. V. m. § 13 Abs. 2 Nr. 3 EGAB bzw. die Polizeibehörde nach § 17 Abs. 3 SächsPolG.

Ordnungswidrigkeitenrecht und Kriminalstrafrecht unterscheiden sich in der Art der Rechtsverletzung und der Rechtsfolge. Ordnungswidrigkeiten weisen einen geringeren Grad an ethischem Unwertgehalt auf als Straftaten. Demnach ist auch die Geldbuße keine echte Strafe, weil ihr das mit dieser verbundene Unwerturteil fehlt. Sie stellt jedoch eine Sanktion wegen eines Verstoßes gegen die Rechtsordnung dar und hat deshalb repressiven Charakter.
Repression aber ist eine ausschließlich obrigkeitliche, also staatliche Aufgabe. Die Verfolgung von Ordnungswidrigkeiten fällt in diesen Kernbereich hoheitlichen Handelns, da sie der Ausübung von Repression dient.

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). Es darf sich dabei aber nur um Ausnahmefälle handeln. Würde die ständige Ausübung hoheitlicher Befugnisse in größerem Umfang auf Nichtbeamte übertragen, so wäre dies mit dem Grundgesetz nicht vereinbar (BVerfGE 9, 268, 284).
Da der Staat das Gewaltmonopol besitzt und dieses unteilbar ist, können weder durch Gesetz noch durch Rechtsverordnung oder Erlass, erst recht nicht durch einen Vertrag, Aufgaben und Befugnisse der Repression auf private Dritte übertragen werden. Als einzige Ausnahme vom staatlichen Gewaltmonopol lässt das Gesetz das Festnahmerecht für jedermann gemäß § 127 StPO zu, welches dem Bürger insoweit eine öffentliche Aufgabe überträgt (KK-Boujong, § 127 StPO, Rdnr. 6). Weitere Ausnahmen für die Ausübung staatlicher Repression gegen Private durch Private kennt die deutsche Rechtsordnung nicht.
Die Verfolgungskompetenz kann also nicht durch eine entsprechende Beauftragung auf Private übertragen werden. Zur Verfolgungskompetenz gehört die Herrschaft über den Geschehensablauf bei der Überwachung, also Anordnung und Durchführung der maßgeblichen Ermittlungen (KG NJW 1997, 2894, 2896 lSp. unten).

Dadurch, dass nicht die Stadt selbst als entsorgungspflichtige Körperschaft, sondern stattdessen das von ihr mit der Entsorgung des Abfalls beauftragte private Entsorgungsunternehmen seinerseits einen Privaten beauftragte, den Sachverhalt zu ermitteln und diese Ermittlungen der zuständigen Verwaltungsbehörde in Form einer Anzeige zur Kenntnis zu bringen, würde die Sache nicht besser.
Denn auch das liefe auf eine Übertragung hoheitlicher Befugnisse auf Private hinaus. Dem privaten Dritten dürfen gerade 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. Gerade dies war hier aber nicht bezweckt. Die Stadt, die Kenntnis von den Zuständen hat, wollte den Sachverhalt durch Private „ausermitteln“ lassen und auf Grundlage dieser Erkenntnis eine Entscheidung im Ordnungswidrigkeitenverfahren fällen. Die Anzeige würde nur pro forma erstattet.
Zwar hätte auch das private Entsorgungsunternehmen ein Interesse an einer ordnungsgemäßen Durchführung der Abfallentsorgung und damit an der Ermittlung der Verursacher der Abfallablagerungen. Dies Interesse reichte aber sicher nicht so weit, dass staatliche Aufgaben und Befugnisse auf eigene Kosten wahrgenommen würden (wer bezahlt das Detektivunternehmen?), zumal die Kosten der Entsorgung der rechtswidrig gelagerten Abfälle nicht das beauftragte Entsorgungsunternehmen, sondern die Stadt trägt. Damit wird deutlich, dass das eigentliche Interesse an der Ermittlung bei der Stadt, also der zuständigen Behörde selbst, liegt. Die Grenze des Jedermannsrechtes auf Anzeige von Rechtsverletzungen wäre damit eindeutig hin zu einer gesetz- und verfassungswidrigen Übertragung hoheitlicher Aufgaben und Befugnisse auf Private überschritten. Die Tätigkeit der privaten Ermittler sollte ja

systematisch und nicht nur zufällig im Einzelfall erfolgen, und im Übrigen auch berufsmäßig und gegen Entgelt.
Rechtswidrig wäre ein solches Unterfangen also im Wesentlichen aus denselben Gründen, deretwegen das Kammergericht in seinem Beschluss vom 23.10.1996 (2 Ss 171/96 3 Ws (B) 406/96 - NJW 1997, 2894) die Übertragung der systematischen Überwachung des ruhenden Straßenverkehrs und die dabei erfolgende Feststellung entsprechender Zuwiderhandlungen im Rahmen des sog. Berliner Parkraumüberwachungskonzepts für rechtswidrig erklärt hat.

Es sollte eine einfache Lösung des Problems gefunden werden: Ich habe nichts dagegen, die Hausmeister oder bestimmte Mieter zu erhöhter Aufmerksamkeit anzuhalten und vor allem auf eine interne, selbstverwaltete Regelung der Hausgemeinschaften hinzuwirken. Betroffen von den ordnungswidrigen Ablagerungen sind ja zunächst einmal die Anwohner.
Meiner Erfahrung nach hilft es auch, die 'Müllplätze' durch kommunale Bedienstete, z. B. ABM-Kräfte, regelmäßig und sorgfältig reinigen zu lassen; einer aufwendigen Datenerhebung durch die Obrigkeit bedarf es daher nicht.

13 Wissenschaft und Kunst

13.1 Regierungsentwurf einer Neufassung des Sächsischen Hochschulgesetzes: Zentrale Verarbeitung sämtlicher Professuren-Bewerber-Daten im Staatsministerium?

Gegenüber dem SMWK, das sich mir gegenüber nicht an § 13 Abs. 5 Satz 4, Abs. 7 Satz 1 GeschoSReg gehalten, meine Behörde also nicht rechtzeitig eingeschaltet hatte, habe ich zunächst meine bisherigen Einwendungen gegen die Regelungen zur Evaluation der Lehre (ausführlich 4/13.2) im Hinblick auf die geplante Neuregelung bekräftigt.

Vor allem aber habe ich mich dagegen gewandt, dass in dem inzwischen beim Landtag eingebrachten Entwurf in § 42 Abs. 4 Satz 9 (Vorgängerregelung: § 53 Abs. 9 SHG) vorgesehen ist, dass dem SMWK zusätzlich zu den Unterlagen derjenigen, die Eingang in den Berufungsvorschlag gefunden haben, die gleichen Unterlagen, also derselbe Datensatz, auch für diejenigen Bewerber zur Verfügung gestellt werden sollen, die, salopp formuliert, unter „ferner liefen" rangieren.

Aus der Rechtsprechung des Bundesverwaltungsgerichtes sowie der Oberverwaltungsgerichte folgt, wie ich ausführlich nachgeweisen habe, dass eine solche Regelung verfassungsrechtlich problematisch wäre, weil das Staatsministerium diese Daten für die Wahrnehmung seiner Aufgaben bei der Durchführung des normalen, in § 42 Abs. 5 des Entwurfes beibehaltenen Verfahrens (zurzeit: § 53 Abs. 10 SHG) nicht benötigt. Demgemäß beschränkt sich seine Aufgabe darauf, zu prüfen, ob womöglich keiner der Vorgeschlagenen berufungswürdig ist (§ 42 Abs. 5 Satz 2 des Entwurfes). Aber auch die dem Staatsministerium zustehende Rechtsaufsicht über die

Ordnungsmäßigkeit der im Berufungsverfahren vorgenommenen Auswahl derjenigen Bewerber, die nicht vorgeschlagen werden, könnte die vorgesehene Datenübermittlung aus verfassungsrechtlichen Gründen ebenfalls nicht rechtfertigen; die verfassungsrechtliche Garantie der Autonomie der Hochschule, die im Bereich der Berufung von Professoren besonders stark ist (so das Hochschulurteil des Bundesverfassungsgerichts, E 35, 79, 133; auch E 51, 359, 381), stünde dem entgegen.

Erstaunen muss in diesem Zusammenhang, dass der ausführliche Begründungsteil des Regierungsentwurfes es unterlässt, diese Änderung gegenüber dem bisherigen Recht zu erwähnen. Auch besteht ein sachlicher Zusammenhang der geplanten Rechtsänderung mit den Rechtsfragen, auf die es in dem Prozessverfahren ankommt, welches der Sächsische Datenschutzbeauftragte gegen den Sächsischen Staatsminister für Wissenschaft und Kunst vor dem Sächsischen Oberverwaltungsgericht geführt hat (Beschluss vom 25.9.1998 - 3 S 379/98 - SächsVBl. 1999, 35) und zurzeit vor dem VG Dresden noch führt.

Auch wenn das eine oder andere Bundesland eine ähnliche gesetzliche Regelung haben sollte: Mit einer solchen Datensammlung griffe man meines Erachtens unzulässigerweise in die Autonomie der Hochschule im Bereich der Selbstergänzung der Wissenschaftsgemeinschaft sowie in das Grundrecht der Betreffenden auf informationelle Selbstbestimmung ein. Der Verdacht, dass Register über Nachwuchs-Wissenschaftler und deren Bewerbungsverhalten angefertigt werden sollen, liegt nicht fern.

13.2 Forschungsvorhaben zu Strafverfahren gegen Mitglieder einer bestimmten Berufsgruppe

In vielen Wissenschaftszweigen kommt die Forschung nicht ohne personenbezogene Daten aus. Vielfach sind die benötigten Daten nur bei der öffentlichen Verwaltung vorhanden. Diese greift jedoch in das Grundrecht auf informationelle Selbstbestimmung ein, wenn sie personenbezogene Daten Forschern zur Verfügung stellt. Solche Übermittlungen sind vereinzelt spezialgesetzlich geregelt (z. B. für Archiv-, Sozial- und Statistikdaten). Im Übrigen sind die in den allgemeinen Datenschutzgesetzen enthaltenen besonderen Erlaubnisregeln für eine zu Forschungszwecken stattfindende Datenübermittlung maßgebend. Diesen Regelungen ist gemeinsam, dass sie eine Abwägung verlangen zwischen dem öffentlichen bzw. wissenschaftlichen Interesse an der Durchführung des Forschungsvorhabens und dem persönlichkeitsrechtlichen Interesse des Betroffenen am Unterbleiben der Übermittlung (vgl. § 12 Abs. 2 Nr. 4 i. V. m. § 13 Abs. 1 oder § 15 Abs. 1 Nr. 1 SächsDSG).

Ohne dem - was ich in der F.A.Z. vom 9.9.1998 versucht habe - näher nachzugehen: Es liegt auf der Hand, dass das eine schwierige Abwägung zweier nicht ohne weiteres miteinander vergleichbarer Größen ist. Bei allem Respekt vor dem Grundrecht der Freiheit der wissenschaftlichen Forschung führt jedoch kein Weg an der Durchführung dieser Abwägung vorbei, nachdem nun einmal die informationelle Selbstbestimmung mit Grundrechtsrang ausgestattet ist (Volkszählungsurteil; Art. 33

SächsVerf), so dass ein Eingriff in dies Recht eines überwiegenden Allgemeininteresses als Grundlage bedarf (BVerfGE 65, 1, 44; Verfassungsgrundsatz der Verhältnismäßigkeit).

Die wissenschaftliche Bedeutung eines Forschungsvorhabens kann man als Verwaltungsjurist oder auch als Richter nur schwer beurteilen und gewichten. In der Regel wird man auch als Datenschutzbeauftragter sehr vorsichtig sein, einem wissenschaftlichen Vorhaben das jeweils nötige 'Übergewicht' abzusprechen.
Es gibt aber auch Fälle, in denen dies, also eine negative Stellungnahme zu einer Übermittlung an Forscher, geboten ist. Lehrreich ist dazu die Entscheidung des OLG Hamm vom 28.11.1995 (1 VAs 38/94 - NJW 1996, 940), welche eine Weigerung der Justizverwaltung des Landes Nordrhein-Westfalen bestätigt hat, für eine Habilitationsschrift im Fach Psychiatrie Akten im Zusammenhang mit Fällen von Tötungen von Patienten durch medizinisches Personal in Landeskrankenhäusern zur Verfügung zu stellen.

Es ist ein Ausnahmefall, dass ich mich im Berichtsjahr deutlich gegen die Überlassung von Unterlagen - in diesem Falle der Justiz - für ein universitäres Forschungsvorhaben ausgesprochen habe:
Der Inhaber eines Strafrechtslehrstuhls an einer außerhalb Sachsens gelegenen Hochschule beabsichtigt, ein bundesweit angelegtes Forschungsvorhaben zu Strafverfahren gegen Ärzte durchzuführen. Im Rahmen des Forschungsvorhabens sollen Lehrstuhlmitarbeiter Strafverfahrensakten der Staatsanwaltschaften auswerten. Es war beabsichtigt, auch eine sächsische Staatsanwaltschaft in die Untersuchung einzubeziehen.

Überlässt eine Behörde Forschern Akten zur Auswertung, wird damit der gesamte personenbezogene Inhalt im Rechtssinne übermittelt, auch wenn, wie es hier der Fall ist, Name und Anschrift der betreffenden Personen die Forscher nicht interessieren, weil sie nicht mit diesen in Kontakt treten wollen, um zusätzliche Daten zu bekommen (was andererseits bei manchen Forschungsvorhaben nötig ist).
Da Spezialvorschriften nicht existieren, insbesondere das Justizmitteilungsgesetz leider keine Regelung für Datenübermittlungen zu Forschungszwecken enthält, blieb als mögliche Rechtsgrundlage für eine Einsichtnahme in Strafverfahrensakten das Sächsische Datenschutzgesetz. Da Bedienstete der Universität oder doch aufgrund eines Werk- oder Dienstvertrages für die Universität Tätige in die Akten Einsicht nehmen sollten, hätte es sich, jedenfalls nach allgemein üblicher Rechtsauffassung, um eine Datenübermittlung an eine öffentliche Stelle gehandelt. Maßstab, an dem die Gewährung der Einsichtnahme zu messen war, war also die bereits erwähnte Vorschrift des § 13 Abs. 1 i. V. m. § 12 Abs. 2 Nr. 4 SächsDSG.
Es war dabei davon auszugehen, dass der Forschungszweck nicht erreicht werden könnte, wenn eine vollständig anonymisierte Kopie der Verfahrensakte zur Verfügung gestellt worden wäre. Denn wenn jeder Bezug auf eine in den Akten vorkommende Person (Amtsträger ausgenommen) unmöglich gemacht würde, ließen sich vermutlich die Erkenntnisse, die den Akten entnommen werden sollten, nicht mehr gewinnen. Außerdem wäre der Aufwand für die Staatsanwaltschaften ganz erheblich. Noch größer wäre der Aufwand einer Pseudonymisierung, also einer einheitlichen

Umbenennung der handelnden Personen sowie Tilgung aller Angaben, aus denen deren wahre Identität mit Zusatzwissen zu gewinnen wäre, z. B. in einer Aktenkopie.

Zweifel sind mir hinsichtlich der Eignung der geplanten Verarbeitung personenbezogener Daten (aus den Akten) zur Gewinnung der benötigten Erkenntnisse gekommen. Die Erforderlichkeit des Erhebungsprogramms schien mir in manchen Teilen zweifelhaft, die in den mir eingereichten Unterlagen gegebene Begründung für den Datenbedarf war in Teilen nicht schlüssig.

In dieser vorläufigen Einschätzung bin ich dann vom SMJus bestärkt worden, und zwar auf der Grundlage des dort vorhandenen Praxiswissens über staatsanwaltschaftliche Ermittlungsakten. Das SMJus wäre diejenige Stelle, die darüber entschiede, ob die betreffende Staatsanwaltschaft die Akten den Forschern zur Verfügung stellt.

Ich habe sodann meine Einwände dem Lehrstuhlinhaber im Einzelnen dargelegt. Ich habe auch nach dem Vorliegen einer Pilotstudie oder eines Gutachtens zur wissenschaftlichen Neuheit und zur Gestaltung der geplanten empirischen Untersuchung gefragt. Eine solche Begutachtung durch dritte Wissenschaftler ist im Wissenschaftsbetrieb ja dann üblich, wenn in größerem Umfang finanzielle Förderung benötigt wird.

Bei einer Abwägung des Interesses an der Durchführung des Forschungsvorhabens mit dem Interesse des Betroffenen am Unterbleiben der Übermittlung musste ich zu dem Ergebnis kommen, dass letzteres überwiegt. Dass die Betroffenen durch ein Strafverfahren wegen beruflicher Fehlleistungen in besonderem Maße buchstäblich „betroffen“ sind, ist offensichtlich.

Andere Justizministerien und andere Datenschutzbeauftragte haben Einwände gegen die Konzeption (Eignung) der Studie nicht geltend gemacht, sondern sich darauf beschränkt, die Gestaltung der bei der Auswertung der Akten angefertigten Erhebungsbögen datenschutzfreundlich zu beeinflussen.

Bis jetzt sieht es danach aus, dass die Studie ohne die Verwendung von Akten einer sächsischen Staatsanwaltschaft durchgeführt wird.

13.3 Selbstdarstellung der Hochschule

Eine Hochschule plant eine Ausstellung, in der unter Verwendung personenbezogener Daten ehemaliger Mitarbeiter die jüngere Geschichte der Hochschule dargestellt werden soll.
Willigen die ehemaligen Mitarbeiter in diese Verwendung ihrer Daten nicht ein (wovon in den meisten Fällen nicht ausgegangen werden muss) und sind diese Daten auch noch nicht an anderer Stelle, namentlich in den üblichen Personal- und Lehrveranstaltungsverzeichnissen, bereits veröffentlicht worden, ist eine Veröffentlichung nur zulässig, wenn eine Rechtsvorschrift dies erlaubt.
Befinden sich die Daten in einem regulären Archiv nach dem Sächsischen Archivgesetz (vgl. § 14 SächsArchivG), hat die Hochschule das Recht, das Archivgut zu

benutzen und die so erhaltenen Daten auch zu veröffentlichen, beides jedoch erst nach Ablauf der Schutzfristen. Eine Verkürzung der Schutzfristen nach § 10 Abs. 4 Satz 2 SächsArchivG kommt nicht in Betracht, da die Ausstellung kein Forschungsvorhaben ist. Schutzfristen gelten allerdings nicht für die Benutzung solcher Daten, welche zur Amtsausübung des Mitarbeiters der Hochschule gehören, so z. B. die Zeitdauer der Tätigkeit an der Hochschule und die Unterrichtsfächer. Dies habe ich in 6/5.8.5 ausführlich dargelegt.
Sind die Daten noch Bestandteil der bei der Hochschule aufbewahrten Personalakten, richtet sich die Zulässigkeit der Veröffentlichung der Daten nach dem Sächsischen Hochschulgesetz, dem Beamten- und Angestelltenrecht und § 31 SächsDSG. Dahingestellt bleiben kann, ob die entsprechenden Vorschriften (§ 135 Abs. 3 SHG, § 124 i. V. m. § 121 SächsBG sowie § 31 Abs. 1 SächsDSG) auch für die Daten ausgeschiedenen Personals gelten, da keine dieser Vorschriften eine Verarbeitung personenbezogener Daten zu dem Zweck der Darstellung der geschichtlichen Entwicklung der Hochschule für zulässig erklärt. Auch § 12 Abs. 1 und Abs. 2 SächsDSG ist keine Erlaubnis der mit der geplanten Datennutzung verbundenen Zweckänderung der Daten zu entnehmen.

Da eine gesetzliche Grundlage für die Veröffentlichung der personenbezogenen Daten im Rahmen einer solchen Ausstellung nicht gegeben ist, ist die Hochschule auf die Bereitschaft der ehemaligen Mitarbeiter angewiesen, zusätzliche Angaben auf Einwilligungsgrundlage zur Verfügung zu stellen.
Diese Rechtslage war für mich Anlass, im Rahmen des Verfahrens zur Neufassung des Sächsischen Hochschulgesetzes anzuregen, in § 105 Abs. 3 Satz 1 den Verarbeitungs-Zweck der Darstellung der Leistungsfähigkeit der Hochschule und ihrer jüngeren Geschichte in Ausstellungen und Veröffentlichungen ergänzend aufzunehmen. Zudem habe ich angeregt, in § 105 Abs. 1 Satz 1 und Abs. 2 SHG ergänzend als weiteren Datenverarbeitungs-Zweck aufzunehmen die Pflege des Kontaktes der Hochschule mit ehemaligen Studenten. Auch hier sehe ich ein praktisches Bedürfnis sowohl seitens der Hochschule wie seitens der ehemaligen Hochschulangehörigen.

13.4 OECD-Studie „PISA“

Die OECD (Organisation für wirtschaftliche Zusammenarbeit und Entwicklung) führt in rund 30 Industriestaaten eine Untersuchung zur Qualität des Schulwesens, vor allem in den Fächern Mathematik, Naturwissenschaften und Landessprache („Leseverständnis“) sowie zu fächerübergreifenden Fähigkeiten, durch: „*P*rogramme for *I*nternational *S*tudent *A*ssessment - Schülerleistungen im internationalen Vergleich“.

Den deutschen Teil der Schulleistungsuntersuchung betreut im Auftrag der Kultusministerkonferenz ein von Universitätsprofessoren und Forschungsinstituten gebildetes Konsortium unter Federführung des Max-Planck-Instituts für Bildungsforschung in Berlin (MPIB).
Sachsen gehört zu den für eine repräsentative Auswahl ausgesuchten Bundesländern. Zunächst wird, und zwar von Mitte April bis Mitte Mai 1999, ein sog. Feldtest durchgeführt, an dem aus Sachsen zwei Gymnasien und drei Mittelschulen beteiligt sind, pro Schule 35 Schüler der Altersstufe 15 Jahre. Schüler und Eltern (genauer

gesagt: Erziehungsberechtigte) nehmen freiwillig teil; nach einer schriftlichen Belehrung füllen sie die Bögen mit den Testaufgaben bzw. ergänzende Fragebögen aus. Die Lehrer erfahren die Leistungen ihrer Schüler nicht.
Im Mai 2000 soll dann die Haupterhebung folgen.

Trotz der hochkarätigen Autorenschaft (die Testaufgaben sind Ergebnis internationaler Zusammenarbeit) gab es einige Schwierigkeiten: Das MPIB hat den Kultusverwaltungen viel zu spät die Unterlagen für den Feldtest zur Verfügung gestellt, so dass die Datenschutzbeauftragten der beteiligten Länder nur noch jeder einzeln kurzfristig zu den Unterlagen Stellung nehmen konnten. Angesichts der Kürze der Zeit und der Unklarheiten über den Inhalt der jeweils vorliegenden Texte des MPIB haben sich die Stellungnahmen der Landesdatenschutzbeauftragten nur schlecht koordinieren lassen.

Trotz der improvisierten Verfahrensweise haben sich hoffentlich doch die nötigen Verbesserungen im Wesentlichen erreichen lassen. Vor allem konnte im Wege umfangreicher Textänderungen dafür gesorgt werden, dass die Schüler und Eltern nun vollständig darüber aufgeklärt werden, zu welchen Themen sie neben den Testaufgaben befragt werden (z. B. auch zum Verhältnis zwischen Kindern und Eltern), und auch darüber, dass die Teilnahme wirklich freiwillig ist. Irreführende Behauptungen über eine vollständige Anonymität der Studie unterbleiben nunmehr. Ferner sind wesentlich verbesserte Vorkehrungen zu Erhöhung des Anonymisierungsgrades getroffen worden, insbesondere wurde auf die Erhebung des Geburtstages der Schüler verzichtet.

Innerhalb dieser Rahmenbedingungen war die Zusammenarbeit mit dem SMK so gut, wie man sie sich nur wünschen konnte.

Vgl. auch oben 1, 5.1.10 und 5.1.17.

14 Technischer und organisatorischer Datenschutz

14.1 Telemedizin

Die Medizin ist einer der Bereiche, in denen zurzeit die Anwendung neuer Informationstechnologien am stärksten fortschreitet. Unterstützung bei der Diagnostik, schneller Informationsaustausch zwischen medizinischen Einrichtungen, digitale Bildbearbeitung, Führung einer elekronischen Patientenakte - all dies spielt auch in einem sächsischen Projekt eine Rolle.

In Zusammenarbeit mit mehreren Krankenhäusern hat das SMS ein Modellprogramm zur „Digitalisierung bildgebender Verfahren und Bildkommunikation der Krankenhäuser im Freistaat Sachsen“ initiiert.
Dabei soll der Aufbau einer funktionierenden Bildkommunikation nicht nur in den einzelnen Einrichtungen, sondern auch darüber hinaus - mit anderen Einrichtungen und mit niedergelassenen Ärzten - getestet werden. Aspekte sind dabei die Erprobung

von Hard- und Software u. a. zur internen und externen Vernetzung bzw. Bildkommunikation, zur Nutzung digitaler Archivierung, zur Befundung, die Erstellung und Anwendung von Standards für die digitale Bildübertragung, sowie die Einbeziehung der Aufnahmeplätze und Funktionsstellen in die digitale Bildkommunikation und Archivierung.

Im Rahmen des gesamten Modellprogramms wurden acht regionale Modellprojekte mit jeweils spezifischen Anwendungsschwerpunkten ins Leben gerufen**.** Jedem Projekt gehören mehrere Kooperationspartner an: Krankenhäuser, Universitätskliniken und niedergelassene Ärzte. Die Realisierung der einzelnen Modellprojekte wird jeweils einem Generalunternehmer übertragen. An der Erstellung der dafür notwendigen Ausschreibungsunterlagen habe ich mich beteiligt und unter Rückgriff auf die Arbeit des Arbeitskreises Technik die Aufnahme der sechs Grundziele des technisch-organisatorischen Datenschutzes (siehe unten 14.6) empfohlen. Im Einzelnen habe ich die Erfüllung folgender Forderungen vorgeschlagen:
- Eindeutigkeit der Autorenschaft und des Empfängers
- Digitale Signatur, Zertifizierungsstelle
- kryptographische Verfahren (insbesondere bei besonderen Gefährdungen, z. B. mobilen Systemkomponenten, Datenträgertransport und Datenübermittlung)
- Vermeidung unbefugter Nutzung und Veränderung von Daten und Datenträgern
- Möglichkeiten zur Korrektur und Sperrung von Daten
- Aktualisierung von Daten
- Schutz vor zufälliger Veränderung oder Verlust von Daten (auch bei Archivierung)
- Aufrechterhaltung der Systemintegrität
- Protokollierung von Eingaben und Zugriffen
- Zugangs- und Zugriffsregelungen
- Regeln zur Systemadministration
- Regeln zur Wartung und Fernwartung
- Sicherung des Datenschutzes bei Auftragsdatenverarbeitung
- Datenschutz bei Testverfahren (Testdaten, Freigabe)

Die Anbieter sind aufgefordert, sowohl ihre grundsätzliche Konzeption als auch die Einzelmaßnahmen darzustellen. Nach dem Zuschlag ist auf dieser Grundlage ein Sicherheitskonzept zu erstellen. Ich werde dies und die einzelnen Modellprojekte weiter begleiten.

14.2 Gemeinsames Verzeichnis auf einem Server

Zur Bekanntgabe allgemeiner und nicht vertraulicher Informationen hat eine Stadtverwaltung ein Verzeichnis „Post“ auf dem Server eingerichtet. Für dieses Verzeichnis besitzen alle Beschäftigten Lese-, Schreib- und Löschrechte. Jeder Beschäftigte der Stadtverwaltung kann durch Kopieren oder Verschieben seiner Dateien in dieses Verzeichnis allen Beschäftigten allgemein interessierende Informationen zur Verfügung stellen.

Nunmehr soll dieses Verzeichnis auch zur elektronischen Übermittlung personenbezogener Daten benutzt werden können. Dazu sollen die Dateien „passwortgeschützt“

(so die getroffene Regelung) in das Verzeichnis gestellt werden. Dahinter steht die Möglichkeit, bei Standardsoftware zum Schutz von Dateien oder Dokumenten beim Speichern ein Passwort vergeben zu können. Leider ist dieser Passwortschutz unzureichend. Im Internet existieren mittlerweile Crackprogramme, mit denen dieser Schutz mühelos geknackt werden kann. Darüber hinaus erfolgt weder eine Protokollierung etwaiger Fehlversuche noch ist durch die notwendige Bekanntgabe des Kennwortes an den Kreis der berechtigten Nutzer ein ausreichender Schutz gegeben. Meist wird das einmal verwendete Kennwort auch für andere Dokumente genutzt, obwohl diese nur einem anderen Nutzerkreis zugänglich sein sollen. Eine solche Verfahrensweise ist für die Übermittlung personenbezogener Daten ungeeignet.

Besser wäre beispielsweise die Einrichtung spezieller „Übermittlungs"-Verzeichnisse auf dem Server der Stadtverwaltung. Bei Verwendung eines geeigneten Betriebssystems werden dann nur für die Beschäftigten Zugriffsrechte vergeben, die die entsprechenden personenbezogenen Daten verarbeiten dürfen. Ein unbefugter Zugriff anderer Beschäftigter auf diese Verzeichnisse würde abgewiesen und bei entsprechender Protokolleinstellung vom Betriebssystem protokolliert. Bei regelmäßiger Auswertung der Systemprotokolle könnte bereits der Versuch des Zugriffes festgestellt werden.

14.3 Dateien- und Geräteverzeichnis nach § 10 SächsDSG

Bei unangemeldeten datenschutzrechtlichen Kontrollen habe ich mehrfach festgestellt, dass die gemäß § 10 SächsDSG bestehende Verpflichtung der öffentlichen Stellen des Freistaates Sachsen, der Gemeinden und Landkreise sowie der sonstigen der Aufsicht des Freistaates Sachsen unterstehenden juristischen Personen des öffentlichen Rechts, ein Dateien- und Geräteverzeichnis zu führen, nicht erfüllt oder nicht so genau genommen wird. Auch die mir im Zusammenhang mit automatisierten Verfahren der Personaldatenverarbeitung zugesandten Dateien- und Geräteverzeichnisse weisen vielfach datenschutzrechtliche Defizite auf. Oft werden automatisierte Dateien mit personenbezogenen Daten gespeichert, deren Erforderlichkeit (§ 31 Abs. 1 SächsDSG) nicht festzustellen ist.

Im Folgenden sei nochmals auf einige Schwerpunkte hingewiesen:
Die Vorschrift des Sächsischen Datenschutzgesetzes enthält die Verpflichtung, *alle* automatisierten Dateien, in denen personenbezogene Daten gespeichert sind, und die hierzu eingesetzten Anlagen schriftlich zu verzeichnen. Die Dateibeschreibungen sind für automatisierte und für nicht automatisierte (manuelle) Dateien zu führen. Für die Erarbeitung des Verzeichnisses verweise ich nochmals nachdrücklich auf das in der Anlage zu meiner Bekanntmachung (siehe SächABl. 1993, S. 1175) abgedruckte Muster.

Das Dateien- und Geräteverzeichnis dient der internen Kontrolle durch den Dienststellenleiter und die Dienst- und Fachaufsichtsbehörde. Es ist unentbehrliches Hilfsmittel zur Erfüllung der Auskunftspflicht (§ 17 SächsDSG) seitens der Behörde als speichernde Stelle. Eingeschlossen ist auch die Art der automatisierten Auswertung der Daten des Beschäftigten (§ 31 Abs. 3 SächsDSG). Dem Sächsischen

Dastenschutzbeauftragten ist es für seine Kontrollen auf Verlangen vorzulegen (§ 28 Abs. 1 SächsDSG).

Mit der Bezeichnung der Datei nach § 10 Abs. 1 Nr. 1 SächsDSG ist nicht nur das Verfahren, sondern auch die *Zweckbestimmung* exakt festzuhalten. Denn danach lässt sich prüfen, ob das eingesetzte Verfahren gesetzlich zulässig und zur Aufgabenerfüllung *erforderlich* ist. Das bedeutet, dass die öffentliche Stelle *ohne* die Daten im konkreten Einzelfall ihre Aufgabe nicht, nicht vollständig oder nicht in rechtmäßiger Weise erfüllen kann. Es genügt demnach nicht, dass die Daten zur Aufgabenerfüllung „geeignet" und „zweckmäßig" sind; vielmehr sind Geeignetheit und Zweckmäßigkeit weitere Voraussetzungen für die Erforderlichkeit. Es reicht auch nicht aus, dass mit der automatisierten Datei die Aufgaben der öffentlichen Stelle „vereinfacht" und „beschleunigt" werden. Vielmehr muss es der Behörde unmöglich sein, ihre Aufgaben ohne Kenntnis der Daten ordnungsgemäß zu erfüllen (vgl. im Übrigen Simitis/ Dammann/Geiger/Mallmann/Walz, § 13 Rdnr. 23).
Die Zweckbestimmung ist auch erforderlich im Rahmen der Auskunftspflicht der Behörde gegenüber dem Betroffenen, die sich gemäß § 17 Abs. 1 Nr. 2 SächsDSG auch auf den *Zweck der Speicherung* erstreckt. Als Bezeichnung der Datei ist ein möglichst „sprechender" Begriff zu wählen, der bei automatisierten Dateien nicht mit dem systeminternen Dateinamen übereinstimmen muss.

Genauso sorgfältig sind die Aufgaben nach Abs. 1 Nr. 2 zu beschreiben, für die die Datei benötigt wird. Als Rechtsgrundlage ist die Textstelle (Paragraph, Absatz, Nummer) der einschlägigen Rechtsvorschrift (Gesetz, Rechtsverordnung, Satzung) sowie die Fundstelle (z. B. BGBl. I, SächsGVBl. S. ...) aufzuführen.

Wichtig ist auch, dass die nach Abs. 1 Nrn. 6 bis 9 erforderlichen Angaben genau bezeichnet werden. Insbesondere Angaben über personelle, technische und organisatorische Maßnahmen (vgl. § 9 SächsDSG), die in einem angemessenen Verhältnis zum Schutzzweck stehen sollen, wobei die Art der zu schützenden Daten zu berücksichtigen ist.

Bei meinen Kontrollen werde ich auch die Aktualität der Dateien- und Geräteverzeichnisse prüfen.

14.4 Mobi-Finder

Ende 1997 wurden im Zusammenhang mit dem Entwurf eines Begleitgesetzes zum Telekommunikationsgesetz sogenannte IMSI-Catcher erwähnt - Geräte, mit denen Verbindungs- und Inhaltsdaten bei Mobilfunkkommunikation schnell und örtlich flexibel erfasst werden können. Diese sollten von den Strafverfolgungsbehörden bei der Beobachtung des Mobilfunkverkehrs eingesetzt werden können. Mittlerweile hat die gleiche Herstellerfirma ein neues Gerät auf den Markt gebracht, den sogenannten Mobi-Finder.

Der zunehmende Einsatz moderner Kommunikationsmittel wirft immer mehr die Frage nach der Datensicherheit und der Vertraulichkeit von Gesprächen auf. Mobil-

funktelefone können die Sicherheit gefährden, indem sie in bestimmten Situationen andere lebenswichtige elektronische Einrichtungen in ihrer Funktion beeinträchtigen. Dies ist vor allem der Fall in Flugzeugen und auf Flughäfen, in der Nähe von Kraftstoffdepots und Tankstellen, neben Chemiewerken, bei Sprengarbeiten, in medizinischen Messbereichen (z. B. Computertomografie, Intensivstationen) sowie in Kernkraftwerken. Vor allem in Sicherheitsbereichen ist deshalb die Benutzung von Mobilfunkgeräten untersagt.

Nutzer von Mobilfunktelefonen können allerdings auch bewusst Sicherheitsmaßnahmen unterlaufen. Die Vertraulichkeit von persönlichen Gesprächen kann dadurch preisgegeben werden, wenn mit Absicht ein Handy eingeschaltet ist. Mobilfunktelefone können in Verbindung mit einem Modem komplette Datenbestände aus einem eigentlich gesicherten Bereich weltweit verschicken. Dabei können sie intern so beschaltet werden, dass sie keine Anzeige ihres Dauersendebetriebes am Display erkennen lassen. Auch in Gefängnissen steht das Aufsichtspersonal zunehmend vor dem Problem, unerlaubte Kommunikation über Mobilfunkgeräte zu unterbinden.

Für diese Fälle wurde nach Angaben des Herstellers der „Mobifinder“ entwickelt. Er ist ein Detektor, der sofort erkennt und aufzeichnet, wenn in einem näheren Umkreis ein Mobilfunktelefon in den Sendezustand übergeht.

Er signalisiert wahlweise akustisch mit einem Signal, optisch über eine blinkende LED oder „still“ mit Vibrationen und speichert die Daten für die spätere Auswertung.

Ich habe den Mobifinder in einem belebten Bereich einer öffentlichen Stelle auf seine Verwendbarkeit getestet. Er erfüllt seinen Zweck, wobei allerdings die Entfernung zum Mobilfunktelefon nicht sehr groß sein darf. Unterschiede waren in den verschiedenen Netzfrequenzen erkennbar. So erforderte das E-Netz eine größere Nähe beim erfolgreichen Nachweis eines sendenden Telefons. Zur genauen Lokalisation steht allerdings nur ein Gradientenanzeiger zur Verfügung - dies dürfte das genaue Auffinden eines Mobilfunktelefons in der Praxis erschweren. Fehlalarme durch Bündelfunkgeräte wurden nicht festgestellt.

Zusammenfassend kann festgestellt werden, dass der Mobifinder von seiner Wirkungsweise her kein „abgerüsteter“ IMSI-Catcher ist. In übersichtlichen Bereichen ist er sinnvoll anwendbar; in größeren und unübersichtlichen Arealen ist jedoch ein gezieltes Auffinden von Mobilfunktelefonen schwierig. Seine Anwendung ist aufgrund seiner anonymen Messwerterfassung und -darstellung für mich kein datenschutzrelevantes Problem. Derzeit steht der Einsatz des Mobifinders in sächsischen Behörden nicht zur Debatte.

14.5 Datenschutz und -sicherheit bei Öffentlichkeitsfahndungen im Internet[1]

In Beantwortung der Anfrage des Arbeitskreises Justiz zur öffentlichen Fahndung im Internet ist Folgendes festzustellen:

zu 1:
Gewährleistung der Authentizität und der Integrität der Informationen auf dem Webserver der Polizei (Homepage)

a) Durch welche technischen Maßnahmen lässt sich sicherstellen, dass unberechtigte Veränderungen an den Fahndungsaufrufen der Polizei ausgeschlossen sind?

Um den unbefugten schreibenden Zugriff auf die Fahndungsaufrufe auf dem Webserver der Polizei selbst zu verhindern, kommen verschiedene Zugriffsschutzmechanismen in Betracht. Dazu gehören insbesondere Firewalls auf der Netzebene sowie der Zugriffsschutz und regelmäßige automatisierte Datenintegritätsprüfungen auf der Betriebssystemebene. Erforderlich ist in jedem Falle eine sichere Konfiguration aller Komponenten und des Gesamtsystems.

Durch kryptographische Verfahren wie z. B. digitale Signaturen ist es möglich, unbefugte Änderungen sowohl der einstellenden Dienststelle als auch Dritten erkennbar zu machen. Dritte sind dazu allerdings auf eine Infrastruktur angewiesen, die derzeit noch nicht gegeben ist. Darüber hinaus ist bei HTML-Seiten nicht deutlich darzustellen, zu welchem Bereich einer Seite eine entsprechende Signatur gehört.

b) Ist eine Einschränkung der Kopierbarkeit der zur Verfügung gestellten Informationen möglich?

Bislang ist die Kopierbarkeit der Informationen technisch nicht einschränkbar. Jede HTML-Seite kann mitsamt der enthaltenen Grafiken an eine beliebige andere Stelle im Internet kopiert werden. Einmal ins WWW eingestellte Informationen können sich verselbständigen, ohne dass der Ersteller der Informationen dies bemerken muss. Der ursprüngliche Informationsersteller kann nicht mit Sicherheit herausfinden, wo überall unautorisierte Kopien der Informationen zu finden sind.

c) Falls ja, welche Folgen hätten ggf. solche Einschränkungen auf den Nutzen einer Internetfahndung?

Entfällt, da solche Einschränkungen nicht möglich sind.

zu 2:
Gewährleistung der Authentizität und Integrität der abgerufenen Informationen

a) Ist es möglich, dass ein Dritter Fahndungsinformationen, die er abgerufen hat und später veröffentlichen will, hierfür die Internetadresse der Polizei vortäuscht?

Die einfachste Methode ist, dass ein offiziell klingender Domainname (z. B. www.bremen.lka.de, www.bremen-lka.de, www.bremen.einseinsnull.de oder www.lka-bremen.de, um nur einige mögliche zu nennen, der Phantasie sind hier wenig Grenzen gesetzt) von einer Nicht-Polizeistelle reserviert wird und unter dieser Domain kopierte, manipulierte oder gänzlich falsche Fahndungsaufrufe veröffentlicht werden. Dies gelingt jedoch nur, soweit diese Domainnamen nicht durch die Polizei bereits vorsorglich reserviert wurden.

Darüber hinaus gibt es eine Reihe von technischen Möglichkeiten vorzutäuschen, dass Daten von einem Polizei-Server stammen (z. B. durch Manipulation einer bestehenden Internetkommunikation, von Domain Name Servern (DNS), Dienstleistungsprogrammen (sog. Proxies) und lokalen Zwischenspeichern (sog. Caches)).

b) Lassen sich Manipulationen an abgerufenen Bildern erkennbar machen?

Prinzipiell lassen sich Bilder digital signieren oder auch mit einem elektronischen Wasserzeichen markieren. Die Signatur stellt sicher, dass das übertragene Bild Bit für Bit mit dem Original übereinstimmt. Jede Manipulation - auch Konvertierung in andere Formate - kann daher entdeckt werden. Um das Verfahren sinnvoll anwenden zu können, müsste beim Benutzer die entsprechende Infrastruktur zur Verfügung stehen, damit beim Aufruf signierter Informationen möglichst automatisch die entsprechende Überprüfung erfolgen kann.

Digitale Wasserzeichen überstehen zwar auch Konvertierungen und kleine Veränderungen. Sie überstehen in der Regel jedoch nicht das Einscannen eines (auch mit einem hochwertigen Drucker) gedruckten Bildes. Auf diesem Weg lassen sich also digitale Wasserzeichen auch wieder aus Bildern entfernen. Da digitale Wasserzeichen aber eher dazu dienen, die Herkunft eines (unzulässig) kopierten Bildes zu ermitteln, müssten die Polizeibehörden die von ihnen ins Internet eingestellten Bilder immer mit einem digitalen Wasserzeichen versehen, um derart Falsifikate erkennen zu können. Sie sind also für den angestrebten Zweck, Echtheitsprüfung durch den Internet-Benutzer, weniger geeignet.

c) Wären die Angaben eines Gültigkeitszeitraumes oder Maßnahmen nach dem Signaturgesetz wie z. B. eine digitale Signatur oder ein digitales Wasserzeichen geeignete Mittel, Manipulationen erkennbar zu machen? Lässt sich dies an Beispielen plastisch darstellen?

Digitale Signaturen gehören inzwischen zum Stand der Technik. Wie unter 2 b) ausgeführt, sind sie technisch für den angegebenen Zweck geeignet. Digitale Signaturen können auch eine zeitliche Beschränkung beinhalten. Bei einer Überprüfung der Signatur könnte zwar vom Internetnutzer - sofern er Zugriff auf den entsprechenden öffentlichen Schlüssel hat - festgestellt werden, dass die Gültigkeit bereits abgelaufen ist, an der Verbreitung des Bildes würde dies aber nichts ändern. Des Weiteren ist es jederzeit möglich, die Ursprungssignatur entweder ganz wegzulassen oder durch eine neue zu ersetzen.

Zusammenfassung:

Grundsätzlich muss berücksichtigt werden, dass die in das WWW eingestellte Information zum Zwecke der Verbreitung dort eingestellt wird und per se nicht rückholbar ist. Der originale Fahndungsaufruf auf dem WWW-Server der Polizei lässt sich zwar durch die Polizei wieder löschen, aber auf mögliche Kopien dieses Fahndungsaufrufs auf anderen Servern im Internet hat das keine Auswirkungen.

Die WWW-Server der Polizei und die darauf präsentierte Information können durch konsequente Anwendung dem Stand der Technik entsprechender Zugriffsschutzmechanismen und Sicherheitsinfrastrukturen gegen unbefugte Manipulation geschützt werden.

Zusätzliche und höhere Sicherheit - auch für die verbreitete Information - können kryptographische Verfahren (digitale Signatur, digitale Wasserzeichen, Zertifikate für Server) bieten, die aber nur wirken können, wenn ausreichend starke Verschlüsselungsalgorithmen verwendet werden, eine entsprechende Infrastruktur bereit steht und diese Verfahren konsequent angewendet werden - auch durch den Internet-Benutzer. Diese Infrastruktur ist derzeit jedoch noch nicht gegeben.

Aber auch Zertifikate für Server schützen kaum vor der Verwendung offiziell erscheinender Domainnamen, da auch für diese Server Zertifikate zu erhalten sind. Server-Zertifikate bestätigen nur, dass sich der Internet-Benutzer auf dem Server befindet, auf den er auch zugreifen wollte. Sie geben aber nicht unbedingt erschöpfend Auskunft darüber, welche Institution hinter einem solchen Server steht.

Abschließend sei darauf hingewiesen, dass für die Personen, die auf Daten im WWW zugreifen, damit rechnen müssen, identifiziert zu werden, sofern dies nicht durch zusätzliche technische oder organisatorische Maßnahmen verhindert wird. Es ist daher zu prüfen, ob eine solche Identifikation zulässig ist. Falls nicht, so muss die Möglichkeit zur Identifikation technisch und organisatorisch ausgeschlossen werden. Insbesondere dürfen dann keine adressbezogenen Zugriffsprotokolle erstellt, Cookies verwendet oder durch andere Verfahren identifizierende Daten gewonnen werden.

Insgesamt ergibt sich, dass Fahndungsaufrufe der Polizei im Internet nicht sicherer sind als jede andere dort publizierte Information. Deshalb sollten zumindest die verfügbaren Datenschutz- und Datensicherheitsmaßnahmen vorgesehen werden. Ob die dann noch verbleibenden Restrisiken akzeptiert werden können, bleibt einer rechtlichen Bewertung vorbehalten.

14.6 Vereinheitlichung der Technikregelungen in den Datenschutzgesetzen[2]

1. Regelungsziele für technische und organisatorische Maßnahmen zur Datensicherheit im künftigen Datenschutzrecht

Wie die Analyse der Erfahrungsberichte der Mitglieder des AK-Technik ergeben hat, sollten die bisherigen „10 Gebote“ ersetzt werden durch allgemeine - auch für konventionelle Verarbeitungsprozesse geltende - technikunabhängige Anforderungen. Die entsprechende Vorschrift sollte inhaltlich die folgenden Punkte aufweisen:

(1) Die Ausführung der Vorschriften der Datenschutzgesetze sowie anderer Vorschriften über den Datenschutz ist durch technische und organisatorische Maßnahmen sicherzustellen.

(2) Es sind die technischen und organisatorischen Maßnahmen zu treffen, die nach dem Stand der Technik und nach der in einer Risikoanalyse festgestellten Schutzbedürftigkeit geeignet, erforderlich und angemessen sind. Die datenverarbeitenden Stellen haben die Verantwortlichkeiten und Berechtigungen zur Verarbeitung personenbezogener Daten so festzulegen, dass sie den besonderen Anforderungen des Datenschutzes gerecht werden. Sie haben die ordnungsgemäße Verarbeitung zu überwachen.

(3) Dabei ist insbesondere zu gewährleisten,
- dass nur Befugte personenbezogene Daten zur Kenntnis nehmen können (*Vertraulichkeit*),
- dass personenbezogene Daten während der Verarbeitung unverfälscht, vollständig und widerspruchsfrei bleiben (*Integrität*),
- dass personenbezogene Daten zeitgerecht zur Verfügung stehen und ordnungsgemäß verarbeitet werden können (*Verfügbarkeit*),
- dass jederzeit personenbezogene Daten ihrem Ursprung zugeordnet werden können (*Authentizität*),
- dass festgestellt werden kann, wer wann welche personenbezogene Daten in welcher Weise verarbeitet hat (*Revisionsfähigkeit*),
- dass die Verfahrensweisen bei der Verarbeitung personenbezogener Daten vollständig, aktuell und in einer Weise dokumentiert sind, dass sie in zumutbarer Zeit nachvollzogen werden können (*Transparenz*).

Begründung zu Abschnitt 1:

Die Regelungen zu den technischen und organisatorischen Maßnahmen in den Datenschutzgesetzen stammen aus den 70er Jahren und orientieren sich an der damaligen Technik und Datenverarbeitungsstruktur. Diese Zeit war bestimmt von zentral organisierten Rechenzentren, Telekommunikation und Vernetzungen spielten nur eine untergeordnete Rolle. Die Datensicherheitsüberlegungen waren deshalb geprägt von der Vorstellung einer monolithischen Großrechnerwelt und primär verbunden mit dem Schutz der Rechner, die in hermetisch abgeschlossenen Rechenzentren betrieben wurden. In einer Zeit, in der Datenverarbeitung zunehmend dezentral in weltumspannenden Rechnernetzen betrieben wird, sind solche Regelungen nur noch bedingt oder gar nicht mehr wirksam. Die nachfolgenden Beispiele sollen dies verdeutlichen:

- *Zugangskontrolle*: Unbefugten soll mit dieser Maßnahme der physische Zugang zu Räumen verwehrt werden, in denen sich Datenverarbeitungsanlagen befinden. Heute stehen Rechner aber nicht mehr ausschließlich in besonders gesicherten Räumen eines Rechenzentrums, sondern jede Mitarbeiterin und jeder Mitarbeiter hat einen Personalcomputer auf dem Schreibtisch. Zugangskontrollen der herkömmlichen Art sind damit nicht mehr praktikabel bzw. nicht mehr ausreichend.

- *Datenträgerkontrolle*: Die Datenträgerkontrolle konnte in Zeiten der Großrechner durch die Einrichtung von zentralen Datenträgerarchiven realisiert werden. Heute müssen jedoch Datenträger für eine große Zahl von Nutzerinnen und Nutzern dezentral verfügbar sein. Außerdem sind die verschiedenen Formen der Daten-

träger weitaus vielfältiger geworden (wie z. B. Festplatten, Disketten, CD-ROMs, Bildplatten, Chipkarten, Bänder usw.). Das Ziel der Regelung, ein unbefugtes Auswerten, Verändern und Entfernen der Daten auf Datenträgern zu verhindern, ist auf dem Wege der konventionellen Daten*träger*kontrolle nicht mehr erreichbar.

- *Speicherkontrolle*: Die unbefugte Eingabe von Daten sowie deren Kenntnisnahme, Veränderung und Löschung ist nicht mehr nur über die Konsole im Rechenzentrum möglich und beschränkt sich nicht mehr nur auf Speichermedien als Träger von Daten, sondern ist in einer vernetzten DV-Landschaft von jedem Endgerät aus möglich unter Einbeziehung der verbindenden lokalen Netzwerke (LAN) bzw. der Weitverkehrsnetze (WAN) selbst. Die bisherige Regelung bleibt daher weitgehend wirkungslos.

- *Benutzerkontrolle*: Die Benutzung eines Datenverarbeitungssystems mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte soll hierdurch verhindert werden. Die Nutzung von Mechanismen zur Datenfernübertragung sind heute keine Besonderheit mehr, sondern der Regelfall. Insofern bedarf es keiner Regelung, die dies besonders hervorhebt. Allgemein muss sichergestellt werden, dass die Benutzer eines Datenverarbeitungssystems nur im Rahmen ihrer Berechtigungen personenbezogene Daten verarbeiten können, mit welchen technischen Einrichtungen ist dabei ohne Belang.

- *Zugriffskontrolle*: Die Zugriffskontrolle soll sicherstellen, dass Benutzer ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können. Damit beinhaltet die Zugriffskontrolle die Benutzerkontrolle. Die Benutzerkontrolle ist eine redundante Regelung.

- *Übermittlungs- und Eingabekontrolle*: Mit der Übermittlungskontrolle und der Eingabekontrolle werden zwei Maßnahmen definiert, die beide auf die Revisionsfähigkeit abzielen. Beide Maßnahmen greifen aber zu kurz, da sie nur die Verarbeitungsschritte Eingabe und Übermittlung erfassen. Alle übrigen Phasen der Datenverarbeitung werden nicht berücksichtigt und wären so einer Revision nicht zugänglich.

Die derzeit geltenden Regelungen definieren Sicherheits*maßnahmen* und haben im Wesentlichen die *technischen Komponenten* von Datenverarbeitungsanlagen zum Gegenstand. Dadurch sind sie stark technologieabhängig und müssten ständig neueren Entwicklungen angepasst werden. Sicherheitsmaßnahmen sind individueller Natur und abhängig von dem Schutzbedarf der zu verarbeitenden Daten, der konkreten Bedrohungslage, dem Stand der Technik, der Architektur der zu betrachtenden DV-Systeme und den Verfahren, die auf diesen Systemen zum Ablauf gebracht werden sollen. Die Festlegung der Maßnahmen, die zur Sicherung eines konkreten Systems erforderlich sind, ist erst das Ergebnis einer individuellen Sicherheitsanalyse auf der Grundlage eines Sicherheitskonzepts und lässt sich nicht in einer gesetzlichen Regelung abschließend definieren.

Nicht zuletzt bedingt durch die rasante Entwicklung der Informationstechnologie vollzieht sich ein Paradigmenwechsel im Datenschutz. Die bisherige primäre Ausrichtung des Schutzes der bei der Datenverarbeitung eingesetzten technischen Komponenten ist heute nicht mehr durchhaltbar, da nicht mehr eine zentral ausgerichtete Datenverarbeitung im Vordergrund steht, sondern dezentralisierte und verteilte Strukturen vernetzter multimedialer Systeme. Heute schwirren die Daten über Datenautobahnen und es existieren vielfältige Möglichkeiten auf diese Datenautobahnen zu gelangen, um an der globalen elektronischen Kommunikation teilzunehmen. Die möglichen Formen der Datenverarbeitung von morgen sind nicht absehbar. Die Innovationszyklen in der Informationstechnologie werden immer kürzer, Entwicklungen immer dynamischer und die Technik immer komplexer.

Damit erhält der Datenschutz eine neue Qualität. Datenschutz ist nicht nur an technischen Anlagen festzumachen, sondern auch - im eigentlichen Sinne des Wortes - an den Daten selbst. Attribute wie vertraulich, integer und authentisch sind als Eigenschaften der Daten anzusehen, die unabhängig vom aktuellen Aufenthaltsort der Daten, der Art und dem Stadium ihrer Verarbeitung und den technischen Verarbeitungskomponenten gesichert werden müssen.

Daraus resultiert, dass für die Formulierung neuer Regelungen methodisch ein anderer Ansatz zu wählen ist. Es werden nicht mehr an der Technik orientierte Sicherheits*maßnahmen*, sondern auf einem abstrakteren Niveau primär an den Daten ausgerichtete Sicherheits*ziele* definiert.

Damit wird Folgendes erreicht:

- Die verwendeten Begrifflichkeiten entsprechen denen, die in der einschlägigen Sicherheitsliteratur verwendet werden. Auch die EU-Datenschutzrichtlinie bedient sich dieser Begriffe.

- Datenschutzkontrollinstanzen und die am Sicherheitsprozess beteiligten Akteure (Entwicklungsingenieure, Softwarespezialisten, Sicherheitsexperten, Systembetreiber, Revisoren) sprechen die „gleiche“ Sprache.

- Die Sicherheitsziele sind technologieunabhängig und bilden einen allgemein gültigen Sicherheitsrahmen, der umfassend ist und auch bei neuen Formen der Datenverarbeitung Bestand haben wird. Die genannten Ziele haben sich in Forschung und Praxis als stabil erwiesen.

- Das „Füllen“ des Sicherheitsrahmens mit konkreten Maßnahmen erfolgt auf der Grundlage von Risikoanalysen. Hierzu können die gängigen Methoden (z. B. die des Bundesamtes für Sicherheit in der Informationstechnik) verwendet werden, da die definierten Sicherheitsziele mit diesen konform sind.

- Die Ziele definieren eine „Messlatte“, an der die Sicherheit eines DV-Systems abgelesen werden kann.

- Die vorgeschlagenen Regelungen führen zu mehr Rechtssicherheit, da sie Anforderungen definieren, die im Bereich der IT-Sicherheit „verstanden“ werden, in der Praxis anwendbar sind, für jede Form der Datenverarbeitung und jede technische Architektur Gültigkeit haben und einer methodischen Vorgehensweise bei ihrer Umsetzung zugänglich sind.

- Die Regelungen stellen die Kontrollierbarkeit der DV-Systeme sicher, da die zu treffenden Sicherheitsmaßnahmen im Sicherheitskonzept dokumentiert sind und damit überprüfbar werden.

Da sich in der Praxis erwiesen hat, dass vor allem aufgrund von nicht ausreichender Dokumentation die Verfahren oft weder von den mit der Datenverarbeitung befassten Personen noch von den Kontrolleuren ausreichend nachvollzogen und damit auch den Betroffenen nicht verständlich gemacht werden können, wird der Begriff der „Transparenz“ als neue Anforderung eingeführt.

Ein häufiger Mangel, der bei Kontrollen festgestellt wird, ist die unzureichende nachträgliche Feststellbarkeit einzelner Datenverarbeitungsvorgänge insbesondere mangels ausreichender Protokollierung. Dieser Missstand führt häufig dazu, dass Ursachen und Verantwortliche nicht ermittelt werden konnten. Um dem entgegenzuwirken, wird die Forderung nach „Revisionsfähigkeit“ erhoben.

2. Besondere Maßnahmen zur Datensicherheit beim Einsatz automatisierter Verfahren

Die Anforderungen nach Abschnitt I sollten speziell für *automatisierte Verfahren* gesetzlich, gegebenenfalls auf Verordnungsebene wie folgt konkretisiert werden:

(1) Der Einsatz automatisierter Verfahren zur Verarbeitung personenbezogener Daten ist von vorherigen systematischen Tests und von einer Freigabe der datenverarbeitenden Stelle abhängig zu machen. Die Verarbeitung personenbezogener Daten in nicht freigegebenen Verfahren ist zu unterbinden.

(2) Das Anlegen personenbezogener Datenbestände muss einer Genehmigungspflicht durch Personen unterliegen, denen von der datenverarbeitenden Stelle hierzu die Befugnis erteilt worden ist. Für ungenehmigte Datenbestände muss eine Pflicht zur unverzüglichen Löschung bzw. Sperrung bestehen. Deshalb bedarf es einer gesetzlichen Pflicht zur Dokumentation der Datenprofile und Speicherorte.

(3) Es sind Mindestanforderungen an die Dokumentation automatisierter Verfahren festzulegen. Zur Dokumentation automatisierter Verfahren müssen Schutzkonzepte einschließlich Risikoanalysen gehören.

(4) Bei Speicherung personenbezogener Daten ausschließlich in automatisierten Dateien und bei automatisierten Datenübermittlungen müssen Protokolle vorliegen, die die Revisionsfähigkeit nach I Nr. 3 Spiegelstrich 5 sicherstellen.

(5) Bei der Verarbeitung personenbezogener Daten auf Systemen und Datenträgern, die besonderen Gefährdungen unterliegen, z. B. mobiler Einsatz, Transport von Datenträgern, Datenübermittlungen, sind geeignete kryptographische Verfahren zu verwenden.

(6) Zu Testzwecken dürfen personenbezogene Daten nicht verwendet werden.

(7) Die Datenverarbeitung soll so organisiert sein, dass bei der Verarbeitung, insbesondere der Übermittlung, der Kenntnisnahme im Rahmen der Aufgabenerfüllung und der Einsichtnahme, die Trennung der Daten nach den jeweils verfolgten Zwecken und nach unterschiedlichen Betroffenen möglich ist.

(8) Die datenverarbeitenden Stellen müssen verpflichtet werden, nur bestimmten und hinreichend qualifizierten Mitarbeitern die Genehmigung zur Systemadministration zu erteilen. Die übrigen Mitarbeiter sind durch technische und organisatorische Maßnahmen daran zu hindern, diese Funktion auszuüben. Administrationstätigkeiten sind zu protokollieren oder anderweitig zu überwachen.

(9) Automatisierte Verfahren sind so zu gestalten, dass sie eine Verarbeitung personenbezogener Daten erst ermöglichen, nachdem die Berechtigung der Benutzenden festgestellt worden ist.

(10) Automatisierte Verfahren sind technisch und organisatorisch so zu gestalten, dass Betroffene ihre Ansprüche effektiv geltend machen können.

Begründung zu Abschnitt 2:

Zu (1)
Da das Datenschutzrecht offenbar auch in Zukunft von der Maxime ausgehen wird, dass allen Datenverarbeitungsprozessen eine hinreichend bestimmte rechtliche Befugnis zugrunde liegen muss (vgl. z. B. Erwägungsgründe 10, 11 und 30 und Art. 6 und 7 der EU-Datenschutzrichtlinie), bedürfen die Verarbeitungsregeln bzw. -verfahren (die Software) ausnahmslos der Freigabe durch eine hierfür zuständige Behörde bzw. Person. Dies bedeutet im Umkehrschluss, dass der Einsatz nicht freigegebener automatisierter Verfahren durch technische und organisatorische Maßnahmen unterbunden werden muss. Die hierfür erforderliche Aufbau- und Ablauforganisation ist in der Host-Welt nach einer fast 20jährigen Entwicklungsphase „Stand der Technik". In der PC-Welt fehlen äquivalente Methoden. Gleichwohl findet in der Praxis mehr und mehr automatisiertes Verwaltungshandeln in einer systemtechnischen Umgebung statt, die für die individuelle Datenverarbeitung geschaffen worden ist. An die Stelle systematischer Tests tritt zunehmend das „Prinzip Hoffnung". Die Richtigkeit und Rechtmäßigkeit der Ergebnisse wird eher empirisch als systematisch ermittelt. Man unterstellt die Richtigkeit der Ergebnisse solange, bis das Gegenteil bewiesen wird. Dies kann insbesondere bei automatisierten Datenübermittlungen Folgen haben, die nicht rückgängig gemacht werden können.

Zu (2)
Die Anzahl der Datenbestände steigt in noch stärkerem Maße als die der Datenverarbeitungssysteme. Bei den derzeit praktizierten Organisationsformen kann jeder Benutzer de facto unbegrenzt viele Datenbestände anlegen, ohne dass die datenverarbeitende Stelle (Behördenleitung) „etwas davon merkt". Der sogenannte Infrastruktur-Ansatz bei der Hardware- und Software-Ausstattung hat dazu geführt, dass die weit überwiegende Mehrzahl der Arbeitsplätze mit einer Standard-Bürokommunikationssoftware ausgestattet ist. Die Produkte „Texteditor", „Tabellenkalkulation", „Datenbankgenerator" und „Mailing" sind bewusst so konzipiert, dass individuelle Datenbestände problemlos erzeugt, kopiert und transportiert (importiert und exportiert) werden können. Zugriffsbefugnisse werden nicht mehr durch das Behördenmanagement, sondern durch den „Eigentümer" (diejenigen, die die Datenbestände erzeugt haben) vergeben. Vielfältige Duplizierungen lassen nicht mehr erkennen, welches der Original-Datenbestand und welches eine (Teil-)Kopie ist. Damit entfällt auch die „Aktualitätsgewähr". Letztlich ist nicht mehr erkennbar, welchen Verbindlichkeitsgrad die Daten haben und ob ihnen revisionsfähige Dokumente zugrunde liegen.

Zu (3) und (4)
Eine der wesentlichen Ursachen für die immer wieder beklagte Softwarekrise liegt in der fehlenden Revisionsfähigkeit aufgrund unzureichender Dokumentationen und Protokollierungen. Die extremen Probleme im Zusammenhang mit dem „Jahr 2000" haben dies erneut deutlich gemacht. Solange in der Verwaltung alle wesentlichen Aktivitäten auf der Basis von papierenen Unterlagen und Akten nachgewiesen wurden, hat man das Problem der EDV-Dokumentation und der Protokollierung automatisierter Abläufe verdrängen können. In dem Maße, wie die personenbezogene Datenverarbeitung ausschließlich in automatisierter Form abgewickelt wird, gewinnen diese Probleme auch unter sicherheitstechnischen Aspekten an Bedeutung. Bereits heute müssten die Revisionsinstanzen (Rechnungsprüfung, interne Revision, Datenschutzbeauftragte) in weiten Bereichen ihren Prüfungsauftrag eigentlich mit der Begründung zurückgeben, dass eine Nachvollziehbarkeit zurückliegender Verarbeitungsprozesse mangels Dokumentation und Protokollierung nicht mit dem erforderlichen Maß an Genauigkeit gegeben ist. Es ist der Zeitpunkt abzusehen, zu dem die Kontrollstellenfunktion nach Art. 28 der EU-Datenschutzrichtlinie faktisch nicht mehr wahrgenommen werden kann.

Die Kontrollpraxis lehrt, dass bei der Auswahl und Implementation von Datensicherheitsmaßnahmen oft kein methodischer Ansatz gewählt wird. Technische Mittel und auch organisatorische Vorgaben werden ad hoc festgelegt. Um dieses Defizit zu beseitigen, wird die Erstellung eines Sicherheitskonzeptes vorgeschrieben. Es dient zum „Füllen" des durch die Anforderungen der genannten Datensicherheitsziele vorgegebenen Sicherheitsrahmens mit konkreten Maßnahmen. Dafür sind die Schutzbedürftigkeit der Daten zu ermitteln, eine Bedrohungsanalyse vorzunehmen und eine Risikoabschätzung durchzuführen. Die Überlegungen dazu sind in dem Sicherheitskonzept zu dokumentieren.

Zu (5)
In verschiedenen Einsatzfällen, wie bei der Datenübertragung über „unsichere“ Netze oder beim Transport von Datenträgern können personenbezogene Daten unbefugt verändert, unterdrückt oder kopiert werden, ohne dass die verantwortliche Stelle dies bemerkt. Auch beim Einsatz mobiler Technik wie Laptop-/Notebook-Computer oder auch Chipkarten sind diese Risiken vorhanden. Ferner muss bei stationär betriebenen Datenverarbeitungssystemen oft festgestellt werden, dass Geräte oder/und Datenträger infolge mangelnder Zugangssicherung gestohlen werden oder unbefugten Zugriffen ausgesetzt sind. Um diesen Risiken zu begegnen, sind kryptographische Verfahren besonders geeignet. Mit Hilfe dieser modernen Technologie können sowohl das unbefugte Nutzen von personenbezogenen Daten verhindert als auch unerlaubte Änderungen an personenbezogenen Daten erkannt werden. Im Hinblick auf die zurzeit und künftig verfügbaren Verarbeitungsgeschwindigkeiten von Prozessoren sind Performance-Probleme nicht mehr zu befürchten.

Zu (6)
Werden Echtdaten zu Testzwecken eingesetzt, bestehen Gefahren für Vertraulichkeit, Integrität und Verfügbarkeit der Daten. Da diese Risiken schwer abschätzbar sind und es in der Testphase kaum möglich ist, sinnvolle Gegenmaßnahmen gegen alle oben genannten Gefährdungen zu ergreifen, ist der Testbetrieb mit personenbezogenen Daten grundsätzlich verboten. In der Regel verstoßen solche Tests gegen die in den Datenschutzgesetzen enthaltenen Vorschriften zur Zweckbindung.

Zu (7)
Die Trennung der Daten nach Betroffenen und nach unterschiedlichen Erforderlichkeiten ist Voraussetzung, um dem Grundsatz der Zweckbindung gerecht zu werden und um die im europäischen Recht immer weiter verbreiteten allgemeinen Informationsrechte (Datenöffentlichkeit) ohne unzumutbaren Aufwand zu realisieren.

Zu (8)
Die Anzahl der Datenverarbeitungssysteme hat sich mit der Abkehr von den Host-Konzepten zu den Client-Server-Architekturen vertausendfacht. Der Trend hält an, in einigen Behörden werden bereits auf Abteilungsebene gleich mehrere Server betrieben; auch kleine und kleinste Verwaltungseinheiten organisieren ihre automatisierte Datenverarbeitung mittels vernetzter PC selbst. Damit ist die zunächst wenigen Spezialisten vorbehaltene, sicherheitstechnisch äußerst sensible Aufgabenstellung der „Systemadministration“ auf eine unübersehbare Anzahl von in der Regel nicht adäquat ausgebildeten Mitarbeitern übergegangen. Teilweise administrieren die Benutzer ihre Systeme selbst; ihr in der Regel privat erworbenes Wissen kann von der Behördenleitung mangels entsprechend ausgebildeter Vorgesetzter nicht verifiziert werden. Es sind dadurch revisionsfreie Räume entstanden.

Zu (9)
Voraussetzung zum Betrieb sicherer, datenschutzgerechter Systeme ist die Identifikation und Authentifikation von Nutzern. Ohne sie sind die Datensicherheitsziele sowie die weitergehenden Forderungen beispielsweise nach Protokollierung und Verschlüsselung nicht umsetzbar.

Zu (10)
Die Forderung ist Ausfluss des Transparenzgebotes, insbesondere der Pflicht zur Außentransparenz. Es ist das datenschutztechnische Pendant zu den in den Datenschutzgesetzen verankerten materiell-rechtlichen Ansprüchen der Betroffenen insbesondere auf Auskunft, Löschung, Sperrung und Berichtigung.

3. Regelungen für spezielle technische Systeme

Für technische Systeme, von denen - unabhängig von der Art der zu verarbeitenden personenbezogenen Daten - eine besondere Gefahr für das informationelle Selbstbestimmungsrecht ausgeht, sind spezifizierte Sicherheitsmaßnahmen normativ festzulegen. Das kommt für die nachfolgenden Systeme in Betracht:

1. Mobile Datenverarbeitungssysteme
(1) Informationstechnische Systeme zum Einsatz in automatisierten Verfahren, die an die Betroffenen ausgegeben werden, und die über eine von der ausgebenden Stelle oder Dritten bereitgestellte Schnittstelle Daten automatisiert austauschen können (mobile Datenverarbeitungssysteme), dürfen nur mit der Einwilligung der Betroffenen oder aufgrund einer Rechtsvorschrift eingesetzt werden.
(2) Es muss für die Betroffenen jederzeit erkennbar sein, ob Datenverarbeitungsvorgänge stattfinden, welche Daten dabei verarbeitet werden und welcher Verarbeitungsvorgang im Einzelnen abläuft. Auskünfte sind auf Wunsch schriftlich zu erteilen.
(3) Die Aufklärung über die Rechte der Betroffenen hat nicht erst bei dem ersten Datenverarbeitungsvorgang mit oder auf dem System, sondern bereits bei Ausgabe des Systems bzw. bei Änderung des Verfahrens zu erfolgen.
(4) Die das Verfahren betreibende Stelle ist als verantwortliche Stelle zu benennen.

Begründung zu 1:
Die vorgeschlagene Regelung zielt darauf ab, die Rechte der Betroffenen auch unter den Bedingungen des Einsatzes mobiler Datenverarbeitungssysteme zu gewährleisten. Mit dem Begriff „mobile Datenverarbeitungssysteme“ werden nach dem heutigen Stand der Technik vor allem Chipkarten erfasst. Allerdings sind schon Entwicklungen absehbar, bei denen der Chip nicht länger in Form einer Karte angewandt wird. Auch ist der Chip keine zwingende Voraussetzung für mobile Speichertechniken. Aus diesem Grund kann nicht einfach auf den Begriff Chipkarte abgestellt werden. Es ist vielmehr erforderlich, zur Regelung der Phänomene, die erfasst werden sollen, eine Legaldefinition vorzunehmen. Wesensmerkmale dieser Phänomene sind:

- Die Systeme werden von einer Stelle an die Betroffenen ausgegeben.
- Es existieren Schnittstellen, die von den ausgebenden Stellen oder von Dritten bereitgestellt werden.
- Über diese Schnittstellen können Daten automatisiert ausgetauscht werden; dazu gehört auch, dass durch den Datenaustausch Datenverarbeitungsprozesse auf den mobilen oder den stationären Systemen angestoßen werden.

Derartige Systeme bringen besondere Gefährdungen für die Rechte der Betroffenen mit sich. Ihnen ist es regelmäßig nicht möglich, selbst festzustellen, was in den

Datenverarbeitungssystemen gespeichert wird. Bereits heute existieren Anwendungen, bei denen die Betroffenen nicht bemerken können, dass ein Datenaustausch zwischen den mobilen Systemen und einer anderen Schnittstelle stattfindet (z. B. kontaktlose Chipkarten). Aufgrund dieser Gefährdungslage sind besondere Schutzvorschriften erforderlich.

Darüber hinaus ist bei mobilen Verarbeitungssystemen die mangelnde Transparenz für die Betroffenen besonders gefährlich. Daher hat die ausgebende Stelle ein Höchstmaß an Transparenz sicherzustellen. Damit haben die Betroffenen auch einen Anspruch darauf, dass ihnen die entsprechenden Auskünfte auf Wunsch in Papierform erteilt werden. Sofern zur Wahrnehmung der Auskunftsrechte besondere Geräte oder Einrichtungen erforderlich sind, hat die ausgebende Stelle dafür Sorge zu tragen, dass diese in angemessenem Umfang zur Verfügung stehen.

2. Optisch-elektronische Überwachung und Aufzeichnung

(1) Die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen zur Personenerkennung ist zulässig, soweit dies zur Aufgabenerfüllung oder zur Wahrnehmung des Hausrechts erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen Betroffener überwiegen. Die Tatsache der Beobachtung ist durch geeignete Maßnahmen erkennbar zu machen.

(2) Die Speicherung von nach Absatz 1 Satz 1 gewonnenen Daten ist zulässig, wenn dies zur Erreichung der verfolgten Zwecke unverzichtbar ist. Die Tatsache der Speicherung ist durch geeignete Maßnahmen erkennbar zu machen.

Begründung zu 2:

Der Einsatz optisch-elektronischer Überwachungs- und Aufzeichnungstechnik, etwa Videotechnik, hat auch im öffentlichen Bereich erheblich zugenommen. Soweit nicht bereichsspezifisch geregelt, fehlt es an entsprechenden Datenschutzvorschriften. Die vorgeschlagene Regelung stellt Rechtsklarheit darüber her, unter welchen Voraussetzungen optisch-elektronische Überwachungs- und Aufzeichnungstechnik zulässig ist und ggf. für welche Zwecke gespeicherte Aufnahmen genutzt werden dürfen. Insbesondere wird klargestellt, dass die betroffenen Personen ausdrücklich auf die Beobachtung und Speicherung hinzuweisen sind.

3. Wartung

(1) Wartung sind alle Maßnahmen zur Sicherstellung der Verfügbarkeit und Integrität von Datenverarbeitungssystemen.

(2) Datenverarbeitungssysteme sind grundsätzlich so zu gestalten, dass bei ihrer Wartung nicht auf personenbezogene Daten zugegriffen werden kann. Sofern dies nicht gewährleistet ist, hat die Daten verarbeitende Stelle durch technische und organisatorische Maßnahmen sicherzustellen, dass nur auf die für die Wartung unbedingt erforderlichen personenbezogenen Daten zugegriffen werden kann.

(3) Die Maßnahmen haben insbesondere folgende Anforderungen zu erfüllen:
Es ist sicherzustellen, dass
- nur dafür autorisiertes Personal die Wartung vornimmt,

- jeder Wartungsvorgang nur mit Wissen und Wollen der speichernden Stelle erfolgen kann,
- Dateien mit personenbezogenen Daten im Rahmen der Wartung nicht unbefugt entfernt oder übertragen werden,
- alle Wartungsvorgänge während der Durchführung kontrolliert und nach der Durchführung nachvollzogen werden können,
- bei der Wartung keine Programme unbefugt aufgerufen werden können, die für die Wartung nicht benötigt werden,
- bei der Wartung Datenverarbeitungsprogramme nicht unbefugt verändert werden können.

(4) Eine Wartung durch andere Stellen darf nur aufgrund schriftlicher Vereinbarungen erfolgen. Darin sind die im Rahmen der Wartung notwendigen technischen und organisatorischen Maßnahmen festzulegen. Die mit den Wartungsarbeiten betrauten Personen sind zur Wahrung des Datengeheimnisses zu verpflichten.

(5) Wenn bei der Wartung nur auf verschlüsselte, anonymisierte oder pseudonymisierte Daten zugegriffen werden kann, so dass der mit der Wartung betrauten Stelle eine Reidentifizierung von Betroffenen nicht möglich ist, so sind nur Maßnahmen nach Absatz 4 Satz 1 und 2 zu treffen. Ein Zugriff darf nur zweckgebunden erfolgen.

Begründung zu 3:
Wartung, auch die für die Vertraulichkeit und Integrität besonders risikoreiche Fernwartung über Datenfernverarbeitungseinrichtungen, wurde bisher als Datenverarbeitung im Auftrag behandelt, obwohl die dafür geltenden Merkmale nicht voll erfüllt werden. So werden bei der Wartung normalerweise keine personenbezogenen Daten benötigt, ihre Offenbarung kann jedoch im Störungsfall unvermeidbar sein. Die Nutzung personenbezogener Daten ist nicht Gegenstand des Wartungsauftrages, sondern muss im Einzelfall hingenommen werden. Aus diesem Grunde wird die Offenbarung personenbezogener Daten bei der Wartung hier neben Übermittlung und Überlassung zur Auftragsdatenverarbeitung in einer dritten Fallgestaltung behandelt.

Absatz 1 definiert den Begriff „Wartung“. Danach gehören zur Wartung auch die Installation, Pflege, Überprüfung und Korrektur der Software sowie Überprüfung und Reparatur oder Austausch von Hardware.

Absatz 2 verlangt, alle Möglichkeiten auszuschöpfen, dass bei der Wartung und Fernwartung auf die Offenbarung personenbezogener Daten verzichtet werden kann. Dies bedeutet auch, dass bei der Auswahl von Wartungs-, insbesondere von Fernwartungskonzepten jenen der Vorzug zu geben ist, die den Zugriff auf personenbezogene Daten ausschließen oder zumindest minimieren. Da dies nicht in jedem Fall möglich ist, ist der Zugriff auf personenbezogene Daten seitens der Daten verarbeitenden Stelle auf das erforderliche Maß zu beschränken.

In Absatz 3 werden konkrete Maßnahmen vorgegeben, die bei einer Wartung wirksam werden müssen. Diese Maßnahmen decken sich mit den Anforderungen aus der veröffentlichten Orientierungshilfe der Datenschutzbeauftragten des Bundes und der

Länder. Sie sollen insbesondere die notwendige Sicherheit bei der Fernwartung ermöglichen.

Absatz 4 verlangt die vertragliche Absicherung der Wartung und der dabei zu treffenden Maßnahmen. Mit der Verpflichtung auf das Datengeheimnis wird auch eine strafrechtliche Verantwortlichkeit vorgegeben.

Absatz 5 privilegiert die Wartung von Systemen, an deren Wartungsschnittstelle nur ausreichend verschlüsselte, anonymisierte oder pseudonymisierte personenbezogene Daten auftreten können. Diese Eigenschaft der Daten führt zu keinen Einschränkungen der Wartung, wohl aber zu einer entscheidenden Sicherung der Vertraulichkeit dieser Daten.

4. Fernmess- und Fernwirkdienste

(1) Öffentliche Stellen dürfen in Wohnungen oder Geschäftsräumen ferngesteuerte Messungen vornehmen (Fernmessdienste) oder mittels einer Übertragungseinrichtung andere Wirkungen auslösen (Fernwirkdienste), wenn der Betroffene eingewilligt hat und für ihn erkennbar ist, wann ein Dienst in Anspruch genommen wird und welcher Art der Dienst ist. Die Einwilligung kann jederzeit widerrufen werden. Das Abschalten eines Dienstes durch den Betroffenen gilt im Zweifel als Widerruf der Einwilligung.

(2) Die Erbringung einer Leistung sowie der Abschluss oder die Abwicklung eines Vertragsverhältnisses dürfen nicht von der Einwilligung nach Absatz 1 abhängig gemacht werden. Verweigert oder widerruft der Betroffene seine Einwilligung, so dürfen ihm daraus keine Nachteile entstehen, die über die nachweisbaren Mehrkosten einer anderen Art der Datenerhebung hinausgehen.

Begründung zu 4:

Angesichts der stark zunehmenden Nutzung von Techniken zum Fernmessen und Fernwirken auch im öffentlichen Bereich und der Schwierigkeit, auf dieses Phänomen die allgemeinen Vorschriften anzuwenden, ist es nötig, spezielle Regelungen zu treffen.

Bereits aus den allgemeinen Vorschriften über die Unterrichtung bei der Einholung der Einwilligung und bei der Datenerhebung ergibt sich, dass der Betroffene vollständig über Verwendungszweck, Art, Umfang und Zeitraum des Einsatzes des Fernmessdienstes zu unterrichten ist. Entsprechendes gilt für Fernwirkdienste. Auch auf eine besondere Vorschrift zur Zweckbindung konnte verzichtet werden, da insoweit die allgemeine Vorschrift nach § ? Platz greift.

Satz 1 in Absatz 1 definiert die Dienste und macht ihren Einsatz von der Einwilligung des Betroffenen und der Erkennbarkeit ihrer Anspruchnahme abhängig. Dadurch wird dem Transparenzgebot Rechnung getragen und der Betroffene von einer ungewollten Erfassung seiner Daten geschützt. Die Sätze 2 und 3 ermöglichen dem Betroffenen einen jederzeitigen Ausstieg aus der telemetrischen Datenverarbeitung.

Durch Absatz 2 soll verhindert werden, dass der Betroffene aus wirtschaftlichen Gründen gezwungen ist, diese Dienste in Anspruch zu nehmen oder von einem Ausstieg aus ihrer Nutzung abzusehen.

5. Elektronische Einwilligung
Eine Einwilligung kann auch elektronisch erklärt werden, wenn sichergestellt ist, dass

1. sie nur durch eine eindeutige und bewusste Handlung des Betroffenen erfolgen kann,
2. sie nicht unerkennbar verändert werden kann,
3. sie ihrem Urheber zugeordnet werden kann und
4. die Einwilligung bei der verarbeitenden Stelle protokolliert wird.

Begründung zu 5:
Informationen zwischen Bürgern und Verwaltung werden zukünftig auch elektronisch ausgetauscht werden. Wie im Teledienste- und Medienrecht sollte in den allgemeinen Datenschutzgesetzen die Möglichkeit vorgesehen werden, die datenschutzrechtliche Einwilligung statt in der grundsätzlich vorgeschriebenen Schriftform nach Wunsch auch elektronisch abzugeben. Eine notwendige Voraussetzung ist die digitale Signatur nach dem Signaturgesetz.

4. Begriffsdefinitionen

Anonymisieren
Anonymisieren ist das Verändern personenbezogener Daten derart, dass Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig hohen Aufwand einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.

Pseudonymisieren
Pseudonymisieren ist das Verändern personenbezogener Daten durch eine Zuordnungsvorschrift derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse ohne Kenntnis oder Nutzung der Zuordnungsvorschrift nicht mehr einer natürlichen Person zugeordnet werden können.

Verschlüsseln
Verschlüsseln ist die Transformation von Daten in eine Darstellung, die ohne Kenntnis des Schlüssels und ohne unverhältnismäßig hohen Aufwand keine Rückschlüsse auf die ursprünglichen Daten erlaubt.

Hinweise zu weiteren Begriffsbestimmungen
Die Arbeitsgruppe hat sich mit der Frage beschäftigt, ob die Begriffe

- automatisierte Verfahren und
- Veröffentlichung

in den Datenschutzgesetzen zu definieren sind. Die Arbeitsgruppe hat davon abgesehen, weil keine Regelungsnotwendigkeit bzw. kein vorrangig technischer Schwerpunkt erkennbar waren.

5. Grundsätze

1. Datensparsamkeit

(1) Die Gestaltung von Verfahren und die Auswahl von informationstechnischen Produkten zum Einsatz in automatisierten Verfahren hat sich am Grundsatz größtmöglicher Datensparsamkeit zu orientieren.

(2) Verfahren sollen so gestaltet werden, dass personenbezogene Daten so weitgehend und früh wie möglich anonymisiert oder, falls dies nicht möglich ist, pseudonymisiert werden.

Begründung zu 1:

Das Prinzip der Datensparsamkeit lässt sich wie folgt vom Grundsatz der Erforderlichkeit abgrenzen: Während die Erforderlichkeit als rechtliche Anforderung den Umfang der Datenverarbeitung in jedem Einzelfall beschränkt, sind die Regelungen zur Datensparsamkeit vor allem als Gestaltungsanforderungen für IT-Systeme zu verstehen, die auch mehreren unterschiedlichen Aufgaben dienen können. Im Rahmen der Deregulierung wird die Tendenz zu „offen“ formulierten Generalklauseln vermutlich zunehmen. Gerade aber dort, wo die Art der zu verarbeitenden personenbezogenen Daten im Gesetz, in der Verordnung oder in der Satzung nicht explizit festgelegt ist, hat der Grundsatz der Datensparsamkeit bei der Gestaltung von Verfahren und bei der Auswahl von Produkten besondere Bedeutung. Schließlich soll er auch bewirken, dass zeitgerechte Datenlöschungen nicht durch „systembedingte“ Speicherungen unterlaufen werden. Ein Beispiel für ein System, das diesen Anforderungen nicht entspricht, sind solche Datenträger, bei denen die sequentielle Löschung einzelner nicht mehr erforderlicher Daten nicht möglich ist (z. B. CD-ROM). Ein positives Beispiel sind Abrechnungssysteme, die die Bezahlung der Nutzung kostenpflichtiger öffentlicher Einrichtungen auch ohne namentliche Erfassung des Zahlungspflichtigen ermöglichen (z. B. Prepaid-Verfahren). Wichtigster Anwendungsbereich wird die Beschaffung von IT-Systemen sein. Die Vorschrift versteht sich auch als ein Signal an die Anbieter, dass sie künftig mit entsprechenden Anforderungen von öffentlich-rechtlichen Kunden rechnen müssen.

2. Hinweise zu weiteren Grundsätzen

Die Arbeitsgruppe hat sich mit den Themen Datenschutz-Audit und Vorabkontrolle beschäftigt und ist zu der Auffassung gelangt, dass hierzu keine Regelungsnotwendigkeit besteht bzw. kein vorrangig technischer Schwerpunkt erkennbar ist.

[1] Erarbeitet vom Arbeitskreis Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder.

[2] Erarbeitet vom Arbeitskreis Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder.

16 Materialien

16.1 Entschließungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder

16.1.1 Entschließung der 56. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 5./6. Oktober 1998 in Wiesbaden zur Prüfungskompetenz der Datenschutzbeauftragten bei den Gerichten

Die Datenschutzbeauftragten des Bundes und der Länder stellen fest, dass in der Praxis die Abgrenzung ihrer Zuständigkeiten bei den Gerichten immer wieder Anlass von Unsicherheiten ist. Sie weisen daher darauf hin, dass die Beschränkung der Prüfkompetenz bei den Gerichten einzig und allein den Zweck hat, den grundgesetzlich besonders geschützten Bereich der richterlichen Unabhängigkeit von Kontrollen freizuhalten.

Deshalb erstreckt sich die Kontrolle der Datenschutzbeauftragten bei den Gerichten u. a. auch darauf, ob die erforderlichen technischen und organisatorischen Maßnahmen zur Datensicherung getroffen und eingehalten werden, insbesondere bei automatisierter Datenverarbeitung.

Die Datenschutzbeauftragten des Bundes und der Länder halten eine gesetzliche Klarstellung für hilfreich, dass Gerichte der Kontrolle des Bundesbeauftragten bzw. der Landesbeauftragten für den Datenschutz unterliegen, soweit sie nicht in richterlicher Unabhängigkeit tätig werden.

16.1.2 Entschließung der 56. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 5./6. Oktober 1998 in Wiesbaden zu fehlenden bereichsspezifischen Regelungen bei der Justiz

Derzeit werden in allen Bereichen der Justiz - bei Staatsanwaltschaften, Gerichten und Gerichtsvollziehern - im Zuge von Modernisierungsvorhaben umfassende Systeme der automatisierten Datenverarbeitung eingeführt mit der Folge, dass sensible personenbezogene Daten auch hier in viel stärkerem Maße verfügbar werden als bisher. Sogar die Beauftragung Privater mit der Verarbeitung sensibler Justizdaten wird erwogen. Gerade vor dem Hintergrund dieser vollkommen neuen Qualität der Datenverarbeitung in der Justiz wird deutlich, dass die Rechtsprechung des Bundesverfassungsgerichts zum sogenannten Übergangsbonus hier keine tragfähige Grundlage für Eingriffe in die informationelle Selbstbestimmung mehr darstellen kann. Vielmehr müssen die Entscheidungen des Gesetzgebers den Maßstab für die weitere technische Ausgestaltung der Datenverarbeitung innerhalb der Justiz bilden und nicht umgekehrt. Dabei ist nicht nur für formell ausreichende Rechtsgrundlagen Sorge zu tragen. Auch Fragen der Datensicherheit und der Ordnungsmäßigkeit der Datenverarbeitung bedürfen der Regelung.

Seit dem Volkszählungsurteil des Bundesverfassungsgerichts sind 15 Jahre vergangen. Dennoch werden ausgerechnet im Bereich der Justiz sensible personenbezogene Daten nach wie vor ohne die vom Bundesverfassungsgericht geforderten bereichsspezifischen gesetzlichen Grundlagen erhoben und verarbeitet.

Die Datenschutzbeauftragten des Bundes und der Länder bekräftigen deshalb im Anschluss an ihren Beschluss der 48. Konferenz vom 26./27.09.1994 in Potsdam ihre wiederholten Forderungen zu bereichsspezifischen Regelungen bei der Justiz.

Zwar hat der Gesetzgeber in der abgelaufenen Legislaturperiode zumindest Regelungen über Datenerhebungen, -verarbeitung und -nutzung im Strafvollzug sowie über die Datenübermittlung von Amts wegen durch Gerichte und Staatsanwaltschaften an Gerichte, Behörden und sonstige öffentliche Stellen geschaffen.

Trotzdem sind in wichtigen Bereichen gesetzliche Regelungen weiterhin überfällig. Ausreichende gesetzliche Regelungen fehlen vor allem für

- weite Bereiche der Datenverarbeitung im Strafverfahren, insbesondere in automatisierten Dateien

  namentlich die
- Übermittlung von Strafverfahrensdaten an nicht am Strafverfahren beteiligte dritte Stellen;

- Rechte der Betroffenen (nicht nur der Beschuldigten, sondern auch von Zeugen und sonstigen Personen, deren Daten gespeichert werden) in Bezug auf Daten, die im Zusammenhang mit einem Strafverfahren gespeichert werden.

- Aufbewahrung von Akten, Karteien und sonstigen Unterlagen sowie die Dauer der Speicherung in automatisierten Dateien;

- Datenübermittlung zu wissenschaftlichen Zwecken;

- Datenverarbeitung in der Zwangsvollstreckung;

- Datenverarbeitung im Jugendstrafvollzug;

- Datenverarbeitung im Vollzug der Untersuchungshaft.

Der Gesetzgeber sollte daher in der kommenden Legislaturperiode zügig die notwendigen Novellierungen, für die zum Teil ja schon erhebliche Vorarbeiten geleistet worden sind, aufgreifen. Dabei ist nicht die jeweils geübte Praxis zu legalisieren, sondern es muss vorab unter datenschutzrechtlichen Gesichtspunkten geprüft werden, welche Form der Datenerhebung und -verarbeitung in welchem Umfang erforderlich ist. Ferner hat der Gesetzgeber jeweils bereichsspezifisch zu prüfen, inwieweit Aufgaben der Justiz und damit verbundene Datenverarbeitungen Privaten übertragen werden dürfen.

Der Entwurf für ein „StVÄG 1996“ erfüllt diese Voraussetzungen nicht, im Gegenteil fällt er teilweise hinter den bereits erreichten Standard der allgemeinen Datenschutzgesetze und anderer bereichsspezifischer Regelungen (wie z. B. dem Bundeszentralregistergesetz und den Polizeigesetzen der Länder) zurück. Zu kritisieren sind vor allem:

- Mangelnde Bestimmtheit der Voraussetzungen für Maßnahmen der Öffentlichkeitsfahndung

- Unangemessen weite Auskunfts- und Akteneinsichtsmöglichkeiten für nicht Verfahrensbeteiligte

- Unzureichende Regelungen über Inhalt, Ausmaß und Umfang von staatsanwaltlichen Dateien und Informationssystemen

Die Datenschutzbeauftragten halten es deshalb zum Schutz des Rechts des Einzelnen auf informationelle Selbstbestimmung für geboten, wegen der mit der Datenerhebung, Verarbeitung und Nutzung verbundenen Rechtseingriffe unverzüglich in der neuen Legislaturperiode bereichsspezifische Regelungen der materiellen Voraussetzungen sowie der organisatorischen und verfahrensrechtlichen Vorkehrungen zu schaffen, welche der Gefahr einer Verletzung des Persönlichkeitsrechtes der Bürgerinnen und Bürger entgegenwirken.

16.1.3 Entschließung der 56. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 5./6. Oktober 1998 in Wiesbaden zur Verweigerung der Auskunft durch das Bundesamt für Finanzen auf Anfragen Betroffener über ihre Freistellungsaufträge

Die Datenschutzbeauftragten des Bundes und der Länder betonen das Recht der Bürgerinnen und Bürger auf Auskunft über ihre Daten auch gegenüber der Finanzverwaltung (§ 19 BDSG). Die Betroffenen haben Anspruch, von dem Bundesamt für Finanzen Auskunft über die Freistellungsaufträge zu erhalten, die sie ihrer Bank im Zusammenhang mit dem steuerlichen Abzug von Zinsen erteilt haben.

Der Bundesbeauftragte für den Datenschutz hat die Verweigerung der Auskünfte gegenüber dem Bundesministerium der Finanzen beanstandet und dieses aufgefordert, den entsprechenden Erlass an das Bundesamt aufzuheben. Bisher hat das Ministerium in der Sache allerdings nicht eingelenkt.

Für die Betroffenen ergibt sich hierdurch ein unhaltbarer Zustand. Ihnen wird die Auskunft zu Unrecht vorenthalten.

Die Datenschutzbeauftragten der Länder unterstützen mit Nachdruck die Forderung des Bundesbeauftragten für den Datenschutz gegenüber dem Bundesministerium der Finanzen, seinen Erlass an das Bundesamt für Finanzen aufzuheben und dieses anzuweisen, dem Auskunftsanspruch der Auftraggeber von Freistellungsaufträgen nachzukommen.

16.1.4 Entschließung der 56. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 5./6. Oktober 1998 in Wiesbaden zur Weitergabe von Meldedaten an Adressbuchverlage und Parteien

Bei den Datenschutzbeauftragten des Bundes und der Länder gehen viele Beschwerden ein, in denen deutlicher Unmut über veröffentlichte Daten in Adressbüchern und unverlangt erhaltene Werbesendungen geäußert wird. Vor Wahlen nehmen die Beschwerden noch zu. Überrascht stellten Betroffene fest, dass sie persönlich adressierte Wahlwerbung der Parteien bekommen. Ihnen ist unerklärlich, wie Adressbuchverlage und Parteien an ihre Adressen gekommen sind. Sie erhalten auf Anforderung Daten aus den kommunalen Melderegistern. Damit sind die Adressbuchverlage und Parteien gegenüber anderen gesellschaftlichen Gruppen privilegiert.

Dieser Umgang mit Meldedaten ist weder transparent noch angemessen. Die Konferenz tritt dafür ein, die Rechte der Bürgerinnen und Bürger zu verbessern. Die Information über die Widerspruchsmöglichkeit erreicht die Menschen häufig nicht. Vorzuziehen ist deshalb eine Einwilligungslösung. Sie würde das Grundrecht auf informationelle Selbstbestimmung konsequent umsetzen - erst fragen, dann handeln. Nach der Einwilligungslösung ist eine Erklärung informierter Bürgerinnen und Bürger gegenüber dem Meldeamt nötig, ob sie mit den Datenweitergaben an die genannten Empfänger einverstanden sind oder nicht.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder empfiehlt den gesetzgebenden Körperschaften, künftig die Einwilligungslösung vorzusehen.

16.1.5 Entschließung der 56. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 5./6. Oktober 1998 in Wiesbaden zu Entwicklungen im Sicherheitsbereich

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder stellt fest, dass die Sicherheitsbehörden in den vergangenen Jahren umfangreiche zusätzliche Eingriffsbefugnisse erhalten haben. Demgegenüber fehlen in weiten Teilen Erkenntnisse über die Wirksamkeit und Grundrechtsverträglichkeit der Anwendung dieser Instrumente, wie z. B. bei der Schleppnetzfahndung und der Ausweitung der Telefonüberwachung.

Die Datenschutzbeauftragten des Bundes und der Länder erwarten vom Bundesgesetzgeber und der Bundesregierung, dass die Erforderlichkeit und die Wirksamkeit aller Eingriffsbefugnisse anhand objektiver Kriterien überprüft werden (Evaluierung).

16.1.6 Entschließung der 56. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 5./6. Oktober 1998 in Wiesbaden zur Dringlichkeit der Datenschutzmodernisierung

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt und unterstützt grundsätzlich die vom 62. Deutschen Juristentag (DJT) im September

1998 in Bremen gefassten Beschlüsse zum Umgang mit Informationen einschließlich personenbezogener Daten. Von den gesetzgebenden Körperschaften erhofft sich die Konferenz die Berücksichtigung dieser Beschlüsse bei der nunmehr dringend erforderlichen Umsetzung der EG-Datenschutzrichtlinie in Bundes- und Landesrecht.

Insbesondere betont die Konferenz folgende Punkte:

- Die materiellen Anforderungen des Datenschutzrechts sind angesichts der wachsenden Datenmacht in privater Hand auf hohem Niveau grundsätzlich einheitlich für den öffentlichen wie für den privaten Bereich zu gestalten.

- Die anlassfreie Aufsicht für die Einhaltung des Datenschutzes im privaten Bereich muss in gleicher Weise unabhängig und weisungsfrei ausgestaltet werden wie die Datenschutzkontrolle bei öffentlichen Stellen.

- Die Rechte der Bürgerinnen und Bürger sind zu stärken; als Voraussetzung für die Ausübung des Rechts auf informationelle Selbstbestimmung der Betroffenen sind die Verpflichtungen zu ihrer Information, Aufklärung und ihren Wahlmöglichkeiten ohne faktische Zwänge auszuweiten.

- Ein modernisiertes Datenschutzrecht hat die Grundsätze der Datenvermeidung, des Datenschutzes durch Technik, der Zweckbindung der Daten und ihres Verwendungszusammenhangs in den Mittelpunkt zu stellen.

- Zur Sicherstellung vertraulicher und unverfälschter elektronischer Kommunikation ist die staatliche Förderung von Verschlüsselungsverfahren geboten, nicht eine Reglementierung der Kryptographie.

16.1.7 Entschließung der 57. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25./26. März 1999 in Schwerin zur Modernisierung des Datenschutzrechts jetzt - umfassende Novellierung des BDSG nicht auf schieben

Die deutschen Datenschutzbeauftragten haben bereits früh gefordert, die Novellierung des BDSG zur Umsetzung der EG-Datenschutzrichtlinie zu einer gründlichen Modernisierung des veralteten deutschen Datenschutzrechts zu nutzen. Da die dreijährige Anpassungsfrist im Oktober 1998 verstrichen ist, besteht jetzt ein erheblicher Zeitdruck. Für die Neuregelung, die derzeit in der Bundesregierung und in Koalitionsgremien vorbereitet wird, ist daher ein „Zwei-Stufen-Konzept“ vorgesehen. Einem ersten, in Kürze vorzulegenden Novellierungsgesetz soll zu einem späteren Zeitpunkt eine zweite Änderung folgen, die weitere Verbesserungen enthalten soll. Die Konferenz geht davon aus, dass das Zweistufenkonzept von dem festen politischen Willen getragen wird, die zweite Stufe nach Einbindung des ersten Gesetzentwurfes zügig in Angriff zu nehmen und noch in dieser Legislaturperiode abzuschließen. Auch der in dieser Stufe bestehende Handlungsbedarf duldet keinen Aufschub.

Die Konferenz begrüßt, dass jetzt mit Hochdruck an der BDSG-Novellierung gearbeitet wird und Verantwortliche in Regierung und Fraktionen zugesagt haben, die erste Stufe der Neuregelung werde sich nicht auf das von der Richtlinie geforderte Minimum beschränken. Sie unterstützt die Vorschläge, Regelungen zur Videoüberwachung, zu Chipkarten und zum Datenschutzaudit aufzunehmen. Gleiches gilt für die Übernahme der zukunftsweisenden Bestimmungen zur Datenvermeidung sowie zur anonymen bzw. pseudonymen Nutzung von Telediensten aus dem Multimediarecht. Diese sind wichtige und dringend notwendige Regelungen zur Modernisierung des Datenschutzrechts. Die Konferenz drückt daher ihre Erwartung darüber aus, dass diese Vorschriften in der ersten Stufe des Gesetzgebungsverfahrens zügig verabschiedet werden.

Zu den Punkten, die keinen Aufschub dulden, gehört auch die Verbesserung der Voraussetzungen für eine effektive Datenschutzkontrolle. Die völlig unabhängige Gestaltung der Kontrolle im nichtöffentlichen Bereich muss institutionell sichergestellt und durch eine sachgerechte finanzielle und personelle Ausstattung unterstützt werden. Gegenwärtig noch bestehende Einschränkungen der Kontrollkompetenzen im öffentlichen Bereich müssen abgebaut, den Aufsichtsbehörden müssen wirksame Befugnisse an die Hand gegeben werden.

Zum Schutz der Bürgerinnen und Bürger sind bei massenhaften Datenerhebungen mit unkalkulierbaren Datenverarbeitungsrisiken oder ungeklärter Zweckbestimmung klare materielle Grenzen durch den Gesetzgeber zu ziehen.

Die bereichsspezifischen Gesetze, z. B. die Sicherheitsgesetze, dürfen nicht vom Bundesdatenschutzgesetz mit den dort zu erwartenden substantiellen Fortschritten für die Bürgerinnen und Bürger, wie beispielsweise einem verbesserten Auskunftsrecht, abgekoppelt werden.

Notwendig ist nach Auffassung der Konferenz, dass das Datenschutzrecht auch in Zukunft bürgerfreundlich und gut lesbar formuliert ist. Dies ist eine unverzichtbare Akzeptanzvoraussetzung für den Datenschutz bei Bürgern, Wirtschaft und Verwaltung.

16.1.8 Entschließung der 57. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25./26. März 1999 in Schwerin zur geplanten erweiterten Speicherung von Verbindungsdaten in der Telekommunikation

Die Bundesregierung und der Bundesrat werden demnächst über den Erlass der seit längerem überfälligen Rechtsverordnung zum Datenschutz in der Telekommunikation aufgrund des Telekommunikationsgesetzes zu entscheiden haben.

Im Gegensatz zur früheren analogen Vermittlungstechnik erzeugt und verarbeitet das digitalisierte Telekommunikationsnetz (ISDN-Netz) in großem Umfang personenbezogene Verbindungsdaten. Dies zwingt zu begrenzenden, am Grundsatz der Datensparsamkeit orientierten Regelungen, um das Fernmeldegeheimnis und das

Grundrecht auf Telefonkundinnen und -kunden auf unbeobachtete Kommunikation zu garantieren.

Die bisher geltende Telekommunikationsdienstunternehmen-Datenschutzverordnung von 1996 sieht vor, dass die Verbindungsdaten unter Kürzung der Zielrufnummer regelmäßig bis zu 80 Tagen nach Versendung der Rechnung gespeichert werden dürfen. Über diese Frist hinaus dürfen Verbindungsdaten nur gespeichert bleiben, wenn Streit zwischen dem Telekommunikationsunternehmen und den Kunden über die Richtigkeit der Abrechnung entsteht.

Demgegenüber gibt es Überlegungen für eine neue Telekommunikations-Datenschutzverordnung, dass alle Verbindungsdaten in der Regel selbst bei unbestrittenen oder bezahlten Rechnungen zwei Jahre lang nach Ende der Verbindung gespeichert bleiben können. Da die Speicherungsfrist erst am Ende des Jahres beginnen soll, in dem die Verbindung stattfand, kann dies in Einzelfällen dazu führen, dass die Daten bis zu drei Jahre lang vorgehalten werden.

Hiergegen wenden sich die Datenschutzbeauftragten des Bundes und der Länder mit Entschiedenheit. Sie sehen darin einen unverhältnismäßigen Eingriff in das Grundrecht der Telefonkundinnen und -kunden auf unbeobachtete Kommunikation. Auch das Telekommunikationsgesetz hebt die Grundsätze der Verhältnismäßigkeit und der Zweckbindung ausdrücklich hervor. Personenbezogene Daten, die für Zwecke der Telekommunikation erhoben und verarbeitet werden, dürfen nur solange gespeichert bleiben, wie es zu diesen Zwecken erforderlich ist. Auch die vom Gesetz geforderte Höchstfrist für die Speicherung von Verbindungsdaten muss sich am Grundsatz der Datensparsamkeit orientieren, solange sich die Kundin und der Kunde nicht ausdrücklich für eine längere Speicherung entscheiden.

Die Dauer einer zivilrechtlichen Verjährungsfrist kann ebenfalls kein rechtfertigender Anlass für eine solche Datenspeicherung sein. Jedenfalls müssen die Daten unverzüglich gelöscht werden, wenn die Rechnung beglichen und unbestritten ist und damit der vertragliche Speicherzweck erledigt ist.

Da eine telekommunikations- oder zivilrechtlich bedingte Notwendigkeit für eine derart lange Speicherfrist der Verbindungsdaten somit nicht ersichtlich ist, würde sie eine unzulässige Datenspeicherung auf Vorrat zu unbestimmten Zwecken darstellen.

Diese Speicherung von Kommunikationsdaten wäre auch nicht mit der Überlegung zu rechtfertigen, dass diese Daten zum Zwecke eventueller künftiger Strafverfolgung benötigt werden könnten. Die mit einer solchen Speicherung verbundene vorsorgliche Überwachung unverdächtiger Bürgerinnen und Bürger wäre unzulässig.

16.1.9 Entschließung der 57. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25./26. März 1999 in Schwerin zum Entwurf einer Ratsentschließung zur Überwachung der Telekommunikation (ENFOPOL ‘98)

Gegenwärtig berät der Rat der EU über den Entwurf einer Entschließung zur grenzüberschreitenden Überwachung der Telekommunikation und der Internet-Nutzung (ENFOPOL ‘98).

Die Konferenz der Datenschutzbeauftragten hält es für inakzeptabel, dass der entsprechende Entwurf bisher geheim gehalten und ohne Einbeziehung der Datenschutzbeauftragten beraten wird.

Sie fordert die Bundesregierung auf, der Schaffung gemeinsamer Standards zur grenzüberschreitenden Überwachung der Telekommunikation nur insoweit zuzustimmen, als damit nicht zusätzliche Eingriffe in das Grundrecht auf unbeobachtete Kommunikation und das Fernmeldegeheimnis verbunden sind und die Nutzung datenschutzfreundlicher Technologien (z. B. prepaid cards) nicht konterkariert wird.

16.1.10 Entschließung der 57. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25./26. März 1999 in Schwerin zur transparenten Hard- und Software

Die Datenschutzbeauftragten des Bundes und der Länder haben sich wiederholt für die Nutzung datenschutzfreundlicher Technologien eingesetzt. Sie sehen jedoch mit Sorge die Entwicklung im Bereich der Informationstechnik, die zu neuen Industriestandards und Produkten führt, die für die Benutzerinnen und Benutzer kaum durchschaubar und selbst für Fachleute nur noch eingeschränkt revisionsfähig sind.

Beispielsweise sind seit kurzem mit dem Intel Pentium III-Prozessor bestückte PCs auf dem Markt, deren Prozessor bei der Herstellung mit einer eindeutigen Nummer (Processor Serial Number - PSN) versehen wurde. Intel sieht vor, das Auslesen der PSN durch die Nutzerinnen und Nutzer kontrollieren zu lassen. Die mittlerweile bekannt gewordenen Manipulationsmöglichkeiten der dafür erforderlichen Software machen deutlich, dass die Existenz einer solchen eindeutigen Kennung kaum kontrollierbare Nutzungsmöglichkeiten eröffnet, die dem Datenschutz diametral zuwider laufen.

Die durch den Intel Pentium III initiierte Debatte um eindeutige Kennungen brachte ans Tages- licht, dass Softwarehersteller Nutzern neuerer Office-Produkte ohne deren Wissen eindeutige Kennungen zuordnen. Diese Kennungen können in Dokumenten versteckt sein und bei der Nutzung des Internets von Softwareherstellern verdeckt abgefragt werden.

Werden Daten der Nutzerinnen und Nutzer übermittelt, ohne dass sie dies bemerken, kann deren missbräuchliche Verwendung die Anonymität der Anwender von Informationstechnik weiter aushöhlen. Den Erfordernissen des Datenschutzes wird aber

nur dann ausreichend Rechnung getragen, wenn zum Schutz der Privatheit transparente und von den Nutzerinnen und Nutzern in eigener Verantwortung bedienbare Sicherheitsfunktionen zur Verfügung stehen.

Deshalb erwarten die Datenschutzbeauftragten des Bundes und der Länder von Herstellern von Informations- und Kommunikationstechnik, Hard- und Software so zu entwickeln und herzustellen, dass Anwender und unabhängige Dritte sich jederzeit von der Wirksamkeit von Sicherheitsvorkehrungen überzeugen können.

Den Anwendern moderner Technik empfehlen die Datenschutzbeauftragten, nur solche Produkte einzusetzen, welche auch eine Transparenz der Verfahrensabläufe gewährleisten.

16.2 Sonstiges

Einwilligungserklärung für Videomitschnitte von Unterrichtsstunden

Einwilligungserklärung

Ich bin/Wir sind damit einverstanden, dass [Name der ausbildenden Stelle] während des Unterrichts filmt und ein Video erstellt. Das Video dient ausschließlich der Ausbildung von Lehramtsanwärtern/Studienreferendaren und wird gelöscht, sobald es für diese Zwecke ausgewertet wurde.

Ich bin/Wir sind darauf hingewiesen worden, dass diese Einwilligung verweigert werden darf und der Schülerin bzw. dem Schüler dadurch keine Nachteile entstehen.

_____ _____

Ort Datum

_____ _____

Name, Vorname, Klasse der Schülerin/des Schülers

Unterschrift der Schülerin/des Schülers
(nur wenn älter als 15 Jahre)

_____

Unterschrift mindestens einer sorgeberechtigten Person
(entfällt bei volljährigen Schülerinnen und Schülern)