Sächsischer Landtag DRUCKSACHE 2/9004
2. Wahlperiode

# Schutz des Persönlichkeitsrechts im öffentlichen Bereich

## 6. Tätigkeitsbericht

## des

## Sächsischen Datenschutzbeauftragten

Dem Sächsischen Landtag

vorgelegt zum 31. März 1998

gemäß § 27 des Sächsischen Datenschutzgesetzes

Eingegangen am: 19. August 1998 Ausgegeben am: 20. August 1998

Vorbemerkung zum Sprachgebrauch in diesem Bericht:

Logisch ist zu unterscheiden zwischen biologischem und grammatischem Geschlecht (sexus und genus). Es wäre ein Verlust, diese Unterscheidung aufzugeben; es wäre das Unterfangen, Sprache zu sexualisieren. Ich beteilige mich nicht an solchen Versuchen. Frauen bitte ich, sich auch von scheinbar männlichen, in Wahrheit nur generellen Bezeichnungen gemeint zu wissen: Bauherr, Lehrer, Beamter, Betroffener etc. (Übrigens gibt es auch den umgekehrten Fall: Der [männliche] Entbindungspfleger ist eine Hebamme i. S. v. § 53 Abs. 1 Nr. 3 StPO.)

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

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

Vervielfältigung erwünscht.

Herstellung: OTTO Verlag und 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.

| | |
|---|---|
| AO | Abgabenordnung |
| ArbschG | Arbeitsschutzgesetz vom 7. August 1996 (BGBl. I S. 1246), zuletzt geändert durch Gesetz vom 16. Dezember 1997 (BGBl. I S. 2970) |
| ArbZG | Arbeitszeitgesetz vom 6. Juni 1994 (BGBl. I S. 1170) |
| AsylVfG | Gesetz über das Asylverfahren (Asylverfahrensgesetz) in der Fassung der Bekanntmachung vom 27. Juli 1993 (BGBl. I S. 1361), zuletzt geändert durch Artikel 2 des Gesetzes vom 29. Oktober 1997 (BGBl. I S. 2584) |
| AuslG | Gesetz über die Einreise und den Aufenthalt von Ausländern im Bundesgebiet (Ausländergesetz) vom 9. Juli 1990 (BGBl. I S. 1354), zuletzt geändert durch Art. 14 des Ersten Gesetzes zur Änderung des Dritten Buches Sozialgesetzbuch und anderer Gesetze vom 16. Dezember 1997 (BGBl. I S. 2970) |
| BauGB | Baugesetzbuch |
| BDSG | Gesetz zur Fortentwicklung der Datenverarbeitung und des Datenschutzes (Bundesdatenschutzgesetz) |
| BildscharbV | Verordnung über Sicherheit und Gesundheitsschutz bei der Arbeit an Bildschirmgeräten (Bildschirmarbeitsverordnung) vom 4. Dezember 1996 (BGBl. I S. 1841) |
| BImSchG | Gesetz zum Schutz vor schädlichen Umwelteinwirkungen durch Luftverunreinigungen, Geräusche, Erschütterungen und ähnliche Vorgänge (Bundes-Immissionsschutzgesetz) vom 15. März 1974 (BGBl. I S. 721, 1193) in der Neufassung vom 14. Mai 1990 (BGBl. I S. 880), zuletzt geändert durch Art. 1 des Gesetzes vom 9. Oktober 1996 (BGBl. I S. 1498) |

| | |
|---|---|
| 1. BMeldDÜV | Verordnung zur Durchführung von regelmäßigen Datenübermittlungen zwischen Meldebehörden verschiedener Länder (1. Meldedaten-Übermittlungsverordnung des Bundes) vom 18. Juni 1983 (BGBl. I S. 943) |
| BNDG | Gesetz über den Bundesnachrichtendienst (BND-Gesetz) vom 20. Dezember 1990 (BGBl. I S. 2979) |
| BRAO | Bundesrechtsanwaltsordnung vom 1. August 1959 (BGBl. I S. 565), zuletzt geändert durch das Gesetz zur Neuordnung des Berufsrechts der Rechtsanwälte und der Patentanwälte vom 2. September 1994 (BGBl. I S. 2278) |
| BSHG | Bundessozialhilfegesetz in der Fassung der Bekanntmachung vom 10. Januar 1991 (BGBl. I S. 94, ber. S. 808), zuletzt geändert durch Art. 11 des Ersten Gesetzes zur Änderung des Dritten Buches Sozialgesetzbuch und anderer Gesetze vom 16. Dezember 1997 (BGBl. I S. 2970) |
| BSO | Verordnung des Sächsischen Staatsministeriums für Kultus über die Berufsschule im Freistaat Sachsen (Schulordnung Berufsschule) vom 11. März 1994 (GVBl. S. 477) |
| BStatG | Gesetz über die Statistik für Bundeszwecke (Bundesstatistikgesetz) vom 22. Januar 1987 (BGBl. I S. 462, 565), zuletzt geändert durch Art. 2 des Mikrozensusgesetzes und Gesetzes zur Änderung des Bundesstatistikgesetzes vom 17. Januar 1996 (BGBl. I S. 34) |
| BtBG | Gesetz über die Wahrnehmung behördlicher Aufgaben bei der Betreuung Volljähriger (Betreuungsbehördengesetz) vom 12. September 1990 (BGBl. I S. 2002, 2025) |
| BtG | Gesetz zur Reform des Rechts der Vormundschaft und Pflegschaft für Volljährige (Betreuungsgesetz) vom 12. September 1990 (BGBl. I S. 2002) |
| BVerfSchG | Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz vom 20. Dezember 1990 (BGBl. I S. 2954), zuletzt geändert durch § 38 Abs. 2 des Sicherheitsüberprüfungsgesetzes vom 20. April 1994 (BGBl. I S. 867) |

| | |
|---|---|
| BVG | Gesetz über die Versorgung der Opfer des Krieges (Bundesversorgungsgesetz) vom 20. Dezember 1950 (BGBl. I S. 791) in der Fassung der Bekanntmachung vom 22. Januar 1982 (BGBl. I S. 21), zuletzt geändert durch Art. 25 des Gesetzes zur Reform der gesetzlichen Rentenversicherung vom 16. Dezember 1997 (BGBl. I S. 2998) |
| DA | Dienstanweisung für die Standesbeamten und ihre Aufsichtsbehörden vom 23. November 1987 (BAnz. Nr. 227 a), zuletzt geändert durch Änderungsverwaltungsvorschrift vom 31. März 1994 (BAnz. S. 3881) |
| DVStB | Verordnung zur Durchführung der Vorschriften über Steuerberater, Steuerbevollmächtigte und Steuerberatungsgesellschaften vom 12. November 1979 (BGBl. I S. 1922) |
| EGGVG | Einführungsgesetz zum Gerichtsverfassungsgesetz in der Fassung des Justizmitteilungsgesetzes (JuMiG) vom 18. Juni 1997 (BGBl. I S. 1430) |
| 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 |
| GewO | Gewerbeordnung |
| GG | Grundgesetz für die Bundesrepublik Deutschland (Grundgesetz) |
| HandwO | Gesetz zur Ordnung des Handwerks (Handwerksordnung) |
| IHK-Gesetz | Gesetz zur vorläufigen Regelung des Rechts der Industrie- und Handelskammern vom 18. Dezember 1956 (BGBl. I S. 920), zuletzt geändert durch Gesetz vom 23. November 1994 (BGBl. I S. 3475) |
| IuKDG | Gesetzes zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste (Informations- und Kommunikationsdienstegesetz - IuKDG) vom 22. Juli 1997 (BGBl. I S. 1870) |
| JGG | Jugendgerichtsgesetz in der Fassung der Bekanntmachung vom 11. Dezember 1974 (BGBl. I S. 3427), zuletzt geändert durch das Verbrechensbekämpfungsgesetz vom 28. Oktober 1994 (BGBl. I S. 3186) |

| | |
|---|---|
| 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) |
| KomWG | Gesetz über die Kommunalwahlen im Freistaat Sachsen (Kommunalwahlgesetz - KomWG) vom 18. Oktober 1993 (GVBl. S. 937), geänd. durch Art. 3 des Gesetzes zur Umsetzung der RL 94/80/EG vom 14. Dezember 1995 (GVBl. S. 414) |
| 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) |
| MHG | Gesetz zur Regelung der Miethöhe vom 18. Dezember 1974 (BGBl. I S. 3603, 3604), zuletzt geändert durch das Gesetz zur Änderung des Gesetzes zur Regelung der Miethöhe vom 15. Dezember 1995 (BGBl I S. 1722) |
| MV | Verordnung über Mitteilungen an die Finanzbehörden durch andere Behörden und öffentlich-rechtliche Rundfunkanstalten (Mitteilungsverordnung) vom 7. September 1993 (BGBl. I S. 1554), zuletzt geändert durch Erste Verordnung zur Änderung der Mitteilungsverordnung vom 19. Dezember 1994 (BGBl. I S. 3848) |
| OWiG | Gesetz über Ordnungswidrigkeiten (Ordnungswidrigkeitengesetz) |
| PAuswG | Gesetz über Personalausweise in der Fassung der Bekanntmachung vom 21. April 1986 (BGBl. I S. 548), zuletzt geändert durch Gesetz vom 30. Juli 1996 (BGBI. I S. 1182) |
| PStG | Personenstandsgesetz |
| RHG | Gesetz über den Rechnungshof des Freistaates Sachsen vom 11. Dezember 1991 (GVBl. S. 409) |
| RVO | Reichsversicherungsordnung |
| SächsArchG | Archivgesetz für den Freistaat Sachsen vom 17. Mai 1993 (GVBl. S. 449) |

| | |
|---|---|
| SächsBeurtVO | Verordnung der Sächsischen Staatsregierung über die dienstliche Beurteilung der Beamten vom 11. Januar 1994 (GVBl. S. 90) |
| SächsBG | Beamtengesetz für den Freistaat Sachsen in der Fassung der Bekanntmachung vom 16. Juni 1994 (GVBl. S. 1153), zuletzt geändert durch Art. 1 des Gesetzes vom 7. April 1997 (GVBl. S. 353) |
| SächsBrandschG | Gesetz über den Brandschutz und die Hilfeleistung der Feuerwehren bei Unglücksfällen und Notständen im Freistaat Sachsen vom 2. Juli 1991 (GVBl. S. 227), zuletzt geändert durch Gesetz vom 19. August 1993 (GVBl. S. 815) |
| 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) |
| SächsGDG | Gesetz über den öffentlichen Gesundheitsdienst im Freistaat Sachsen (Sächsisches Gesundheitsdienstgesetz) vom 11. Dezember 1991 (GVBl. S. 413) |
| SächsGemO | Gemeindeordnung für den Freistaat Sachsen vom 21. April 1993 (GVBl. S. 301), zuletzt geändert durch Gesetz vom 20. Februar 1997 (GVBl. S. 105) |
| SächsHKaG | Gesetz über Berufsausübung, Berufsvertretungen und Berufsgerichtsbarkeit der Ärzte, Zahnärzte, Tierärzte und Apotheker im Freistaat Sachsen (Sächsisches Heilberufekammergesetz) vom 24. Mai 1994 (GVBl. S. 935) |
| SächsKAG | Sächsisches Kommunalabgabengesetz vom 16. Juni 1993 (GVBl. S. 502) |
| SächsKHG | Gesetz zur Neuordnung des Krankenhauswesens (Sächsisches Krankenhausgesetz) vom 19. August 1993 (GVBl. S. 675), zuletzt geändert durch Art. 2 Haushaltbegleitgesetz 1997 vom 12. Dezember 1997 (GVBl. S. 537) |
| SächsMeldDÜVO | Dritte Verordnung des Sächsischen Staatsministeriums des Innern zur Durchführung des Sächsischen Meldegesetzes (Sächsische Meldedaten-Übermittlungsverordnung) vom 10. September 1997 (GVBl. S.557), in der Fassung der Bekanntmachung vom 11. April 1997 (GVBl. 377) |

| | |
|---|---|
| SächsMG | Sächsisches Meldegesetz vom 21. April 1993 (GVBl. S. 353), zuletzt geändert durch § 15 des Gesetzes über die Errichtung der Sächsischen Anstalt für kommunale Datenverarbeitung (SAKDG) vom 15. Juli 1994 (GVBl. S. 1432) |
| SächsPersPaßG | Sächsisches Gesetz über Personalausweise und zur Ausführung des Paßgesetzes vom 19. Mai 1998 (GVBl. S. 198) |
| 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) |
| SächsSchulG | Schulgesetz für den Freistaat Sachsen vom 3. Juli 1991 (GVBl. S. 213), zuletzt geändert durch Gesetz zur Änderung des Schulgesetzes für den Freistaat Sachsen vom 15. Juli 1994 (GVBl. S. 1434) |
| SächsStatG | Sächsisches Statistikgesetz vom 17. Mai 1993 (GVBl. S. 453) |
| SächsStudDatVO | Verordnung des Sächsischen Staatsministeriums für Wissenschaft und Kunst zur Verarbeitung personenbezogener Daten der Studienbewerber, Studenten und Prüfungskandidaten für statistische und Verwaltungszwecke der Hochschulen (Sächsische Studentendatenverordnung) vom 9. Mai 1994 (GVBl. S. 916) |
| SächsSWEG | Gesetz über die Erprobung einer Sächsischen Sicherheitswacht (Sächsisches Sicherheitswachterprobungsgesetz) vom 12. Dezember 1997 (GVBl. S. 647) |
| SächsWG | Sächsisches Wassergesetz vom 23. Februar 1993 (GVBI. S. 201) geändert d. Artikel 5 des Gesetzes vom 4. Juli 1994 (GVBI. S. 1261) |
| SächsVerf | Verfassung des Freistaates Sachsen vom 27. Mai 1992 (GVBl. S. 243) |
| SächsVermG | Sächsisches Vermessungsgesetz in der Fassung der Bekanntmachung vom 2. August 1994 (GVBl. S. 1457) |
| SächsVSG | Gesetz über den Verfassungsschutz im Freistaat Sachsen (Sächsisches Verfassungsschutzgesetz) vom 16. Oktober 1992 (GVBl. S. 459) |

| | |
|---|---|
| SächsVwVG | Sächsisches Verwaltungs-Vollstreckungsgesetz vom 17. Juli 1992 (GVBl. S. 327), geändert durch Erstes Änderungsgesetz vom 24. Oktober 1995 (GVBl. S. 356) |
| SächsWahlG | Gesetz über die Wahlen zum Sächsischen Landtag vom 5. August 1993 (GVBl. S. 723), zuletzt geändert durch Art. 1 des Gesetzes zur Änderung des Sächsischen Wahlgesetzes und des Abgeordnetengesetzes vom 12. Januar 1995 (GVBl. S. 1) |
| SäHO | Vorläufige Haushaltsordnung des Freistaates Sachsen (Vorläufige Sächsische Haushaltsordnung) vom 19. Dezember 1990 (GVBl. S. 21) |
| SchwbAV | Zweite Verordnung zur Durchführung des Schwerbehindertengesetzes (Schwerbehinderten-Ausgleichsabgabeverordnung) vom 28. März 1988 (BGBl. I S. 483), zuletzt geändert durch Art. 29 des Gesetzes zur Reform der gesetzlichen Rentenversicherung vom 16. Dezember 1997 (BGBl. I S. 2998) |
| SchwbG | Gesetz zur Sicherung der Eingliederung Schwerbehinderter in Arbeit, Beruf und Gesellschaft (Schwerbehindertengesetz) in der Neufassung vom 26. August 1986 (BGBl. I S. 421), zuletzt geändert durch Art. 28 des Gesetzes zur Reform der gesetzlichen Rentenversicherung vom 16. Dezember 1997 (BGBl. I S. 2998) |
| 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 3 des Gesetzes zur Reform der gesetzlichen Rentenversicherung vom 16. Dezember 1997 (BGBl. I S. 2998) |
| SGB IV | Sozialgesetzbuch - Gemeinsame Vorschriften für die Sozialversicherung - vom 23. Dezember 1976 (BGBl. I S. 3845), zuletzt geändert durch Art. 4 des Gesetzes zur Reform der gesetzlichen Rentenversicherung vom 16. Dezember 1997 (BGBl. I S. 2998) |
| SGB V | Sozialgesetzbuch - Gesetzliche Krankenversicherung - vom 20. Dezember 1988 (BGBl. I S. 2477), zuletzt geändert durch Artikel 1 des Neunten Gesetzes zur Änderung des Fünften Buches Sozialgesetzbuch vom 8. Mai 1998 (BGBl. I S. 907) |

| | |
|---|---|
| SGB VI | Sozialgesetzbuch - Gesetzliche Rentenversicherung - vom 18. Dezember 1989 (BGBl. I S. 2261, ber. BGBl. 1990 I S. 1337), zuletzt geändert durch Artikel 1 des Gesetzes zur Reform der gesetzlichen Rentenversicherung vom 16. Dezember 1997 (BGBl. I S. 2998) |
| SGB VII | Sozialgesetzbuch - Gesetzliche Unfallversicherung - vom 7. August 1996 (BGBl. I S. 1254), zuletzt geändert durch Artikel 6 des Gesetzes zur Reform der gesetzlichen Rentenversicherung vom 16. Dezember 1997 (BGBl. I S. 2998) |
| SGB VIII | Sozialgesetzbuch - Kinder- und Jugendhilfe - vom 26. Juni 1990 (BGBl. I S. 1163) in der Fassung der Bekanntmachung vom 15. März 1996 (BGBl. I S. 447), zuletzt geändert durch Artikel 13 des Gesetzes zur Reform des Kindschaftsrechts vom 16. Dezember 1997 (BGBl. I S. 2942) |
| SGB X | Sozialgesetzbuch - Verwaltungsverfahren - vom 18. August 1980 (BGBl. I S. 1469) und 4. November 1982 (BGBl. I S. 1450), zuletzt geändert durch Artikel 7 des Ersten Gesetzes zur Änderung des Dritten Buches Sozialgesetzbuch und anderer Gesetze vom 16. Dezember 1997 (BGBl. I S. 2970) |
| SGB XI | Sozialgesetzbuch - Soziale Pflegeversicherung - vom 26. Mai 1994 (BGBl. I S. 1014), zuletzt geändert durch Artikel 7 des Gesetzes zur Reform der gesetzlichen Rentenversicherung vom 16. Dezember 1997 (BGBl. I S. 2998) |
| SHEG | Sächsisches Hochschulerneuerungsgesetz vom 25. Juli 1991 (GVBl. S. 261), zuletzt geändert durch Gesetz vom 31. Juli 1992 (GVBl. S. 401) |
| 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. Juli 1997 (GVBl. S. 353) |
| SOGY | Verordnung des Sächsischen Staatsministeriums für Kultus über allgemeinbildende Gymnasien im Freistaat Sachsen (Schulordnung Gymnasien) vom 15. Dezember 1993 (GVBl. 1994 S. 220) |
| SOGS | Verordnung des Sächsischen Staatsministeriums für Kultus über Grundschulen im Freistaat Sachsen (Schulordnung Grundschulen) vom 2. Mai 1994 (GVBl. S. 1117) |

| | |
|---|---|
| SOMI | Verordnung des Sächsischen Staatsministeriums für Kultus über Mittelschulen im Freistaat Sachsen (Schulordnung Mittelschulen) vom 10. September 1993 (GVBl. S. 879) |
| StBerG | Steuerberatungsgesetz in der Fassung der Bekanntmachung vom 4. November 1975 (BGBl. I S. 2735), zuletzt geändert durch das Jahressteuer-Ergänzungsgesetz 1996 vom 18. Dezember 1995 (BGBl. I S. 1959) |
| StGB | Strafgesetzbuch |
| StPO | Strafprozeßordnung |
| StUG | Gesetz über die Unterlagen des Staatssicherheitsdienstes der ehemaligen Deutschen Demokratischen Republik (Stasi-Unterlagen-Gesetz) vom 20. Dezember 1991 (BGBl. I S. 2272), zuletzt geändert durch Sechstes Gesetz zur Reform des Strafrechts vom 26. Januar 1998 (BGBl. I S. 164, 187) |
| StVO | Straßenverkehrs-Ordnung vom 16. November 1970 (BGBl. I S. 1565, 1971 I S. 38), zuletzt geändert durch Artikel 1 der Verordnung vom 7. August 1997 (BGBl. I S. 2028) |
| StVZO | Straßenverkehrs-Zulassungs-Ordnung |
| SÜG | Gesetz über die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen des Bundes (Sicherheitsüberprüfungsgesetz) vom 20. April 1994 (BGBl. I S. 867) |
| SVermG | Gesetz über die Landesvermessung und das Liegenschaftskataster im Freistaat Sachsen (Sächsisches Vermessungsgesetz) in der Fassung der Bekanntmachung vom 2. August 1994 (GVBl. S. 1457) |
| TDDSG | Gesetz über den Datenschutz bei Telediensten (Teledienstedatenschutzgesetz - TDDSG) vom 22. Juli 1997 (BGBl. I S. 1870) |
| TKG | Telekommunikationsgesetz vom 25. Juli 1996 (BGBl. I S. 1120) |
| TSG | Transsexuellengesetz vom 10. September 1980 (BGBl. I S. 1654) |
| UWG | Gesetz gegen den unlauteren Wettbewerb |
| Verpflichtungs- | Gesetz über die förmliche Verpflichtung nichtbeamteter Perso |

| | |
|---|---|
| gesetz | nen vom 2. März 1974 (BGBl. I S. 469, 545; III 453-17), zuletzt geändert durch Änderungsgesetz vom 15. August 1974 (BGBl. I S. 1942) |
| VerpflVO | Verordnung der Sächsischen Staatsregierung über Zuständigkeiten nach dem Gesetz über die förmliche Verpflichtung nichtbeamteter Personen vom 29. Oktober 1993 (GVBl. S. 1041) |
| VwVfG | Verwaltungsverfahrensgesetz |

*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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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) |
| 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 |
| SML | Sächsisches Staatsministerium für Landwirtschaft, Ernährung und Forsten |
| SMS | Sächsisches Staatsministerium für Soziales, Gesundheit und Familie |
| SMU | Sächsisches Staatsministerium für Umwelt und Landesentwicklung |
| SMWA | Sächsisches Staatsministerium für Wirtschaft und Arbeit |
| SMWK | Sächsisches Staatsministerium für Wissenschaft und Kunst |
| SSG | Sächsischer Städte- und Gemeindetag e. V. |
| StUFA | Staatliches Umweltfachamt |
| TB | Tätigkeitsbericht |
| TCP/IP | Transmission control protocol/Internet protocol |
| TdL | Tarifgemeinschaft deutscher Länder |
| THA | Treuhandanstalt |
| TK-Anlage | Telekommunikationsanlage |
| 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

Am 13. November 1997 bin ich vom Sächsischen Landtag in das Amt des Sächsischen Datenschutzbeauftragten wiedergewählt worden. Von 111 anwesenden Landtagsabgeordneten haben mir 98 ihre Stimme gegeben. Dieser große Vertrauensbeweis ist für meine Mitarbeiter und mich Ansporn, die Fahne des Grundrechtes auf informationelle Selbstbestimmung auch künftig in Sachsen hochzuhalten.

Der nun vorgelegte Tätigkeitsbericht spricht in seiner Fülle und Komplexität für sich. Er zeigt, daß es kaum einen Verwaltungsbereich gibt, in dem Datenschutz keine Rolle spielt. Er zeigt aber auch, daß das Problembewußtsein der öffentlichen Stellen in Sachsen, also unserer Beratungs- und Kontrollpartner, sich kontinuierlich schärft, also verbessert.

In den letzten Wochen hat mir allerdings ein Text Sorgen bereitet, der anläßlich einer „Aschermittwochsveranstaltung“ durch einen Sächsischen Staatsminister wie folgt formuliert wurde:

*„Was nützt uns die schönste politische Debatte, die ja ein Ausdruck der freiheitlichen Gesellschaft ist, wenn die Politik bei jedem Entscheidungsschritt von Verfassungsrichtern, Verwaltungsrichtern, Arbeitsrichtern und Datenschutzbeauftragten umlauert ist. Wer ständig davor zittern muß, daß ein Richter in der zu entscheidenden Sache anderer Auffassung ist, fragt sich natürlich, ob er überhaupt noch etwas entscheiden soll. Was ist das für ein Land, in dem - wie erst vor wenigen Jahren in Bonn geschehen - Minister zum Verfassungsgericht nach Karlsruhe laufen, um ihren politischen Konflikt zu lösen.*

*Ein solches Land ist weder handlungs- noch reformfähig und wenn wir so weiter machen, fahren wir frontal gegen die Wand. Und die versammelten Richter werden uns dann erklären, daß ihnen das ja auch furchtbar leid tue, aber das geltende Gesetz hätte sie gezwungen, so zu handeln. Das ist zwar nicht die reine Wahrheit, denn in einigen Fällen war es schlicht richterliche Anmaßung gepaart mit Ideologie oder grenzenloser Inkompetenz, die die politische Handlungsfähigkeit blockierte. Und wem das bisher noch nicht klar war, dem müßte es spätestens bei dem blamablen Elfmeterschießen der deutschen Verwaltungsgerichte in Sachen Rechtsschreibreform* (so im Original, d. V.) *aufgegangen sein.*

*Aber ich will akzeptieren, daß der Gesetzgeber und damit die Politik das größere Maß Schuld trägt. Die Politik muß durch entsprechende gesetzliche Schritte für sich selbst und für die Verwaltung wieder größere Handlungsräume schaffen, zugleich aber dafür sorgen, daß diese Handlungen dann transparent sind und der öffentlichen Debatte unterliegen. Und sie muß den Einzelnen dazu bringen, Freiheit als Einheit von Chance und Risiko zu begreifen und deshalb mehr persönliche Verantwortung zu akzeptieren. Und Sie, liebe Mitbürgerinnen und Mitbürger, müssen auf eine solche Politik setzen, auch wenn sie keine goldenen Berge oder rosaroten Zeiten verspricht.“*

Was will dieser Autor? Er will „die Politik“ (was immer er sich darunter vorstellt) von richterlicher und datenschutzrechtlicher Kontrolle befreien. Er fühlt sich „umlauert“; dies ist ein böses Wort. Er meint, ein Land, in dem das Recht vor der Politik steht, „fahre frontal gegen die Wand“. Die Richter seien (in einigen Fällen) anmaßend und inkompetent. Die politische Handlungsfähigkeit werde von Richtern und Datenschutzbeauftragten blockiert. Die Politik müsse „durch entsprechende gesetzliche Schritte für die Verwaltung größere Handlungsräume schaffen“.

Auf den ersten Blick hört sich das schön an. Da ist ein starker Mann, der was schaffen will, der endlich loslegen will, und dann kommen die Bedenkenträger, die Juristen. Unser Minister will sich von der Enge der allenthalben behindernden Rechtsvorschriften befreien.

Seine Grundauffassung kann ich prinzipiell nicht teilen:

In der Tat muß im Rechtsstaat der Politiker sich mit aller Selbstverständlichkeit gefallen lassen, daß ein Richter oder ein Datenschutzbeauftragter in der zu entscheidenden Sache anderer Auffassung als die Exekutive ist. Ich stehe zu diesem Rechtsstaat; von jedem Amtsträger, auch von dem, der schon vor der friedlichen Revolution öffentliche Verantwortung getragen hat, muß heute erwartet werden, daß er sich in den Dienst dieses Rechtsstaates stellt und Kontrollkompetenzen der Richter und der Datenschutzbeauftragten akzeptiert. Gott behüte uns vor solchen Politikern, die ihre Handlungen nicht in jedem einzelnen Streitfall von Unabhängigen kontrolliert sehen wollen. Gustav Stresemann hat das schon 1929 auf der Haager Konferenz so formuliert: „Recht steht vor Politik und niemals umgekehrt.“

Wer die Verfassung studiert, wird feststellen, daß sie - insbesondere im Bereich der Wirtschaft, aber auch im Bereich der Kultur - große Freiräume öffnet. Aber auch dort, wo die Verfassung uns engere Grenzen setzt, kann der *Gesetzgeber* (unter Wahrung des Kernbereichs unserer Grundrechte und im Rahmen der Verhältnismäßigkeit) moderne Ideen entwickeln. Aber die *Verwaltung* steht vollkommen unter dem Gesetz. So ist es gewollt. Das will die parlamentarische Demokratie.

Gerichtliche Prozesse, aber auch datenschutzrechtliche Beratungen und Kontrollen sind keine deterministischen Vorgänge, denn auch unter korrekter Anwendung der Normen können Datenschutzbeauftragte oder Richter am Ende ihres Nachdenkens zu unterschiedlichen Auffassungen gelangen. Ihre Entscheidungen dennoch zu akzeptieren wird von Ministern als Amtspflicht, ja sogar von jedem Rechtsunterworfenen als Bürgerpflicht verlangt.

Was rechtens, was gerecht ist, haben in Deutschland die Richter zu entscheiden; in ähnlicher Unabhängigkeit haben Datenschutzbeauftragte die öffentlichen Stellen zu beraten und zu kontrollieren, ob sie mit Informationen über Menschen richtig, d. h. dem Gesetz entsprechend, umgehen. Der Sächsische Datenschutzbeauftragte ist dazu von der Verfassung berufen.

Wir leben in einem Rechtsstaat, also in einem Gemeinwesen, das sich in allen wesentlichen Fragen dem Recht verbunden und unter das Recht gestellt hat. Deswegen begrenzt das Recht die Politik allenthalben. Oder anders gesagt: Politische Angelegenheiten sind fast immer Rechtsangelegenheiten. Es gibt nämlich keine wesentliche politische Entscheidung, die nicht auf dem Boden der Verfassungsordnung erwächst oder Einfluß auf das Recht nimmt. Politik spielt sich in den Parlamenten, also den Orten der verfassungsrechtlich begrenzten Rechtsetzung und in den Kabinetten ab, die die Verwaltung leiten, die ihrerseits ausschließlich an das Recht gebunden ist. Dies will der Grundsatz der Gesetzmäßigkeit der Verwaltung, ein Prinzip jeden Rechtsstaates.

Und jedermann steht unumstößlich das Recht zu, jede ihn persönlich rechtlich belastende obrigkeitliche - wenn man so will auch politische - Entscheidung vor Gericht anzufechten (Art. 19 Abs. 4 GG).

Wo also sieht der zitierte Minister einen breiten Raum für die Politik, ohne ihren engen und allgegenwärtigen Bezug zum Recht? Bezeichnenderweise wird er nicht konkret.

Bei Personalentscheidungen im öffentlichen Dienst sowie bei der Herstellung geeigneter und das Subsidiaritätsprinzip unangetastet lassender Rahmen- und Arbeitsbedingungen in unseren Hierarchieebenen stehen unsere Minister unter dem Gesetz wie jeder Mitarbeiter im öffentlichen Dienst. Seit der Antike lautet die entscheidende staatsrechtliche und folglich wichtigste politische Frage: Wie finde ich einen Herrscher, der sich unter das Gesetz stellt?

In Art. 20 Abs. 3 des Grundgesetzes und gleichlautend in Art. 3 Abs. 3 der Sächsischen Verfassung heißt es deshalb: „Die Gesetzgebung ist an die verfassungsmäßige Ordnung, die vollziehende Gewalt und die Rechtsprechung sind an Gesetz und Recht gebunden.“ So klar, so einfach und so unüberwindlich stark. Ein Gedanke übrigens, der in Großbritannien schon lange zu Hause ist: „Wo das Gesetz aufhört, da beginnt die Tyrannei“ (William Pitt d. Ä., Reden, 1770).

Einige Kontrollvorgänge, die ich vor mir liegen sehe, lassen befürchten, daß datenschutzrechtlich geordnete, d. h. gesetzlichen Verfahrensregelungen entsprechende Datenverarbeitungsvorgänge durch gesetzlich nicht legitimierte, eben politische Einflüsse „von oben“ bestimmt werden. Derartigen Entwicklungen werde ich beratend und kontrollierend entgegenzuwirken versuchen.

Der Schutz unserer Privatsphäre vor einem neugierigen und mächtigen Staatsapparat ist meine vornehmste Pflicht; diese Form einer Machtbegrenzung und Machtkontrolle ist Aufgabe des Sächsischen Landtages, den ich bei seiner parlamentarischen Kontrolle mit meinen Kolleginnen und Kollegen zu unterstützen habe.

Ich hoffe, daß mir dies auch in Zukunft gelingen möge. Dabei hilft mir jeder Bürger, der sich an mich wendet, jeder Mitarbeiter im öffentlichen Dienst, der mich auf

Mißstände oder offene Probleme aufmerksam macht. Aber mir hilft auch jeder Behördenleiter, der die Privatsphäre der Sachsen respektiert und den Widerstreit zwischen Gemeinschaftsbezogenheit und persönlicher Freiheit als Problem erkennt.

Jedenfalls ist „die Politik“ keine verfassungsrechtliche Größe, die einen Freiraum außerhalb des Rechts für sich beanspruchen darf. Jeder Tendenz, die eine solche „absolute Politik“ wünscht, gilt es nach wie vor entschieden zu begegnen.

# 3 Europäische Union/Europäische Gemeinschaft

## Umsetzung der EG-Datenschutzrichtlinie in deutsches Recht

In meinem 5. Tätigkeitsbericht habe ich in Kapitel 1 darüber berichtet, daß die Europäische Richtlinie zum Datenschutz vom 24. Juli 1995 verbindlich vorschreibt, das deutsche Datenschutzrecht bis zum Herbst 1998 entsprechend den Vorgaben der Richtlinie zu ändern. Zwar hat das Bundesministerium des Innern (BMI) mittlerweile einen Referentenentwurf zur Novellierung des BDSG vorgelegt, aber ein zwischen den einzelnen Ressorts abgestimmter Regierungsentwurf liegt bislang noch nicht vor. Vor diesem Hintergrund erscheint eine fristgerechte Umsetzung der Richtlinie in nationales Recht eher zweifelhaft, zumal die Legislaturperiode des Bundestages im September 1998 endet.

Der Referentenentwurf des BMI berücksichtigt wesentliche Grundentscheidungen der Richtlinie nicht in ausreichendem Maße. Defizite gibt es vor allem in der Umsetzung des aus meiner Sicht zentralen Artikels 28 Abs. 1, der vorschreibt, daß die Datenschutzkontrollbehörde auch im privaten Bereich ihre Aufgaben in „völliger Unabhängigkeit“ erfüllen muß. Der Entwurf geht dagegen wie bisher von einem Weisungsrecht der Obersten Landesbehörde gegenüber den als Datenschutzkontrollbehörden fungierenden Aufsichtsbehörden für den privaten Bereich aus. Da die bloße Unabhängigkeit von den kontrollierten Stellen selbstverständlich ist, muß ernsthaft bezweifelt werden, ob ein derartiges Weisungsrecht mit der von der Richtlinie geforderten völligen Unabhängigkeit der Kontrollbehörden vereinbar ist.

Mit Artikel 28 der Richtlinie hat die Gemeinschaft die ihr zustehende Kompetenz wahrgenommen, die Rechtsstellung, die Aufgaben und die Befugnisse einer wirksamen Datenschutzkontrollbehörde in verbindlicher Weise für alle Mitglieder vorzugeben. Mit der völligen Unabhängigkeit ist nach dem Text der Vorschrift zwar keine völlige organisatorische Unabhängigkeit, wohl aber eine Freiheit von sachlichen Weisungen gemeint. Nach meiner Überzeugung ist eine von der Verwaltung unabhängige Kontrolle die wichtigste Voraussetzung, um das Grundrecht auf informationelle Selbstbestimmung zu gewährleisten. Die leidvolle Erfahrung fehlender Gewaltenteilung und Kontrolle staatlichen Handelns in der DDR muß gerade hierorts dazu

führen, sich für die völlige Unabhängigkeit der Datenschutzkontrolle einzusetzen. Ich halte es deshalb für unabdingbar, daß die Novellierung des BDSG jedwede Einbindung der Kontrollinstanzen in ministerielle Weisungsstränge ausschließt. In diesem Zusammenhang ist es auch sinnvoll, daß die Richtlinie nicht zwischen öffentlichem und privatem Bereich unterscheidet. Dies bedeutet freilich, daß im Zuge der Umsetzung in deutsches Recht die weisungsabhängigen Datenschutzkontrollbehörden abgeschafft werden müssen und auch der private Bereich der Kontrolle durch unabhängige Datenschutzbeauftragte zu unterstellen ist.

Eng verknüpft mit der Frage der Unabhängigkeit ist die Vorgabe in Art. 28 Abs. 3, derzufolge den Kontrollstellen wirksame Einwirkungsbefugnisse, wie etwa veröffentlichte Stellungnahmen, Anordnungsrechte, Verwarnungs- und Ermahnungsbefugnisse oder Klagerecht zustehen müssen. Auch hier weist der bis jetzt vorliegende Entwurf des BMI leider noch Defizite auf. Das gegenwärtig in den Datenschutzgesetzen verankerte Beanstandungsrecht bietet insofern keinen Ausgleich, da es im Streitfall nicht durchsetzbar ist. Ich räume ein, daß in den allermeisten Fällen die Beanstandung Beachtung findet, da die Exekutive ihr Verhalten umstellt. Dies ändert aber nichts daran, daß durchsetzbare Einwirkungsbefugnisse für einen wirklich effektiven Datenschutz konstitutiv sind, da Beanstandungen eben gelegentlich auch nicht umgesetzt werden.

Eine so verstandene Entscheidungskompetenz ist auch mit der Unabhängigkeit der Kontrollstellen vereinbar: Ministerialfreie Räume auf dem Gebiet der Verwaltung sind nach der Rechtsprechung nicht schon von vornherein ausgeschlossen. Zwar dürfen Regierungsaufgaben mit politischer Tragweite nicht auf Stellen übertragen werden, die von Regierung und Parlament unabhängig sind. Dies trifft aber auf die Datenschutzbeauftragten nicht zu, da diese vom Parlament auf Zeit gewählt und von ihm auch parlamentarisch kontrolliert werden (wie etwa über den Haushalt, Anfragen oder Berichtspflichten). Die Richtlinie bleibt also nicht bei der bisherigen Beanstandung als der schärfsten Sanktion stehen, bei der keine justitielle Kontrolle stattfindet, sondern geht darüber hinaus. Konsequenterweise ordnet sie in Art. 28 Abs. 3 an, daß „gegen beschwerende Entscheidungen der Kontrollstelle der Rechtsweg offensteht“.

Eine weitere Vorgabe der Richtlinie, nämlich Art. 28 Abs. 2, ordnet an, daß die Kontrollstellen bei der Ausarbeitung von Rechtsverordnungen oder Verwaltungsvorschriften auf dem Gebiet des Datenschutzes angehört werden. Auch nach der Rechtsprechung des Bundesverfassungsgerichts ist es für einen effektiven Schutz des Rechts auf informationelle Selbstbestimmung von hoher Bedeutung, daß der Gesetzgeber rechtzeitige Vorkehrungen zur Beteiligung unabhängiger Datenschutzbeauftragter bei der einschlägigen Rechtsetzung trifft. Notwendig ist deshalb, im Zuge der Novellierung des Deutschen Datenschutzrechts insbesondere in den Geschäftsordnungen der Regierungen und der Parlamente entsprechende Regelungen zu treffen. Diese sollten darauf abzielen, die Datenschutzbeauftragten frühzeitig von Normsetzungsverfahren zu informieren und immer dann zur Beratung hinzuzuziehen, wenn die Verarbeitung personenbezogener Daten erörtert wird. Eine solche Beratung kann freilich nur dann Erfolg haben, wenn sie positive Empfehlungen und konkrete Lösungen anbietet.

Im Interesse einer unabhängigen und effektiven Kontrolle sollten die angesprochenen Grundsatzentscheidungen der EG-Datenschutzrichtlinie daher sobald wie möglich in deutsches Recht umgesetzt werden. Dies würde den Ländern auch die bislang fehlende Orientierung geben, die für die Anpassung ihrer Landesdatenschutzgesetze notwendig ist. Die in meiner Behörde eingesetzte Arbeitsgruppe zur Novellierung des Sächsischen Datenschutzgesetzes hat das Ergebnis ihrer Beratungen dem SMI zugeleitet. Ich habe die Erwartung, daß wesentliche Teile meiner Empfehlungen in den Entwurf der Staatsregierung zur Novellierung des Sächsischen Datenschutzgesetzes einfließen werden.

# 5 Inneres

## 5.1 Personalwesen

### 5.1.1 Verwaltungsvorschrift zur Begründung und Beendigung des Beamtenverhältnisses - Personalbogen des SMI und des SMJus

Am Entwurf der o. g. Verwaltungsvorschrift (vom 11. August 1997 - SächsABl. S. 1060) hat mich das SMI rechtzeitig beteiligt. Meine Stellungnahme dazu und insbesondere mein Drängen auf die Verwendung eines datenschutzgerechten Personalbogens (vgl. 4/5.1.7) haben bewirkt, daß datenschutzrechtliche Defizite erkannt und beseitigt wurden.

So bestanden bislang erhebliche Unsicherheiten bei der Handhabung von Bewerberunterlagen, insbesondere *wann* Unterlagen von Bewerbern, die bei der Einstellung nicht berücksichtigt wurden, zurückzugeben sind (Kontrollen in Personalstellen der öffentlichen Verwaltung haben das immer wieder bestätigt). In Nr. 1.9 der Verwaltungsvorschrift ist jetzt eine klare datenschutzgerechte Regelung enthalten, nämlich daß die Unterlagen *unverzüglich* zurückzugeben und etwaige gefertigte Fotokopien, ärztliche Zeugnisse, der Personalbogen, das vorgelegte Führungszeugnis oder eine eingeholte unbeschränkte Auskunft aus dem Zentralregister zu vernichten sind. Auch die in automatisierten Dateien gespeicherten Bewerberdaten sind mit der Rückgabe der Bewerbungsunterlagen (also unverzüglich), spätestens jedoch nach sechs Monaten zu löschen. Eine andere Verfahrensweise ist allerdings mit ausdrücklicher Zustimmung des Bewerbers zulässig.

Mit der Anlage 1 zu Nr. 1.1 der o. g. Verwaltungsvorschrift wird den Personalstellen in den sächsischen Behörden (gemäß Nr. 11 auch den Gemeinden, den Landkreisen und den sonstigen der Aufsicht des Freistaates Sachsen unterstehenden Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts) ein datenschutzgerechter Personalbogen *zur Anwendung empfohlen* (siehe auch Materialien Nr. 16.2.1). Die wesentlichen Änderungen gegenüber dem bisherigen Personalbogen spreche ich hier nochmals an:

- Die Angaben von *früheren Vornamen* (Feldnummer 3) würde dem Ausforschungsverbot des § 5 Transsexuellengesetz widersprechen. Deshalb wurde die Fußnote Nr. 2 auf *frühere Familiennamen* (Feldnummer 2) beschränkt.
- Auf das Erheben der *Ehegattendaten* (Feldnummer 10) wurde verzichtet. Auch der Hinweis auf die Freiwilligkeit kann die Beachtung des (verfassungsrechtlichen) Grundsatzes der Erforderlichkeit nicht ersetzen.
- Das Erheben der Kinderdaten (Feldnummer 11) ist nur erforderlich und zulässig, sofern die Kinder noch im Haushalt des Bewerbers/Bediensteten leben und soweit sich die Angaben auf Kindergeld und Familienzuschlag auswirken (neue Fußnote 4).

Besonderheiten der einzelnen Ressorts können zu einer Änderung oder Erweiterung des Datenkataloges führen. Beispielsweise sieht der vom SMJus entwickelte Personalbogen für Beamte, Richter, Angestellte und Arbeiter Angaben zu Namen und Beruf des Ehegatten dann vor, wenn Befangenheitsrisiken bestehen, wenn also der

Ehegatte Richter, Staatsanwalt oder Rechtsanwalt ist (Beispiel: In einem Prozeß stehen sich beide Ehegatten als Richter und Staatsanwalt oder Rechtsanwalt gegenüber). Der Inhalt des SMJus-Personalbogens bedarf noch weiterer Erörterung.

### 5.1.2 Richtlinie der Bereitschaftspolizei Sachsen zur Führung von Beurteilungsunterlagen und zur Erstellung von Beurteilungen für Polizeivollzugsbeamte

Die Richtlinie sieht unter anderem folgendes vor:

*„Um den Ansprüchen einer gerechten Leistungsbewertung über Mitarbeiter in Form von Beurteilungen gerecht werden zu können, sind fortlaufend schriftliche Aufzeichnungen über die Arbeitsergebnisse und die Verhaltensweisen der zu Beurteilenden zu führen.*
*Zu diesem Zweck sind anlaßbezogen und/oder in Zeitintervallen von längstens neun Monaten ab Beurteilungsstichtag Leistungsnotizen in schriftlicher Form mit konkreten Aussagen über das Leistungsverhalten und die Befähigung des zu Beurteilenden zu fertigen und aufzubewahren.*
*Soweit diese für den zu Beurteilenden negative Aussagen beinhalten, sind die Leistungsnotizen zeitnah zum Ereignis zu eröffnen, damit der Betroffene dazu Stellung beziehen kann. Mündlich vorgetragene Remonstrationen sind in einem Aktenvermerk festzuhalten und ebenso wie schriftliche Äußerungen des Betroffenen zu den Beurteilungsakten zu nehmen. Werden berechtigte Einwände erhoben, ist diesen nachweislich abzuhelfen. Ist eine Abhilfe nicht möglich oder nicht angezeigt, so sind die Gründe hierfür ebenfalls schriftlich zu den Beurteilungsunterlagen zu nehmen.*
*Alle im Zusammenhang mit Beurteilungen gefertigten Aufzeichnungen sind vertrauliche Personalangelegenheiten und sind dementsprechend gegen unbefugten Zugriff zu sichern. Dies gilt sowohl für personengebundene Unterlagen als auch für Listen, die zu Vergleichszwecken angelegt werden.*
*Die Beurteilungsunterlagen sind von Beurteilern in Beurteilungsakten zusammenzuführen. Die Beurteilungsakten über Beamte des höheren Dienstes werden beim Präsidium der Bereitschaftspolizei Sachsen geführt."*

Sowohl dem SMI als auch dem Präsidium der Bereitschaftpolizei habe ich mitgeteilt, daß das Präsidium der Bereitschaftspolizei im Hinblick auf Art. 75 Abs. 2 SächsVerf, § 115 Abs. 1 Satz 3 SächsBG, wonach die obersten Dienstbehörden (nicht also das Präsidium der Bereitschaftspolizei) die Einzelheiten der Beurteilung für ihren Dienstbereich bestimmen, für einen Erlaß dieser Art nicht zuständig sein dürfte und sich die Richtlinie im übrigen nicht mit den geltenden Vorschriften des SächsBG über die Personalaktenführung (insbesondere §§ 117 ff. i. V. m. der Verwaltungsvorschrift des SMI über die Führung und Verwaltung von Personalakten vom 4. November 1993) sowie der SächsBeurtVO vereinbaren läßt.

Die Anfertigung kontinuierlicher Beurteilungsunterlagen über Leistung und Verhalten der Beamten ist zwar nach der Rechtsprechung (z. B. BVerwG-Urteil v. 2.4.1981 - 2 C 34.79, Beschl. d. I. Wehrdienstsenats v. 10.9.1967, I WB 19.68) - zumindest in größeren Behörden - nicht generell unzulässig. Lückenlose Leistungs- und

Verhaltenskontrolle ist jedoch geeignet, ständigen Überwachungsdruck auf die Vollzugsbeamten auszuüben und greift deshalb m. E. unter Mißachtung des Übermaßverbots und der einschlägigen Gesetze, Verordnungen und Verwaltungsvorschriften in unverhältnismäßiger Weise in deren Persönlichkeitsrecht ein.

Ich stehe auf dem Standpunkt, daß schriftliche Aufzeichnungen über besondere Vorkommnisse negativer oder positiver Natur, wie von der Bereitschaftspolizei vorgesehen, unter Beachtung der §§ 117 ff. SächsBG unverzüglich in die Personalakte aufgenommen werden müssen, da ein unmittelbarer innerer Zusammenhang mit dem Dienstverhältnis besteht. Die Personalakte wird aber von der personalverwaltenden Stelle und nicht von den Beurteilern geführt. Eine zweite (verkürzte) Personalakte im Schreibtisch der Vorgesetzten darf nicht entstehen.

Die Angelegenheit ist noch nicht abgeschlossen.

### 5.1.3 Automatisierte Verarbeitung von Beschäftigtendaten - § 31 Abs. 7 SächsDSG

Wie in den Vorjahren wurde ich gemäß § 31 Abs. 7 SächsDSG an der Einführung vieler Verfahren der automatisierten Verarbeitung von Beschäftigtendaten beteiligt (insbesondere Verfahren der automatisierten Arbeitszeiterfassung und zu Personalinformations- und Personalverwaltungssystemen).

Häufig fehlten in den Verfahrensbeschreibungen, die Bestandteil der Dienstvereinbarung sind, Angaben zu technischen Details. Wird zum Beispiel das Betriebssystem MS-DOS eingesetzt, können die Mindestanforderungen des Datenschutzes nur mit zusätzlichen Sicherheitsvorkehrungen erreicht werden (vgl. 2/14.1.1). Außerdem darf der speicherungsfähige Datensatz nur die zur Aufgabenerfüllung *erforderlichen* personenbezogenen Daten enthalten. Zum Beispiel ist die Speicherung des *Geburtsdatums, der Wohnanschrift und der privaten Telefonnummer* für Zwecke der Arbeitszeiterfassung nicht erforderlich.
Wenn das gemäß § 9 SächsDSG zu erstellende Datenschutz- und Datensicherheitskonzept fehlte oder die darin festzulegenden Maßnahmen für den Schutz der verarbeiteten personenbezogenen Daten unzureichend waren, habe ich als Hilfestellung auf sogenannte „Musterkonzeptionen“ verwiesen, aber gleichzeitig zu bedenken gegeben, daß sich das „eigene Verfahren“ immer an den tatsächlichen Gegebenheiten, insbesondere an der eigenen Verfahrensorganisation, orientieren muß. Es ist wichtig, daß die einzelnen Maßnahmen nicht losgelöst nebeneinander stehen, sondern in ihrer Gesamtheit zu einem abgestimmten und lückenlosen Datensicherheitskonzept führen müssen. Nur so kann die Umsetzung der Maßnahmen nach § 9 SächsDSG sichergestellt werden.

Allgemein sei darauf hingewiesen, daß die automatisierte Verarbeitung von Beschäftigtendaten ohne meine gesetzlich vorgeschriebene *vorherige* Beteiligung (und auch bei *fehlender* Mitbestimmung) rechtswidrig ist. Außerdem kann ich meinem Beratungs- und Kontrollauftrag gemäß § 24 SächsDSG nicht nachkommen. Unangemessene Entscheidungsverzögerungen sind die Folge.

### 5.1.4 Einführung des Verfahrens „Automatisierte Beihilfebearbeitung (ABBA)“ im Landesamt für Finanzen

Es ist beabsichtigt, das Verfahren, nach einer kurzen Pilotphase, im Laufe des Jahres einzusetzen.

Dem SMF habe ich mitgeteilt, daß der speicherungsfähige Datensatz (Stammdaten), der keine Diagnosedaten enthält, datenschutzrechtlich nicht zu beanstanden ist. Aus der Feldbezeichnung *Stammdatenverarbeitung* der Leistungsbeschreibung ist ersichtlich, daß eine Verknüpfung von Beihilfe- und Bezügedaten nicht erfolgt (§ 124 Abs. 2 SächsBG). Allerdings habe ich zu bedenken gegeben, daß die Bezeichnung des Eingabefeldes *Personalaktenzeichen* in der Leistungsbeschreibung mißverständlich sei; besser wäre die Bezeichnung *Beihilfeaktenzeichen.* Damit würde der personalaktenrechtlichen Vorschrift, Unterlagen über Beihilfen stets als Teilakte zu führen und von der übrigen Personalakte getrennt aufzubewahren, entsprochen (vgl. §§ 118, 124 Abs. 2 SächsBG).
Ich habe auch angeregt, entweder auf das *Bemerkungsfeld* in der Eingabemaske zu verzichten oder für die Eintragungen feste Vorgaben zu definieren. Sogenannte Freitextfelder bergen die Gefahr, daß zur Aufgabenerfüllung nicht erforderliche Eintragungen vorgenommen werden. Dies ist insbesondere im Beihilfebereich wegen der Sensibilität der zu verarbeitenden Daten von besonderer Bedeutung.
Die nach der Verfahrensbeschreibung getroffenen Maßnahmen gemäß § 9 SächsDSG sind nach meinem Dafürhalten nicht ausreichend. Ich habe angeregt, in einem Datenschutz- und Datensicherheitskonzept die Maßnahmen (detailliert) zu regeln, die für den Schutz der zu verarbeitenden Beihilfedaten (Personalaktendaten) geeignet, angemessen und erforderlich sind. Dabei sollten insbesondere die Paßwort- und Rechteverwaltung, Zahl der Anmeldefehlversuche, Schutz der Diskettenlaufwerke, räumliche Sicherheit des Servers, Abschottung der automatisierten Beihilfebearbeitung im Netz, Protokollierung, Aufbewahrungs- und Löschungsfristen Bestandteil des Datenschutz- und Datensicherheitskonzeptes sein. Auf die Führung des erforderlichen Dateien- und Geräteverzeichnisses gemäß § 10 SächsDSG habe ich hingewiesen.
Verfahrensmodifikationen und Programmanpassungen an sächsische Bedingungen (z. B. nach der Pilotphase), Erweiterungen des Verfahrens (z. B. Anwendung der Version 2.0.0) und ggf. die optionale Online-Einbindung der Vorprüfungsstelle in das „ABBA-Verfahren“ (die lt. SMF für die sächsische Version nicht vorgesehen ist), erfordern die erneute Beteiligung des Sächsischen Datenschutzbeauftragten.

Die Übersendung des Datenschutz- und Datensicherheitskonzeptes soll in allernächster Zeit erfolgen. Die Information über den Abschluß der Pilotphase und die Aufnahme des „Dauerbetriebes“ stehen noch aus.

### 5.1.5 Bewerbungsbogen für die Bestellung von Bürgern zu Angehörigen der Sächsischen Sicherheitswacht

Das SMI hat mich an der Erarbeitung eines Bewerbungsbogens beteiligt. Grundlage war ein im Freistaat Bayern verwendeter Erhebungsbogen, mit dem jedoch weit mehr Daten als erforderlich abgefragt werden.

Meine datenschutzrechtlichen Änderungsvorschläge, die zum „Abspecken“ des Fragenkatalogs führten, wurden sämtlich berücksichtigt, so daß der in Sachsen verwendete Bewerbungsbogen datenschutzgerecht ist (siehe Materialien, Nr. 16.2.2).

### 5.1.6 Beschäftigtendatenerhebung anläßlich der Neuordnung der Schulaufsicht

Die sächsische Schulaufsicht soll ab 1. Januar 1999 neu geordnet werden. Anstelle der bisherigen drei Oberschulämter und der zwanzig Schulämter soll es dann fünf Regionalschulämter geben.

Um die damit zusammenhängenden Personalmaßnahmen sowie die Wünsche und Vorstellungen der Beschäftigten auch aus Sicht des Datenschutzes koordinieren zu können, hat mich das SMK frühzeitig an den beabsichtigten Maßnahmen beteiligt. Mit einem Erfassungsbogen sollen alle Betroffenen auf freiwilliger Basis gefragt werden, welche Einsatzwünsche hinsichtlich Dienstort und künftiger Tätigkeit (z. B. erforderliche Qualifikationsmaßnahmen für ein neues Aufgabenfeld oder Rückversetzung in den Schuldienst) bestehen. Die Auswertung soll automatisiert erfolgen.

Im Hinblick auf die in § 117 Abs. 4 SächsBG, § 31 Abs. 1 SächsDSG festgelegte Befugnis, Beschäftigtendaten auch zur Durchführung organisatorischer, personeller und sozialer Maßnahmen, insbesondere auch zu Zwecken der Personalplanung und des Personaleinsatzes zu erheben, sowie auf die vorgesehene Freiwilligkeit, habe ich keine datenschutzrechtlichen Bedenken geäußert.

### 5.1.7 Erfassung von Ausfallzeiten der sächsischen Landesbediensteten

Durch Kabinettsbeschluß wurden die obersten Landesbehörden, die nachgeordneten Behörden und die Staatsbetriebe angewiesen, kontinuierlich die Fehlzeiten ihrer Beschäftigten zu erfassen und statistisch auszuwerten. Da die Erhebung differenziert nach Vergütungsgruppen, der Dauer und dem Grund der Ausfallzeit (Krankheit, Urlaub, Kur u. a.) erfolgt, fürchteten einige Personalräte aus dem Bereich des SMK, daß insbesondere an kleinen Schulen, an denen beispielsweise in der Regel nur ein Mitarbeiter verbeamtet ist, ein Personenbezug leicht herzustellen sei.

Weil ausschließlich Beschäftigtendaten verwendet werden, die den Dienststellen ohnehin (rechtmäßig) zur Verfügung stehen, hatte ich gegen deren Auswertung für eine Statistik im Verwaltungsvollzug (§§ 12 Abs. 3 Satz 1 SächsDSG, 7 Abs. 1 SächsStatG) keine durchgreifenden Bedenken. Selbst wenn in Einzelfällen ein Personenbezug herstellbar sein sollte, wäre die Datenübermittlung durch §§ 121 Abs. 1 SächsBG, 31 Abs. 1 SächsDSG gedeckt. Danach ist die Weitergabe von Personalaktendaten an die oberste Dienstbehörde oder an eine im Rahmen der Dienstaufsicht weisungsbefugte Behörde für Zwecke der Personalverwaltung und Personalwirtschaft auch ohne Einwilligung der Betroffenen zulässig.
Ich habe festgestellt, daß dem Gebot der frühestmöglichen Anonymisierung durch die Schulämter und Oberschulämter entsprochen wurde. Auch hat das SMK niemals erwogen, die Daten in die LPDK des SMK aufzunehmen. Grund für die Erhebung war allein die Aufforderung zur Berichterstattung aller Staatsministerien an die SK.

### 5.1.8 Erhebung von Anamnesedaten im Zusammenhang mit Bildschirmarbeitsplatzuntersuchungen

Aus der Bildschirmarbeitsverordnung vom 4. Dezember 1996 (BGBl. I 1996, S. 1841) sowie aus § 4 des Tarifvertrages über die Arbeitsbedingungen von Arbeitnehmern auf Arbeitsplätzen mit Geräten der Informations- und Kommunikationstechnik (Ost) vom 5. Juli 1993 und aus § 4 der Verwaltungsvorschrift der Sächsischen Staatsregierung über Arbeitsbedingungen für Beamte und Richter des Freistaates Sachsen an Bildschirmgeräten vom 26. November 1992 (SächsABl. Nr. 36/92, S. 1911) folgt, daß bei Beschäftigten an Bildschirmarbeitsplätzen eine ärztliche Untersuchung der Augen durchzuführen ist.

Das LfF hat ein privates Unternehmen durch Vertrag beauftragt, diese Bildschirmarbeitsplatzuntersuchungen vorzunehmen. Das beauftragte Unternehmen, das ärztliches Personal beschäftigt, verlangte als Grundlage für die individuelle Bildschirmarbeitsplatzuntersuchung einen umfangreichen Gesundheitsfragebogen, der das für Augenuntersuchungen erforderliche Maß erheblich überschritt.

Ich habe alle Beteiligten gebeten dafür zu sorgen, daß der Datenerhebung beim Betroffenen ausschließlich die zur Beurteilung der Bildschirmtauglichkeit *erforderlichen* Fragen zugrundegelegt werden. Als Muster habe ich den allenthalben verwendeten berufsgenossenschaftlichen „G 37“-Bogen empfohlen, allerdings unter Verzicht auf die nicht erforderlichen Daten
- Versicherungsnummer des Rentenversicherungsträgers
- Geburtsname
- Staatsangehörigkeit
- Krankenkasse
- Einstellungsdatum.

Das SMF hat dies durchgestellt.

### 5.1.9 Arbeitsschutzrechtliche Bildschirmarbeitsplatz-Datenerhebung an einer sächsischen Hochschule

Ein Institutsdirektor einer Universität hatte datenschutzrechtliche Bedenken gegen einen Erhebungsbogen, den sämtliche Bildschirmarbeitsplatzinhaber der Hochschule ausfüllen sollten.

In einem Gespräch mit den zuständigen Stellen der Universität wurde deutlich, daß auch die öffentlichen Arbeitgeber verpflichtet sind, bei Bildschirmarbeitsplätzen die Sicherheits- und Gesundheitsbedingungen insbesondere hinsichtlich einer möglichen Gefährdung des Sehvermögens sowie körperlicher Probleme und psychischer Belastung *zu ermitteln und zu beurteilen* (§§ 5, 6 ArbschG, § 3 Bildschirmarbeitsverordnung). Die Fragen bewegten sich durchweg in diesem Rahmen.

Befürchtungen, daß die ausgefüllten personenbeziehbaren Erhebungsbögen beim Büro für Arbeitssicherheit der Hochschule zu Rückschlüssen führen könnten, haben sich nicht bestätigt.

Die Universität hat nämlich die Verantwortung für den Arbeitsschutz auf die jeweiligen „Vorgesetzten“ delegiert und außerdem den in Frage stehenden Erhebungsbogen den Struktureinheiten zur Anwendung „empfohlen“, also nicht zwingend vorgeschrieben. Die einzelplatzbezogenen Erhebungsunterlagen sollten (zuständigkeitshalber) in der jeweiligen Struktureinheit mit der Maßgabe verbleiben, sie in eigener Verantwortung auszuwerten und ggf. Maßnahmen i. S. d. Bildschirmarbeitsschutzes zu ergreifen.

Das Büro für Arbeitssicherheit war nur an der anonymisierten Gesamtauswertung (ohne jeglichen Personenbezug) interessiert.

### 5.1.10 Erhebung von Seminarteilnehmer- und Dozentendaten (Evaluation)

Ein staatliches Rechnungsprüfungsamt beabsichtigte, von jedem Mitarbeiter, der an Fortbildungsveranstaltungen teilnimmt, einen „Bericht über eine Fortbildungsveranstaltung“ ausfüllen zu lassen, um Rückschlüsse auf die Qualität der Veranstaltung (einschließlich der Dozenten) zu ermöglichen. Plötzliche Bedenken veranlaßten das staatliche Rechnungsprüfungsamt, mich um meine datenschutzrechtliche Einschätzung zu bitten, die auf folgende Datenerhebungsprobleme hinwies:

1. Erhebung personenbezogener Daten beim Seminarteilnehmer selbst und
2. Erhebung personenbezogener Daten bei Dritten (Seminarteilnehmer müssen den Dozenten und seine Unterrichtsmethode, -gestaltung usw. bewerten).

*Zu 1:*
Nach § 31 Abs. 1 SächsDSG darf das Staatliche Rechnungsprüfungsamt Daten von Beschäftigten (hier Seminarteilnehmer) ohne deren Einwilligung nur verarbeiten, soweit dies zur Eingehung, Durchführung oder Beendigung des Dienst- oder Arbeitsverhältnisses *erforderlich* ist oder ein Gesetz, ein Tarifvertrag oder eine Dienstvereinbarung dies vorsieht.

Mir ist weder eine Rechtsvorschrift ersichtlich, die eine Pflicht zur Angabe personenbezogener Daten der Seminarteilnehmer im Zusammenhang mit Evaluationen vorsieht, noch vermag ich eine Erforderlichkeit zu o. a. Zwecken zu erkennen.

Eine Evaluation darf deshalb nur auf freiwilliger Basis und - in Bezug auf den Seminarteilnehmer - anonym erfolgen. Dies schließt auch eine persönliche Abgabe des Evaluationsbogens „im Amt“ aus.

*Fazit:*
Die Betroffenen müßten demnach im Beurteilungsbogen deutlich darauf hingewiesen werden, daß

- das Ausfüllen des Beurteilungsbogens freiwillig ist,
- personenbezogene Daten des Seminarteilnehmers nicht eingetragen werden dürfen,
- der anonyme Beurteilungsbogen in verschlossenem Umschlag *ohne Absenderangabe* dem Amt zugeleitet wird.

*Zu 2:*
Die Evaluation durch die Seminarteilnehmer stellt bezüglich des zu beurteilenden Dozenten eine Datenerhebung bei Dritten dar, deren Zulässigkeit an § 11 Abs. 4 SächsDSG zu messen ist.

Da die übrigen Voraussetzungen nicht zutreffen, darf die Datenerhebung nur mit Einwilligung des Dozenten erfolgen (§ 11 Abs. 4 Nr. 2 SächsDSG). Die Anforderungen an eine solche Einwilligung ergeben sich aus § 4 Abs. 1 Nr. 2 und Absätze 2 und 3 SächsDSG. Außerdem besagt Art. 2 Buchstabe h der EU-Datenschutzrichtlinie, daß unter *„Einwilligung der betroffenen Person jede Willensbekundung zu verstehen ist, die ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage erfolgt und mit der die betroffene Person akzeptiert, daß personenbezogene Daten, die sie betreffen, verarbeitet werden."*

*Fazit:*
Beurteilungsbogen dürfen an die Seminarteilnehmer nur ausgegeben werden, sofern sich der Dozent mit der Evaluationsprozedur einverstanden erklärt hat.

Ich habe angeregt, die bisher eingegangenen, nicht datenschutzgerechten Beurteilungsbögen zuverlässig zu vernichten (§ 19 Abs. 1 Nr. 1 SächsDSG) und den Beurteilungsbogen entsprechend meiner Stellungnahme zu überarbeiten. Außerdem habe ich unter Hinweis auf § 19 Abs. 1 Nr. 2 SächsDSG gebeten, bei künftigen, dann datenschutzgerechten Evaluationen darauf zu achten, daß die Beurteilungsbögen nach ihrer Auswertung vernichtet werden.

Das Staatliche Rechnungsprüfungsamt hat mir kurz darauf mitgeteilt, daß die bisher eingegangenen Beurteilungsbögen vernichtet wurden und daß *„auf eine amtsinterne Auswertung von Lehrgangsveranstaltungen mit Hilfe eines Beurteilungsbogens verzichtet wird"*.

Der geneigte Leser möge aus dieser Reaktion seine Schlüsse ziehen. Ging es ursprünglich tatsächlich nur um die Qualität der Veranstaltung (zu deren Feststellung jedenfalls „personenbeziehbare" Beurteilungsbögen nicht erforderlich sind), oder eben doch um die Qualität der Dozenten?

### 5.1.11 Dienstvereinbarung über die Erfassung und Abrechnung von Telefongesprächen im Gehaltsabzugsverfahren

Im Rahmen meiner Beteiligung (§ 31 Abs. 7 SächsDSG) übersandte mir ein Landratsamt den Entwurf einer Dienstvereinbarung über die Erfassung und Abrechnung von Telefongebühren zur Begutachtung. Im Hinblick auf meinen kritischen Beitrag zur Einbehaltung privater Telefongebühren im Gehaltsabzugsverfahren in 4/5.1.26 hatte man u. a. nachstehende Regelungen vorgesehen:

*„§ 5 Abrechnung privater Telefongespräche*

*Die entstandene Gebühr kann monatlich über das Gehaltskonto abgerechnet werden. Sie erscheint auf dem Gehaltsbogen nur als Gesamtsumme. Einwände gegen die Abrechnung sind innerhalb des laufenden Monats schriftlich zu erheben.*

*In begründeten Ausnahmefällen hat ein Beschäftigter die Möglichkeit, die Höhe der Gebühr anhand des Gesprächseinzelnachweises zu prüfen.*

*Auf diesem Ausdruck werden Name und Amt des Beschäftigten sowie Datum, Uhrzeit, verkürzte Rufnummer, verbrauchte Gebühreneinheiten und Gesprächsdauer nachgewiesen.*

*Aus datenschutzrechtlichen Gründen erscheint die angewählte Rufnummer ohne die drei letzten Stellen. Die PIN-Nummer ist auf der Abrechnung nicht ersichtlich.*

*Alternativ besteht außerdem die Möglichkeit, daß die privaten Telefongespräche anhand einer Kostenrechnung den Beschäftigten berechnet werden. Hierbei ist zur Abgeltung des Verwaltungsaufwandes eine zusätzliche Gebühr von 5,00 DM pro Abrechnung zu zahlen.*

*§ 6 Sonderregelungen*

*In den unter § 1 benannten Objekten ist die Installation eines Gebührenrechners aus wirtschaftlichen Gründen nicht vertretbar. Deshalb werden für die betreffenden Rufnummern Einzelgesprächsnachweise (EGN) bei der Telekom beantragt, die monatlich direkt an die Organisationseinheiten gesandt werden. Die betreffenden Beschäftigten machen die angewählten Rufnummern ihrer Privatgespräche auf dem EGN unkenntlich und vermerken die jeweilige Gesamtsumme ihrer privaten Telefongespräche. Dieser Betrag wird dann über das Gehaltskonto abgerechnet bzw. mittels Kostenrechnung in Rechnung gestellt. Bei einer Rechnungslegung ist für die Abgeltung des Verwaltungsaufwandes zusätzlich eine Gebühr von 5,00 DM pro Abrechnung zu zahlen."*

Meine Stellungnahme hierzu lautete wie folgt:

Ich vermag weder in § 5 noch in § 6 zu erkennen, daß das vorgesehene Gehaltsabzugsverfahren sowie das Kostenrechnungsverfahren durch eine (freiwillige) Einwilligung der Bediensteten gedeckt ist. Vielmehr, so verstehe ich die Formulierungen, erfolgt die Einbehaltung der Telefongebühren im Gehaltsabzugsverfahren ohne Zutun der Betroffenen als „Regelfall". Die Betroffenen können lediglich auf der alternativen, aber gebührenpflichtigen Kostenrechnung bestehen (Motto: „Wenn Dir das Gehaltsabzugsverfahren nicht paßt, mußt Du halt bezahlen.").

Die Anforderungen an eine „freiwillige Einwilligung" (siehe 4/5.1.26) sind auch nicht ansatzweise erfüllt.

Die in §§ 5, 6 getroffenen Regelungen verstoßen zudem gegen das Willkürverbot. So sollen Gehaltsabzüge im Regelfall ohne Einzelnachweis erfolgen. Die Betroffenen erhalten nur in *begründeten Ausnahmefällen* einen Gesprächseinzelnachweis. Ein solcher müßte aber aus datenschutzrechtlicher Sicht der Regelfall sein.

Das Bundesverfassungsgericht äußert sich im „Volkszählungsurteil“ vom 15. Dezember 1983 u. a. wie folgt:

> *„Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffenden Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden. Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß“ (BVerfGE 65, 1, 43).*

Entgegen dieser für die gesamte öffentliche Verwaltung verbindlichen Rechtsprechung führt die in der Dienstvereinbarung vorgesehene Gehaltsabzugsregelung ohne Einzelnachweis zu einer ungerechtfertigten Disposition des Landratsamtes über die Gehaltskonten der Bediensteten.

Wenn aber - anders als bisher - der Einzelnachweis der Regelfall sein muß, vermag die Begründung, daß bei Bareinzahlung (wegen der Erstellung einer Kostenrechnung) ein höherer Verwaltungsaufwand entsteht, der mit 5,00 DM zu Buche schlägt, nicht zu überzeugen.

Die aus datenschutzrechtlicher Sicht gebotene Änderung des Verfahrens hat das Landratsamt daraufhin vorgenommen: Jeder Mitarbeiter erhält nunmehr unaufgefordert seinen Einzelgesprächsnachweis; zur Abgeltung des Verwaltungsaufwandes werden die 5,00 DM nicht mehr erhoben.

### 5.1.12 Einsichtnahme des Geheimschutzbeauftragten in Personalakten im Rahmen von Sicherheitsüberprüfungen

Fraglich war, ob der Geheimschutzbeauftragte zur Einsicht in Personalakten berechtigt ist.

In Sachsen existiert bislang lediglich eine Verwaltungsvorschrift (Sicherheitsrichtlinie - SiR gültig bis 31. Dezember 1998), die dem Geheimschutzbeautragten ausdrücklich die Einsicht in Personalakten gestattet. Nach Angaben des SMI soll jedoch das sich noch im Entwurfsstadium befindliche Sicherheitsüberprüfungsgesetz dieses Recht ausdrücklich auf eine gesetzliche Grundlage stellen.

Bis zum Inkrafttreten dieses Gesetzes halte ich es für vertretbar, das Akteneinsichtsrecht auf § 117 Abs. 3 SächsBG zu stützen. Nach Auffassung von Schütz, Beamtenrecht für das Land Nordrhein-Westfalen (§ 102, Rdnr. 22; Stand: September 1994) sind die Geheimschutzbeauftragten - soweit Sie Befugnisse in Personalangelegenheiten wahrnehmen - Teil der Personalverwaltung und insoweit „mit der Bearbeitung von Personalangelegenheiten“ beauftragt.

Auf Bundesebene ist die Frage des Einsichtsrechts für den Geheimschutzbeauftragten in die Personalakte ähnlich wie in einer Reihe von Bundesländern ausdrücklich in § 13 Abs. 6 SÜG geregelt, wonach „zu diesem Zweck Personalakten eingesehen werden können“.

### 5.1.13 Einsichtnahme in Personalakten durch Praktikanten bei der Polizei

Der Polizei-Bezirkspersonalrat der Bereitschaftspolizei Sachsen fragte an, ob und ggf. unter welchen Voraussetzungen Praktikanten zu Ausbildungszwecken Einsicht in Personalakten gewährt werden dürfe. Im Erlaß des SMI zur Verpflichtung von Praktikanten auf das Datengeheimnis vom 13.1.1997; Az.: 32-055/192 (siehe auch 5/5.9.16) seien keine diesbezüglichen Regelungen enthalten.

Dem Personalrat habe ich mitgeteilt, daß ich die Einsichtnahme in Personalakten durch (behördenfremde) Praktikanten für unzulässig halte, weil gemäß § 117 Abs. 3 SächsBG Zugang zur Personalakte nur Beschäftigte haben dürfen, die im Rahmen der Personalverwaltung mit der Bearbeitung von Personalangelegenheiten beauftragt sind, und nur soweit dies zu Zwecken der Personalverwaltung oder Personalwirtschaft erforderlich ist. Grundsätzlich ist der Kreis der mit der Personalakte befaßten Mitarbeiter so klein wie möglich zu halten, um vor unbefugter Einsicht zu schützen (§ 117 Abs. 1 SächsBG, Nr. 1.3 Abs. 2 VwV Personalakten vom 4.11.93). Im Rahmen der Ausbildung von Praktikanten sind Original-Personalakten regelmäßig nicht erforderlich, da durch den Umgang mit anonymisierten Musterakten die gleichen Ausbildungseffekte erzielt werden können.

### 5.1.14 Schutz personenbezogener Daten von Lehrern

In einer Eingabe beschwerte sich ein Vater, der seinen Sohn krankmelden wollte, daß er über Tage hinweg niemanden telefonisch in der Schule erreichen konnte. Seine Bitte, ihm doch für alle Fälle die Privatanschriften einiger Lehrer mitzuteilen, wurde von der Schule unter Hinweis auf den Datenschutz abgelehnt.

In meiner Antwort an den Petenten bedauerte ich zwar, daß er in der Schule tagelang niemanden erreichen konnte. Das wäre sicher ein Mißstand. Jedoch rechtfertige dies nicht, daß man ihm ohne weiteres private Lehrerdaten mitteilt.

§ 31 Abs. 2 SächsDSG bestimmt nämlich, daß die Übermittlung von Beschäftigtendaten an Personen *außerhalb* des öffentlichen Bereichs nur auf gesetzlicher Grundlage oder *mit Einwilligung* des Betroffenen zulässig ist. Da das Schulgesetz für den Freistaat Sachsen keine Bestimmung über die Übermittlung von Lehrerdaten an

Private enthält und die betroffenen Lehrer offenbar in eine Übermittlung ihrer Daten nicht eingewilligt haben, war die vom Petenten kritisierte Auskunftsverweigerung nicht zu beanstanden.

### 5.1.15 Veröffentlichung von personenbezogenen Daten im Jahresbericht des Sächsischen Rechnungshofes

Ein städtisches Orchester hielt Ausführungen im Jahresbericht des Sächsischen Rechnungshofes für datenschutzrechtlich bedenklich, weil aus Einzelheiten über Vergütung und Arbeitsbelastung unschwer auf einzelne, einer breiten Öffentlichkeit bekannte Orchestermitglieder in herausgehobener Stellung geschlossen werden könne.

Der Sächsische Rechnungshof ist gemäß § 97 SäHO gehalten, die Ergebnisse seiner Prüfungen dem Landtag und der Staatsregierung in seinem Jahresbericht zuzuleiten. In Einzelfällen kann der Bericht nicht ohne (mittelbaren) Personenbezug auskommen. Das Verfassungsgebot einer Finanzkontrolle kann andere verfassungsrechtlich geschützte Rechtspositionen einschränken (vgl. Heuer, Kommentar zur Bundeshaushaltsordnung, § 95, Rdnr. 1 m. w. N.). Es ist in Rechtsprechung und Literatur anerkannt (vgl. OVG Lüneburg DVBl. 1984, 837; v. Köckritz/Ermisch/Maatz, Kommentar zur Bundeshaushaltsordnung, § 95, Anm. 2), daß Eingriffe in das Persönlichkeitsrecht des Einzelnen durch den Rechnungshof verhältnismäßig sein können, wenn es keine andere - das Persönlichkeitsrecht weniger belastende - Möglichkeit gibt.

Es ist also zwischen der Veröffentlichungspflicht des Rechnungshofes und dem Persönlichkeitsrecht des Einzelnen abzuwägen. In der fraglichen Passage werden das jeweils niedrigste und das höchste Monatsgehalt der Musiker genannt. Ohne diese Darstellung wäre dieser Berichtsteil unverständlich. Für die genannten Gehälter ist allenfalls ein mittelbarer Personenbezug herzustellen, da die Höhe der Einzelvergütungen von verschiedenen Faktoren wie Orchesterzugehörigkeit, Familienstand usw. abhängig ist. Die Vergütungsgruppe ergibt sich zudem aus dem Stellenplan des Orchesters, der Teil des - öffentlichen - Haushaltsplanes der Kommune ist.

Die Vorgehensweise des Sächsischen Rechnungshofes war nicht zu beanstanden. Zudem gilt: Wer aus öffentlichen Töpfen bezahlt wird, muß die gebotene Transparenz seiner Bezüge dulden.

### 5.1.16 Veröffentlichung von Beschäftigtendaten in einem Intranet

Eine Hochschule fragte an, ob die Einstellung eines Telefonverzeichnisses des Hochschulpersonals in ein internes, nur den Mitarbeitern zugängliches Hochschulnetz datenschutzrechtlich zulässig sei.

Im Hinblick auf § 31 Abs. 1 SächsDSG, wonach öffentliche Stellen Beschäftigtendaten u. a. für organisatorische Maßnahmen verarbeiten dürfen, halte ich die Telefonliste in einem lokalen Netz für ein geeignetes Mittel zur Gewährleistung der inner-

dienstlichen Kommunikation mit der Möglichkeit zeitnaher Aktualisierung. Da eine Beschränkung auf das für den dienstlichen Ablauf erforderliche Maß an personenbezogenen Daten erfolgte (lediglich Name, Vorname, Funktionsbezeichnung, Arbeitszimmer und Telefonnummer werden aufgeführt) und eine Datenübermittlung an Stellen außerhalb der Hochschule nicht stattfindet, halte ich die vorgesehene Darstellung eines Telefonverzeichnisses im lokalen Hochschulnetz für datenschutzrechtlich unbedenklich.

### 5.1.17 Auskunft über Bezügedaten an das Beamtenheimstättenwerk (BHW) durch das LfF

Einer Petition zufolge habe ein Mitarbeiter der Bezügestelle des LfF dem (privaten!) BHW telefonisch Daten zur Finanzsituation des Petenten bekanntgegeben. Als Folge dieser Auskunftserteilung sei ein Finanzierungsplan nicht termingerecht aufgestellt worden, was zusätzliche Kosten und Mietausfall verursacht hätte.

Aus der vom SMF abgeforderten Stellungnahme ging hervor, daß sich der Mitarbeiter der Bezügestelle aufgrund des forschen Auftretens einer BHW-Angestellten ins Bockshorn hatte jagen lassen und er die gewünschten Auskünfte zum Nachteil des Petenten erteilte. Seitens des BHW wurde der Eindruck erweckt, es liege die Einwilligung des Petenten zur Auskunftserteilung vor (was nicht stimmte).

Aufgrund dieser „mißglückten“ Auskunftserteilung bat ich das SMF, das in Frage kommende Personal des LfF in nachstehendem Sinne zu belehren: Die telefonische Auskunft ist ein exemplarischer Beleg dafür, daß bei manchen Bediensteten das Wissen um den Grundsatz der Gesetzmäßigkeit der Verwaltung noch nicht hinreichend ausgeprägt ist. So verwundert es nicht, daß trotz bestehender rechtlicher Barrieren telefonische Auskünfte bei entsprechend selbstbewußtem Auftreten des Anrufers ohne Ansehung von Art. 33 SächsVerf, §§ 2, 4, 15, 31 SächsDSG, 121 Abs. 2 SächsBG erteilt wurden und werden, was u. U. zu materiellen Nachteilen (wie die im konkreten Fall durch die auskunftsbedingte erneute Überprüfung des Finanzierungsplanes eingetretenen Verzögerungen) führen kann. Dadurch können Schadensersatzverpflichtungen entstehen.

Mir erscheint es notwendig, daß insbesondere im Landesamt für Finanzen publik wird, unter welchen rechtlichen Gesichtspunkten Auskünfte über Beschäftigtendaten an Private (zumal am Telefon) erteilt werden dürfen (siehe allgemein 3/5.3.3.4).

Ausgehend von Art. 33 SächsVerf, wonach u. a. die Weitergabe von personenbezogenen Daten ohne freiwillige und ausdrückliche Zustimmung nur durch Gesetz oder aufgrund eines Gesetzes (das gemäß BVerfGE 65, 1, 44 normenklar und verhältnismäßig sein muß) erfolgen darf, hätten die datenschutzrechtlichen bzw. beamtenrechtlichen Zulässigkeitsvoraussetzungen vor der Auskunftserteilung geprüft werden müssen. Einer solchen Prüfung legt man je nachdem, ob es sich um einen *Arbeitnehmer* oder *Beamten* handelt, über den Auskunft erteilt werden soll, etwa folgende Fragen zugrunde:

1. Auskunft über einen *Arbeitnehmer* an Private

a) Handelt es sich (überhaupt) um personenbezogene Daten i. S. v. § 3 Abs. 1 SächsDSG?
b) Wenn ja, soll die Auskunft durch eine sächsische öffentliche Stelle (§ 2 Abs. 1 SächsDSG) erteilt werden?
c) Wenn ja, gibt es eine besondere Rechtsvorschrift, die dem SächsDSG gemäß § 2 Abs. 4 vorgeht?
d) Wenn ja, Spezialvorschrift anwenden. Wenn nein, läßt das SächsDSG die Auskunft über Arbeitnehmerdaten zu (§ 4 Abs. 1 Nr. 1 SächsDSG)?

*Antwort:* Ja, § 31 Abs. 2 SächsDSG! Da es keine besondere Rechtsvorschrift für Auskünfte über Arbeitnehmer an Private geben dürfte, ist die Auskunftserteilung danach nur mit Einwilligung des Betroffenen zulässig.

2. Auskunft über einen *Beamten* an Private

a) Handelt es sich (überhaupt) um personenbezogene Daten i. S. v. § 3 Abs. 1 SächsDSG?
b) Wenn ja, soll die Auskunft durch eine sächsische öffentliche Stelle (§ 2 Abs. 1 SächsDSG) erteilt werden?
c) Wenn ja, gibt es eine besondere Rechtsvorschrift, die dem SächsDSG gemäß § 2 Abs. 4 vorgeht?

*Antwort:* Ja, § 121 Abs. 2 SächsBG!
(Anmerkung: Eine weitere Prüfung des SächsDSG entfällt an dieser Stelle.)
Die Auskunftserteilung ist danach ebenfalls von der Einwilligung/dem Einverständnis des Betroffenen abhängig. Hinzu kommt (anders als bei Arbeitnehmern) die schriftliche Benachrichtigung des Betroffenen über Inhalt und Empfänger der Auskunft.

Der auskunftgebende Beamte des LfF hätte sich jedenfalls davon überzeugen müssen, daß das vom BHW behauptete Einverständnis des Betroffenen tatsächlich existiert. (z. B. Aufforderung an das BHW, die Einwilligung per Fax zu schicken. Eine solche Forderung ist trotz evtl. geltend gemachter Eilbedürftigkeit heute bei Nutzung der neuen Techniken kein Problem mehr. Schließlich dient das schriftliche Verfahren auch als Nachweis für die Rechtmäßigkeit der Auskunftserteilung). Unschwer hätte er danach erkannt, daß eine Auskunft an das BHW mangels der in § 121 Abs. 2 SächsBG vorgesehenen Einwilligung des Betroffenen rechtswidrig wäre und u. U. als Ordnungswidrigkeit nach § 32 Abs. 1 Nr. 1 a SächsDSG mit Bußgeld belegt werden kann. Die mangelnde Sorgfalt führte außerdem dazu, daß der Beamte des LfF gegen § 6 SächsDSG (Datengeheimnis) verstoßen hat (§ 203 StGB). Nicht unerwähnt bleibt, daß auch das BHW möglicherweise wegen einer Ordnungswidrigkeit gemäß § 32 Abs. 1 Nr. 2 SächsDSG belangt werden kann, weil es vorgab, daß das Einverständnis des Betroffenen vorgelegen habe.

Aus alledem folgt, daß einem schriftlichen Auskunftsverfahren grundsätzlich der Vorzug zu geben ist.

Das SMF hat die schriftliche Belehrung der in Frage kommenden Bediensteten veranlaßt. Den Petenten habe ich von der Rechtswidrigkeit der Auskunftserteilung unter Hinweis auf die einschlägigen Bußgeldbestimmungen unterrichtet.

### 5.1.18 Verhaltens- und Leistungskontrolle mit automatisierter Vorgangsverwaltung

Der Personalrat eines staatlichen Umweltfachamtes informierte mich über die beabsichtigte Einführung eines automatisierten Verfahrens zur budgetierungstauglichen Vorgangsverwaltung, das wegen der leistungsrelevanten Daten zu einer umfassenden Leistungs- und Verhaltenskontrolle aller Bediensteten geeignet sei.

Im Rahmen meiner Ermittlungen habe ich dem Umweltfachamt mitgeteilt, daß öffentliche Stellen Beschäftigtendaten grundsätzlich nur verarbeiten dürfen, 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 und des Personaleinsatzes *erforderlich* ist oder ein Gesetz, ein Tarifvertrag oder eine Dienstvereinbarung dies vorsieht (§ 31 Abs. 1 SächsDSG). Ich habe ferner darauf hingewiesen, daß ein Verfahren, das zur automatisierten Verarbeitung von Beschäftigtendaten geeignet ist - auch und gerade im Zusammenhang mit einem Pilotprojekt - nur im Benehmen mit mir eingeführt, angewendet, geändert oder erweitert werden darf. Außerdem ist meine Stellungnahme den zuständigen Personalvertretungen im Rahmen des personalvertretungsrechtlichen Beteiligungsverfahrens zuzuleiten. Ohne meine Beteiligung nach § 31 Abs. 7 SächsDSG und bei fehlender Mitbestimmung ist jede automatisierte Verarbeitung von Beschäftigtendaten rechtswidrig.

Die Datenbank „Vorgangsverwaltung“ der ersten Projektphase verwaltet neben Postein- und -ausgängen die Registratur, Termine und Bearbeitungsgänge sowie Mengendaten in einem „Auswertungsmodul“. Eine Terminplanung kann jedoch nur sinnvoll für und von dem jeweiligen Benutzer gestaltet werden, wenn ihm die jeweiligen Vorgänge zugeordnet werden können. Da somit schon in dieser Phase eine automatisierte Verarbeitung von Beschäftigtendaten stattgefunden hat, hätte das Benehmen mit mir (§ 31 Abs. 7 SächsDSG) hergestellt werden müssen.

In einer zweiten Projektphase soll nun ein Produktverwaltungssystem zur Terminkoordinierung und produktbezogenen Arbeitszeiterfassung eingeführt werden, das die Vorgangsverwaltung an ein Budgetierungssystem koppelt. Die zwischenzeitlich geschlossene Dienstvereinbarung zwischen dem Personalrat und dem Umweltfachamt sieht ein datenschutzgerechtes Sicherungssystem vor. Zur Identifizierung der jeweiligen Bearbeiter während der Bearbeitung sowie der Kostenstelle wird eine vierstellige Kennzahl verwendet:
1. Stelle: Abteilung
2. Stelle: Referat/Kostenstelle
3. Stelle: Laufbahn
4. Stelle: Name des Bearbeiters

Nach Fertigstellung des Produktes und Ablage der Akte wird vom System selbständig die letzte Stelle dieser Ziffer zur Identifizierung der Bearbeiter physisch gelöscht. Die Aktenzeichen werden mit Einführung des Systems so gestaltet, daß aus ihnen kein Bearbeiter mehr ersichtlich ist. Nach spätestens einem Jahr wird bei allen abgeschlossenen Produkten auch die dritte Stelle der Kennzahl unwiderbringlich gelöscht. Die Daten aus dem computergestützten Produktverwaltungssystem werden nicht personenbezogen zusammengefaßt oder ausgewertet.

Diese Vorgehensweise halte ich für angemessen. Ein Datenschutz- und Datensicherheitskonzept (§ 9 Abs. 2 SächsDSG) ist mir aber noch vorzulegen.

### 5.1.19 Datenschutzrechtliche Einordnung des polizeiärztlichen Dienstes

Wie in den anderen Bundesländern gibt es in Sachsen einen polizeiärztlichen Dienst mit folgenden Aufgaben:
- laufbahn- und beamtenrechtliche Untersuchungen
- Eignungsuntersuchungen für bestimmte Verwendungen in der Polizei
- Begutachtung im Rahmen der Dienstunfallfürsorge
- Gesundheitsvorsorge für Polizeibeamte
- betriebsärztliche Aufgaben nach dem Gesetz über Betriebsärzte, Sicherheitsingenieure und andere Fachkräfte für Arbeitssicherheit vom 12.12.1973 (BGBl. I S. 1885)
- Aufgaben nach dem Arbeitsschutzgesetz
- Polizeisanitätsdienst (insbesondere ärztliche Absicherung der Aus- und Fortbildung und der Polizeieinsätze sowie Aus- und Fortbildung von Sanitätsbeamten der Polizei)
- Erfüllung von Aufgaben zur Gewährleistung der Hygiene und zur Verhinderung von Infektionskrankheiten gemäß Bundesseuchengesetz
- polizeiärztliche Aufgaben im Rahmen der Heilfürsorge
- kurative ärztliche Tätigkeit für heilfürsorgeberechtigte Polizeibeamte

Für problematisch halte ich, daß im polizeiärztlichen Dienst somit ein umfassendes Gesundheitsprofil über jeden Polizeibeamten entsteht, ohne daß es hierfür (anders z. B. als für Krankenkassen und Gesundheitsämter) legitimierende Rechtsgrundlagen gibt. Lediglich für den Teilbereich „Heilfürsorge“ sieht § 147 SächsBG vor, daß Polizeibeamte Heilfürsorge erhalten, solange ihnen Besoldung zusteht. Eine Rechtsverordnung, in der die näheren Vorschriften über Art, Umfang und Trägerschaft der Heilfürsorge zu regeln sind, fehlt bislang. Auch die in § 118 letzter Satz SächsBG vorgesehene Abschottung von Unterlagen über Heilfürsorge und Heilverfahren von der übrigen Personalakte ist wenig hilfreich, weil nicht auszuschließen ist, daß eine Verknüpfung mit den sonstigen Gesundheitsdaten beim polizeiärztlichen Dienst erfolgt. Hinzu kommt, daß der polizeiärztliche Dienst unmittelbar dem SMI zugeordnet ist, was möglicherweise zu Konflikten bezüglich einer erforderlichen Weisungsunabhängigkeit führt. Kein Polizeibeamter kann sicher sein, daß aufgrund der beim polizeiärztlichen Dienst vorhandenen umfassenden Erkenntnisse über seinen Gesundheitszustand seine Dienstfähigkeit nicht in Frage gestellt wird. Polizeibeamte sind jedenfalls in dieser Hinsicht wesentlich schlechter gestellt als andere Beamte und alle

Arbeitnehmer innerhalb und außerhalb des öffentlichen Dienstes. Aus guten Gründen hat man beispielsweise die Betriebskrankenkassen zu von den Mutterbetrieben unabhängigen Körperschaften des öffentlichen Rechts gemacht.

Aus Baden-Württemberg ist mir bekannt, daß das dortige Innenministerium zwar eingeräumt hat, daß die Wahrnehmung von Aufgaben in der Heilfürsorge und im betriebs- und polizeiamtsärztlichen Dienst durch den Polizeiarzt in Personalunion rechtswidrig sei; jedoch hat sich bislang auch dort nichts entscheidendes bewegt.

Problematisch ist auch die datenschutzrechtliche Einordnung der beim polizeiärztlichen Dienst im Rahmen seiner Rundumfürsorge entstandenen Unterlagen.

Nicht geklärt sind z. B. Fragen wie
- was ist Krankenakte, was Personalakte?
- welche Unterlagen des polizeiärztlichen Dienstes, aus denen die Art einer Erkrankung ersichtlich ist, sind gemäß § 123 Abs. 2 SächsBG unverzüglich zurückzugeben?

Insbesondere bedarf der polizeiärztliche Dienst eindeutiger Rechtsgrundlagen, die unter Beachtung der datenschutz- und beamtenrechtlichen Bestimmungen einen vom SMI unabhängigen Dienst gewährleisten.

Eine von mir initiierte Bund-/Länderumfrage war bisher wenig ergiebig. Ich beabsichtige, das Thema im Arbeitskreis Personalwesen der Datenschutzbeauftragten des Bundes und der Länder zu erörtern. Gleichwohl muß der angelaufene Dialog mit dem SMI fortgesetzt werden.

### 5.1.20 Beamtenvereidigung

Nach § 70 Abs. 2 und 3 SächsBG kann der Diensteid auch mit der Beteuerung „So wahr mir Gott helfe“, aber auch mit einer anderen Beteuerungsformel als „ich schwöre“ geleistet werden. Nach Nr. 9.3 i. V. m. Anlage 5 der Verwaltungsvorschrift des Sächsischen Staatsministeriums des Innern zur Begründung und Beendigung eines Beamtenverhältnisses vom 11. August 1997 (SächsABl. S. 1060) ist über jede Vereidigung eine Niederschrift nach Muster zu fertigen, das u. a. auch die religiöse Beteuerung und die anderslautende Beteuerung nach § 70 Abs. 3 SächsBG enthält. Wird der Eid ohne religiöse Beteuerung geleistet, ist der entsprechende Satz zu streichen. Die Niederschrift ist zu den Personalakten zu nehmen.

Damit werden Hinweise auf die religiöse Einstellung der betroffenen Beamten auf Dauer festgehalten, ohne daß dies für die Eingehung, Durchführung oder Beendigung des Beamtenverhältnisses in irgendeiner Form von Nutzen wäre. Daten über religiöse Anschauungen und Verhältnisse sind jedoch besonders schutzwürdig. Ihre Kenntnis führt u. U. zu erheblicher Beeinträchtigung in der gesellschaftlichen/beruflichen Stellung der Betroffenen (vgl. auch § 28 Abs. 2 Satz 2 BDSG und Nr. 2 der Bekanntmachung des Sächsischen Datenschutzbeauftragten zu den Maßnahmen zur Gewährleistung des Datenschutzes vom 30. Juni 1994 - SächsABl. S. 979).

Als Nachweis, daß der Beamte ordnungsgemäß vereidigt wurde, würde es völlig ausreichen, in der Niederschrift zu dokumentieren
- wer
- wann
- durch wen
- gemäß § 70 Abs. 1 SächsBG
(und zwar ohne Wiederholung der Eidesformel und der religiösen Beteuerung) vereidigt worden ist.

Nicht zuletzt im Hinblick auf Art. 8 Abs. 1 der EU-Datenschutzrichtlinie halte ich die Änderung der Anlage 5 zu o. a. VwV für unabdingbar.

Auch an eine entsprechende Bereinigung der Personalakten sollte gedacht werden.

Das SMI habe ich in vorstehendem Sinne unterrichtet.

### 5.1.21 Aufbewahrung von Schriftverkehr, der anläßlich der Petition eines öffentlich Bediensteten in einer Personalangelegenheit entstanden ist

Aus dem Kultusbereich wurde ich auf folgendes grundsätzliches Problem aufmerksam:

Wendet sich ein Bediensteter in einer Personalangelegenheit an den Petitionsausschuß des Sächsischen Landtags, so wird regelmäßig (über das Staatsministerium) eine Stellungnahme der zuständigen Personalstelle des Petenten eingeholt. Damit erfährt die Personalstelle, welcher Bedienstete sich in welcher Angelegenheit an den Petitionsausschuß gewandt hat. Der Information zufolge werden die im Zusammenhang mit solchen Petitionen entstandenen Unterlagen bei einem Oberschulamt in die *Personalakte* des Petenten aufgenommen.

Eine solche Verfahrensweise ist geeignet, die schutzwürdigen Interessen der Bediensteten erheblich zu beeinträchtigen. Muß ein Petent nämlich damit rechnen, daß die seine Petition betreffenden Unterlagen in der Personalakte dauerhaft gespeichert werden und ihm dadurch - wenn auch nicht nachweisbar - Nachteile entstehen können, wird er möglicherweise auf sein verfassungsmäßig verbrieftes Petitionsrecht (Art. 17 GG, Art. 35 SächsVerf) verzichten.

Mit dem Sächsischen Staatsministerium des Innern bin ich darin einig, daß Petitionen in Personalangelegenheiten nicht in einem *unmittelbaren* inneren Zusammenhang mit dem Dienstverhältnis des Betroffenen stehen und daher *keine* Personalaktenqualität besitzen. Die Aufnahme solcher Unterlagen in die Personalakte ist deshalb unzulässig.

Um eine einheitliche Verfahrensweise zu gewährleisten, habe ich alle obersten Dienstbehörden des Freistaates gebeten, die Praxis im eigenen Haus zu überprüfen und den nachgeordneten Bereich zu informieren und aufzufordern, ggf. die Personalakten zu bereinigen.

Das SMI hat den nachgeordneten Bereich in vorstehendem Sinne unterrichtet. Von den anderen Ressorts habe ich noch nichts gehört.

### 5.1.22 Überprüfung der Personalaktenführung in einer Stadtverwaltung (keine Gauck-Überprüfung feststellbar)

Bei der Kontrolle sämtlicher Personalakten einer Stadtverwaltung habe ich u. a. festgestellt, daß die nach Art. 119 SächsVerf erforderliche Überprüfung der Beschäftigten auf MfS-/AfNS-Vergangenheit nicht belegt werden konnte. Weder „Gauck-Mitteilungen“ noch die nach dem Verfahren zur Feststellung der persönlichen Eignung im Beamtenverhältnis und einer Tätigkeit im öffentlichen Dienst erforderlichen Erklärungen (vgl. Verwaltungsvorschrift der Sächsischen Staatsregierung zur Prüfung der persönlichen Eignung im Beamtenverhältnis vom 14. Dezember 1994 - SächsABl. 1995 S. 40, fortgeschrieben durch die Bekanntmachung des Sächsischen Staatsministerium des Innern vom 2. März 1995 - SächsABl. S. 436) befanden sich in den Personalakten. Der Bürgermeister wurde aufgefordert, den entsprechenden Nachweis, daß *jeder* Bedienstete überprüft und nur nicht belastetes Personal beschäftigt wird, zu erbringen (auf § 61 SächsGemO i. V. m. § 9 SächsDSG, wonach nur „geeignetes“ Personal eingestellt und mit der Verarbeitung personenbezogener Daten beauftragt werden darf, sei hingewiesen).
Anhand der aktuellen Beschäftigtenliste stellte ich fest, daß vier Personalakten fehlten (eine schriftliche Kontrolle der Aktenaus- und Aktenrückgabe erfolgt nicht). Der Bürgermeister hatte diese Personalakten im Original entgegen § 31 Abs. 2 SächsDSG und § 121 Abs. 2 SächsBG zur Vorbereitung von Kündigungsverfahren einer Rechtsanwältin gegeben. Die vier Personalakten wurden noch am gleichen Tag ins Rathaus zurückgeholt.
Das Einsichtsrecht des Beschäftigten in seine *vollständige* Personalakte (§§ 120 SächsBG und 31 Abs. 3 SächsDSG) war und ist wegen der vorstehenden Mängel nicht gewährleistet. Es wird darüber hinaus auch erschwert, weil in den geprüften Personalakten ein Verzeichnis über ggf. vorhandene Teilakten fehlte.
Der verwendete Personalbogen entspricht nicht den datenschutzrechtlichen Anforderungen. Ich habe empfohlen, sich an dem Muster nach Anlage 1 zu Nr. 1.1 der Verwaltungsvorschrift des Sächsischen Staatsministerium des Innern zur Begründung und Beendigung eines Beamtenverhältnisses vom 11. August 1997 - SächsABl. S. 1060 - zu orientieren (vgl. Materialien Nr. 16.2.1). Außerdem war die Paginierung der Personalakten nachzuholen.
Auch waren Maßnahmen (über festgelegte Zugriffsberechtigungen und kontrollierbare Schlüsselverwaltung für den Aktenschrank und Zimmerschlüssel), die eine unbefugte Akteneinsichtnahme weitestgehend ausschließen, nicht schriftlich geregelt.
Mir wurde zugesichert, die Personalaktenführung an die Vorgaben der Verwaltungsvorschrift des Sächsischen Staatsministerium des Innern über die Führung und Verwaltung von Personalakten vom 4. November 1993 (SächsABl. S. 1337) und der gemeinsamen Verwaltungsvorschrift der Sächsischen Staatskanzlei und der Sächsischen Staatsministerien zur Führung und Verwaltung von Personalakten für Angestellte, Arbeiter und die zu ihrer Ausbildung Beschäftigten im öffentlichen Dienst des Freistaates Sachsen vom 3. Dezember 1996 (SächsABl. 1997 S. 145) anzupassen.
Zu gegebener Zeit werde ich eine Nachkontrolle vornehmen.

### 5.1.23 Datenschutzkontrolle der Personalaktenführung im Sächsischen Staatsministerium für Umwelt und Landesentwicklung

Eine Prüfung der Personalstelle im SMU ergab, daß die Personalaktenführung den personalaktenrechtlichen Regelungen (§§ 177 ff. SächsBG) und den hierzu ergangenen Verwaltungsvorschriften entsprach.
Die Personalakten werden sicher aufbewahrt und es ist organisatorisch sichergestellt, daß unzuständige Personen keinen Zugang zu den Personalakten haben. Die Vollzähligkeit der Personalakten ist durch eine schriftlich protokollierte Aktenaus- und Aktenrückgabe (Karteikarte) ständig überprüfbar.
Die mit dem Personalrat geschlossene Dienstvereinbarung zur automatisierten Verarbeitung von Personaldaten sowie das Datenschutz- und Datensicherheitskonzept gemäß § 9 SächsDSG haben zur Prüfung vorgelegen. Die darin festgelegten Maßnahmen zur Gewährleistung des Datenschutzes haben den vorgefundenen Bedingungen entsprochen.

Würde nur überall so vorbildlich gearbeitet!

## 5.2 Personalvertretung

#### Personalnebenakten beim Personalrat

Offensichtlich hat 5/5.2.2 bezüglich der Rückgabe- bzw. Vernichtungspflicht von Personalunterlagen zu Irritationen geführt.

*Zur Klarstellung:*

Die in 5/5.2.2 angesprochene Rückgabe- bzw. Vernichtungspflicht bezieht sich auf alle vom Dienststellenleiter im Rahmen des personalvertretungsrechtlichen Beteiligungsverfahrens (Mitbestimmung, Mitwirkung) zur Verfügung gestellten und die Personalmaßnahme begründenden Unterlagen wie Zeugnisse, Lebenslauf, Lichtbild, Urkunden, Tätigkeitsnachweise usw., nicht jedoch den dazugehörenden Schriftwechsel (einschließlich Beteiligungsvordruck) zwischen Dienststellenleiter und Personalrat. Sämtliche Unterlagen verbleiben solange beim Personalrat, bis die Personalmaßnahme bestandskräftig abgeschlossen ist oder sich anderweitig endgültig erledigt hat.

## 5.3 Einwohnermeldewesen; Paß-und Personalausweiswesen

### 5.3.1 Rechtliche Entwicklung: Inkrafttreten der Sächsischen Meldedaten-Übermittlungsverordnung

Am 1. November 1997 trat die SächsMeldDÜVO vom 10. September 1997 (GVBl. S. 557) in Kraft, die die regelmäßige Übermittlung an und den automatisierten Abruf von Meldedaten durch die in dieser Verordnung genannten Behörden oder sonstigen öffentlichen Stellen regelt.

Rechtsgrundlage für den Erlaß dieser Verordnung ist § 36 Nr. 4 SächsMG. § 36 Nr. 4 SächsMG ermächtigt das SMI, die regelmäßige Übermittlung oder den automatisierten Abruf der in § 29 Abs. 1 SächsMG genannten Daten zuzulassen, also nicht „vorzuschreiben“ (so auch Belz/Rimmele/Wunsch, Kommentar zum Sächsischen Meldegesetz, § 36 Rdnr. 19).

Tatsächlich sind in der SächsMeldDÜVO jedoch eine Reihe von Vorschriften enthalten, die die Meldebehörden zu regelmäßigen Meldedatenübermittlungen verpflichten (z. B. §§ 6, 8 und 9). Diese Bestimmungen halte ich für rechtswidrig.

Deshalb habe ich angeregt, § 36 Nr. 4 SächsMG um die Worte „und vorzuschreiben“ zu ergänzen. Das SMI beabsichtigt eine entsprechende Gesetzesänderung auf den Weg zu bringen.

### 5.3.2 Gesetzentwurf der Staatsregierung über Personalausweise und zur Ausführung des Paßgesetzes im Freistaat Sachsen

Das SMI hat mir im Sommer 1997 den Referentenentwurf eines Gesetzes über Personalausweise und zur Ausführung des Paßgesetzes im Freistaat Sachsen (SächsPersPaßG) zur Stellungnahme übersandt. In § 3 Abs. 2 des Entwurfs war vorgesehen, Personen für die ein Betreuer bestellt worden ist oder die voraussichtlich dauernd in Krankenhäusern, Pflegeheimen oder ähnlichen Einrichtungen untergebracht sind, von der allgemeinen Ausweispflicht zu befreien. Seinerzeit bemängelte ich *erfolglos*, daß dies gegen § 1 Abs. 1 des Bundesgesetzes über Personalausweise (PAuswG) verstößt, wonach Deutsche, die das 16. Lebensjahr vollendet haben und der allgemeinen Meldepflicht unterliegen, ausnahmslos *verpflichtet* sind, einen Personalausweis zu besitzen. Mir wurde entgegengehalten, daß es in anderen Bundesländern ebenfalls solche Bestimmungen gäbe.

Der Gesetzentwurf der Staatsregierung wurde inzwischen ohne Berücksichtigung meiner Einwände in den Landtag eingebracht.
§ 3 Abs. 2 des Gesetzentwurfs hat nunmehr folgende Fassung:

*„Personen, für die ein Betreuer bestellt worden ist oder die voraussichtlich dauernd in Krankenhäusern, Pflegeheimen, oder ähnlichen Einrichtungen untergebracht sind, können durch die zuständige Personalausweisbehörde von der Ausweispflicht befreit werden. Die der Personalausweisbehörde hierbei bekannt gewordenen Daten dieser Personen dürfen nur zwischen Personalausweisbehörden übermittelt werden; die Tatsache, daß der Betroffene von der Ausweispflicht befreit ist, darf Behörden und Beamten, die zur Feststellung seiner Personalien ermächtigt sind, zu diesem Zweck mitgeteilt werden.“*

Die zuständigen Ausschüsse des Landtags informierte ich über meine Bedenken zu § 3 Abs. 2 des Gesetzentwurfs wie folgt.

Das Argument, andere Bundesländer würden ebenso eine Befreiung von der Ausweispflicht für den in § 3 Abs. 2 des Gesetzentwurfs genannten Personenkreis vorsehen, überzeugt mich aus folgenden Gründen nicht:

1. § 1 Abs. 1 PAuswG bestimmt, daß Deutsche, die das 16. Lebensjahr vollendet haben und der allgemeinen Meldepflicht unterliegen, ausnahmslos *verpflichtet* sind, einen Personalausweis zu besitzen. Der in § 3 Abs. 2 des Entwurfs aufgezählte Personenkreis, für den nach dieser Vorschrift eine Befreiung von der Ausweispflicht in Betracht käme, unterliegt in Sachsen ohne Ausnahme der allgemeinen Meldepflicht und ist somit gemäß § 1 Abs. 1 PAuswG verpflichtet, einen Personalausweis zu besitzen. Auch wenn es sich bei dem Bundesgesetz über Personalausweise um ein Rahmengesetz gem. Art 75 GG handelt, ist § 1 Abs. 1 Satz 1 PAuswG auf Grund des eindeutigen Wortlauts eine abschließende Vorschrift, die es dem Landesgesetzgeber verbietet, eine abweichende Regelung zu treffen. Denn es ist durchaus zulässig und üblich, daß Rahmengesetze unter Beachtung von Art. 75 Abs. 2 GG abschließende Regelungen enthalten.
   Derartige bundesgesetzliche Vorschriften sind *direkt geltendes Recht*; sie bedürfen keiner landesrechtlichen Umsetzung. Der Entwurf ist insoweit auch „handwerklich“ nicht in Ordnung. Er geht davon aus, daß allein die Tatsache einer Betreuung von der Ausweispflicht befreien kann („oder“). Wer das Betreuungsrecht studiert, wird feststellen, daß schon aus ordnungsrechtlicher/polizeilicher Sicht unbedeutende Zustände eine Betreuung rechtfertigen. Nach welchen (gesetzlichen!) Kriterien soll in diesen Fällen von einer Ausweispflicht befreit werden? Können da nicht „die Falschen“ befreit werden, insbesondere, wenn man an das Zusammenspiel mit Betreuern und Ärzten denkt?

2. Diese Auffassung wird auch nicht durch die Ausführungen der Staatsregierung in der Begründung zum Gesetzentwurf zu meiner Stellungnahme widerlegt. Die Staatsregierung führt dort aus, daß die Umsetzung der Rahmenregelung des § 1 Abs. 1 Satz 1 PAuswG deshalb nicht zwingend erforderlich sei, weil keine Situation denkbar wäre, in der sich der für eine Befreiung von der Ausweispflicht in Betracht kommende Personenkreis gegenüber einer zur Personalienfeststellung ermächtigten Behörde (wie z. B. Melde-, Paß- und Personalausweisbehörden, Staatsangehörigkeitsbehörden, Standesämter oder Polizeidienststellen) ausweisen müsse. So sei z. B. auszuschließen, daß der für eine Befreiung von der Ausweispflicht in Betracht kommende Personenkreis jemals einer Identitätsfeststellung durch die Polizei unterzogen würde.

   Diese Argumentation der Staatsregierung rechtfertigt zum einen keine Abweichung von der in § 1 Abs. 1 PAuswG bindend normierten Pflicht zum Besitz eines Personalausweises, zum anderen geht die Vorschrift des § 3 Abs. 2 des Entwurfs gerade vom Gegenteil aus. Satz 2, 2. Halbsatz dieser Vorschrift läßt nämlich die Mitteilung der Tatsache, daß der Betroffene von der Ausweispflicht befreit ist, an Behörden und *Beamte*, die zur Feststellung seiner Personalien ermächtigt sind, zu diesem Zweck zu. Bei den Beamten, die zur Feststellung der Personalien (Identitätsfeststellung) ermächtigt sind, handelt es sich im übrigen um solche mit vollzugspolizeilichen Befugnissen. Die Vorschrift des § 3 Abs. 2 des Entwurfs geht somit sehr wohl davon aus, daß Personen, denen eine Befreiung von der Ausweispflicht nach § 3 Abs. 2 des Entwurfs gewährt würde, auch einer Identitätsfeststellung durch die Polizei unterzogen werden könnten.

3. § 3 Abs. 2 des Entwurfs ist auch datenschutzrechtlich im engeren Sinne bedenklich. Der gegenteiligen Auffassung der Staatsregierung in der Begründung des Gesetzentwurfs kann nicht gefolgt werden. Um nämlich von der Ausweispflicht befreit werden zu können, haben die Betroffenen gegenüber der Personalausweisbehörde die eine Befreiung rechtfertigenden Angaben i. S. d. § 3 Abs. 2 des Entwurfs zu machen. Diese Angaben beruhen aber auf einer Vorschrift, die, wie oben dargelegt, rahmenrechtswidrig ist. Es besteht daher die Gefahr, daß die Personalausweisbehörde einen Datenbestand erhält, der jeglicher rechtlichen Grundlage entbehrt. Hinzu kommt, daß die Behörde insbesondere zur Entscheidung über ärztliche Diagnosen und Prognosen überfordert sein dürfte.

   Das Argument der Staatsregierung in ihrer Begründung zum Gesetzentwurf, bei Weglassen des Befreiungstatbestandes müßte die Behörde den Antrag am Krankenbett aufnehmen und würde folglich immer von den persönlichen Umständen des Antragstellers Kenntnis erlangen, ist nicht nachvollziehbar. Denn § 3 Abs. 2 des Entwurfs beschränkt den befreiungsberechtigten Personenkreis eben nicht auf ständig bettlägerige Personen selbst, sondern umfaßt deren Betreuer oder Vertretungsberechtigte und bezieht sich auf alle Personen, die voraussichtlich dauernd in Krankenhäusern, Pflegeheimen oder ähnlichen Einrichtungen untergebracht sind. Eine dauerhafte Unterbringung in einem Krankenhaus oder Pflegeheim bedeutet nicht zwangsläufig, daß die Betroffenen solche Einrichtungen nicht vorübergehend verlassen können oder dürfen, zumal diesem Personenkreis, wie oben ausgeführt, nicht nur dauernd bettlägerige Personen angehören. Es sind somit ohne weiteres Fälle denkbar, in denen eine Person, die unter die Vorschrift des § 3 Abs. 2 des Entwurfs fällt, den Antrag auf Ausstellung eines Personalausweises oder den Befreiungsantrag gemäß § 3 Abs. 2 des Entwurfs persönlich oder schriftlich bei der Personalausweisbehörde stellen kann. Die Personalausweisbehörde würde dann von den persönlichen Umständen des Antragstellers erst im Rahmen seines Antrags erfahren.

   Die damit verbundene Datensammlung über medizinische und soziale Daten betrifft oft tiefe Schichten der Persönlichkeit. Ihre Aufbewahrung und Nutzung ist mit hohem Verwaltungsaufwand verbunden.

   Die Daten müßten auch immer wieder aktualisiert werden, denn der ärztlichen Kunst sind keine Grenzen gesetzt. (Da kann sich auch jemand „verstecken".)
   Schließlich: Was spricht dagegen, allen über 16 Jahre alten Deutschen einen Personalausweis zu geben? Warum dieses Stigma? Das Befreiungsverfahren ist aufwendig und birgt allerlei - auch datenschutzrechtliche - Gefahren.

4. Im übrigen sieht § 2a PAuswG, der die Führung und den zulässigen Inhalt des Personalausweisregisters abschließend regelt, keine Speicherung des Datums „Befreiung von der Ausweispflicht" und der sie rechtfertigenden Gründe vor. Dies ist ebenfalls ein Indiz dafür, daß eine Befreiung von der Ausweispflicht unter bestimmten Voraussetzungen durch die Länder nicht zulässig ist.

5. Es ist weiterhin nicht nachvollziehbar, aus welchem Anlaß die Personalausweisbehörde die im Rahmen einer Befreiung von der Ausweispflicht bekannt gewor-

denen personenbezogenen Daten einer anderen Personalausweisbehörde übermitteln darf. § 3 Abs. 2 Satz 2 des Entwurfs läßt eine solche Übermittlung ausdrücklich zu. Die Begründung des Gesetzesentwurfs gibt darüber keine Auskunft.

Ich habe nachdrücklich angeregt, § 3 Abs. 2 des Entwurfs ersatzlos zu streichen. Es bleibt abzuwarten, ob meine Anregung berücksichtigt wird.

### 5.3.3 Folgen von Personenverwechslungen bei Melderegisterauskünften

Einem Petenten flatterten kürzlich Zwangsvollstreckungsankündigungen, eine gerichtliche Ladung zur Abgabe der eidesstattlichen Versicherung und eine kostenpflichtige Untersagung des Betriebes eines Fahrzeuges im öffentlichen Verkehr unter Androhung unterschiedlicher Sanktionen ins Haus.

Was war passiert?

Die Meldebehörde hatte auf verschiedene Anfragen nach der Adresse eines Mannes, der mit Vor- und Familiennamen bezeichnet war, Auskunft über die Anschrift des Petenten gegeben, der den gleichen Vor- und Familiennamen hat. Weitere Personen mit gleichlautendem Namen sind und waren im Melderegister nicht gespeichert.

Es lag eine Personenverwechslung vor. Aufgrund der Gleichheit von Vor- und Familiennamen wurde die Anschrift des Petenten bekanntgegeben, ohne daß sein im Melderegister gespeicherter akademischer Grad (Dr.) berücksichtigt worden war. In den Suchanfragen war jedenfalls kein Dr.-Grad angegeben, so daß die Meldebehörde hätte stutzig werden müssen.

Es kostete den Petenten viel Geduld, Arbeit und Ärger, die jeweiligen Stellen vom Vorliegen einer Personenverwechslung zu überzeugen.

Damit den schutzwürdigen Interessen des Petenten Rechnung getragen wird, habe ich die Meldebehörde aufgefordert, im Meldedatensatz des Petenten einen Hinweis zu speichern, der die Meldebehörde *vor* Auskunftserteilung zur besonderen Vorsicht mahnt.

Daraufhin wurde von der Meldebehörde eine Auskunftssperre gemäß § 34 Abs. 1 SächsMG im Meldedatensatz des Betroffenen gespeichert. Da eine solche Auskunftssperre grundsätzlich nur bei Melderegisterauskünften an Private wirkt, bleibt zu hoffen, daß auch bei Auskunftsersuchen von Behörden besonders sorgfältig vorgegangen wird.

Der Fall widerlegt in eindrucksvoller Weise den vielzitierten Satz „ich habe nichts zu verbergen“. Zeigt er doch, daß auch der „harmlose“ Normalbürger in die Situation kommen kann, sein Recht auf informationelle Selbstbestimmung anmahnen zu müssen, um weiteres Ungemach abzuwenden.

### 5.3.4 Verkehrssicherheitsaktion zur Verhütung von Alkoholunfällen

Der Deutsche Verkehrssicherheitsrat e. V. plante gemeinsam mit dem SMI und dem SMWA eine Verkehrssicherheitsaktion zur Verhütung von Alkoholunfällen. Junge Leute zwischen 16 und 24 Jahren sollten direkt angeschrieben und zur Eigen- und Mitverantwortung animiert werden.

Die Meldedatenübermittlungen an den Deutschen Verkehrssicherheitsrat e. V. waren als Gruppenauskunft an § 32 Abs. 3 SächsMG zu messen. Das geforderte „öffentliche Interesse“ konnte angenommen werden, weil die Verkehrssicherheitsaktion zur Verhütung von Alkoholunfällen in Anbetracht der hohen Unfallzahlen unter Alkoholeinfluß eine sinnvolle Präventivmaßnahme ist. Auswahl und Übermittlung der in Frage kommenden Meldedaten waren durch § 32 Abs. 3 SächsMG gedeckt.

Ich habe jedoch angeregt, dem Deutschen Verkehrssicherheitsrat e. V. lediglich Adreßaufkleber mit der Maßgabe zur Verfügung zu stellen, sie ohne Anfertigung einer Kopie zu verwenden. Unverbrauchte Adreßaufkleber seien zu löschen. Außerdem sollte gemäß § 32 Abs. 6 SächsMG auf die Zweckbindung hingewiesen werden.

Als datenschutzgerechtere Alternative habe ich zudem ein sog. Adreßmittlungsverfahren vorgeschlagen. Der Deutsche Verkehrssicherheitsrat e. V. sollte seine Schreiben in bereits frankierten Kuverts den Meldebehörden zur Verfügung stellen. Diese sollten dann die Kuverts mit ausgedruckten Adreßaufklebern versehen und anschließend die Briefe versenden.

Ich wies daraufhin, daß es sinnvoll sei, die Betroffenen im Anschreiben oder in einem Merkblatt über die Herkunft der Daten und über die melderechtlichen Grundlagen für eine solche Datenübermittlung bzw. Nutzung zu informieren. Damit würde denkbaren Spekulationen, daß die Gemeinde personenbezogene Daten über Alkoholkonsumenten gespeichert haben könnte, ein Riegel vorgeschoben.

### 5.3.5 Einwohnerlisten für den MDR

Der MDR hat der SK (Referat Medien) mitgeteilt, er hielte „Einwohner-Listen“ zum Abgleich und zur Auffrischung der beim MDR vorhandenen Daten für „sehr hilfreich“.

Das von der SK zur Frage der Zulässigkeit um Stellungnahme gebetene SMI kam zu dem Ergebnis, daß das SächsMG eine Überlassung von sog. Einwohner-Listen durch die Meldebehörden an die MDR-Beauftragten nicht zuließe: § 29 Abs. 1 Satz 2 SächsMG bestimme, daß die Meldebehörde personenbezogene Daten auf Listen nur dann übermitteln dürfe, wenn es sich um Daten einer Personengruppe handele. Unter Personengruppe im Sinne dieser Norm seien Einwohner erfaßt, die aufgrund vorab zu bestimmender einzelner personenbezogener Daten zusammengefaßt würden. Demzufolge dürfe die Personengruppe niemals alle Einwohner oder den überwiegenden Teil der Einwohner der Gemeinde umfassen. Die Herausgabe der Einwohner-Listen sei somit rechtswidrig.

Da das SMI seine Auffassung bereits zum nachgeordneten Bereich durchgestellt hatte, teilte ich ihm mit, daß ich im Ergebnis zwar ebenfalls zu dem Schluß gelange, daß die vom MDR gewünschten „Einwohner-Listen“ von den Meldebehörden nicht übermittelt werden dürfen; allerdings lasse sich dies nicht mit der vom SMI dargestellten Interpretation des § 29 Abs. 1 SächsMG begründen.

Grundsätzlich läßt § 29 Abs. 1 Satz 1 SächsMG Meldedatenübermittlungen - auch in Listenform - zu, wenn dies zur Aufgabenerfüllung *erforderlich* ist.

Der Datenempfänger müßte demnach angeben, welche der Daten aus dem Katalog des § 29 Abs. 1 Satz 1 SächsMG (das könnten im Extremfall alle 17 Meldedaten sämtlicher Einwohner sein) für seine Aufgabenerfüllung *erforderlich* sind.

Der MDR hat sich jedoch wegen seiner Gebühren nur für eine Personengruppe zu interessieren, die so nach Meldedaten nicht ermittelt und zusammengefaßt werden kann: Es handelt sich um diejenigen Einwohner, die ein Rundfunkgerät (Fernseher/ Radio) betreiben. Das mögen die allermeisten „Haushaltsvorstände“ sein (die so aber nicht aus den Meldedaten ermittelt werden können), nicht aber Kinder, andere Familienmitglieder oder die große Zahl der von der Rundfunkgebührenpflicht befreiten Personen.

Bezieht sich jedoch das Auskunftsbegehren (von vornherein) auf eine bestimmte Personengruppe, so dürfen der Zusammensetzung der Personengruppe keine anderen als in Satz 1 genannten Daten zugrundegelegt werden. Der Auswahlkatalog des § 29 Abs. 1 Satz 1 SächsMG sieht nämlich nicht sämtliche der in § 5 SächsMG genannten speicherungsfähigen Daten vor, so daß z. B. einer Auswahl der Personengruppe keinesfalls die Daten nach § 5 Abs. 1 Nr. 15, Nr. 16 und Abs. 2 SächsMG zugrundegelegt werden dürfen.

§ 29 Abs. 1 SächsMG bestimmt nach alledem *nicht*, daß die Meldebehörde personenbezogene Daten auf Listen *nur* dann übermitteln darf, wenn es sich um Daten einer Personengruppe handelt.

Da der MDR lediglich von „Einwohner-Listen“ spricht, ist offen, ob an Listen i. S. v. § 29 Abs. 1 Satz 1 oder Satz 2 SächsMG gedacht ist. Unabhängig davon sind solche Datenübermittlungen stets am Grundsatz der *Erforderlichkeit* zu messen. Nach meinem Dafürhalten scheidet die Übermittlung der Listen nicht wegen § 29 Abs. 1 Satz 2 SächsMG aus, sondern sinngemäß aus den in 1/5.3.3 genannten Gründen.

### 5.3.6 Erteilung von Melderegisterauskünften durch die Wegzugsbehörden bei Auskunftssperren

In Fällen einer im Melderegister eingetragenen Auskunftssperre i. S. d. § 34 SächsMG entsteht bei Wegzug des Betroffenen in den Zuständigkeitsbereich einer neuen Meldebehörde das Problem, daß die neue Meldebehörde von der bei der Wegzugsbehörde eingetragenen Auskunftssperre regelmäßig nichts erfährt, es sei denn, der Betroffene wurde gemäß § 34 Abs. 3 Satz 2 SächsMG darauf hingewiesen,

daß eine Auskunftssperre nur für die Meldebehörde gilt, für die sie beantragt wurde. Hier muß also der Betroffene die Initiative ergreifen. Die Eintragung einer Auskunftssperre im Melderegister ist im Freistaat Sachsen kostenpflichtig (30 DM pro Eintragung). Weil im Freistaat Sachsen zwischen den Meldebehörden keine Rückmeldung von Auskunftssperren erfolgt, hat der Betroffene zu seiner Sicherheit bei allen in Frage kommenden Meldebehörden die Eintragung einer Auskunftsperre (jeweils kostenpflichtig) zu beantragen. Dies kann dazu führen, daß Betroffene aus Kostengründen auf ihr Schutzrecht verzichten.

Besser wäre es im Interesse des Betroffenen, Auskunftssperren regelmäßig im Wege der Rückmeldung zwischen den beteiligten Meldebehörden (auch länderübergreifend) mitzuteilen, weil sonst die Gefahr besteht, daß eine Meldebehörde in Unkenntnis einer andernorts bestehenden Auskunftssperre, die dem Schutz von Leib, Leben, Gesundheit, persönlicher Freiheit oder ähnlicher schutzwürdigen Interessen des Betroffenen (§ 32 Abs. 4 SächsMG) dient, eine Auskunft aus dem Melderegister an Dritte erteilt. Durch eine entsprechende Ergänzung von § 1 1.BMeldDÜV, der die Rückmeldung zwischen den Meldebehörden regelt, um die Auskunftssperren würde dem Schutzrecht der Betroffenen in Sachsen im erforderlichen Maße Rechnung getragen.

Um eine bundeseinheitliche Verfahrensweise zu erreichen, habe ich beim SMI angeregt, die Problematik im Unterausschuß „Melde-, Paß- und Personalausweiswesen" des AK I der Ständigen Konferenz der Innenminister des Bundes und der Länder zu behandeln und ggf. beim BMI eine Gesetzesänderung zu fordern. Letzteres ist inzwischen geschehen.

### 5.3.7 Übermittlung von Jubiläumsdaten an den Bürgermeister

Verschiedene Bürgermeister fragten, ob die Meldebehörde berechtigt sei, ihnen die Übermittlung von Jubiläumsdaten zu verweigern.

Nach § 33 Abs. 2 SächsMG *darf* die Meldebehörde Namen, Doktorgrad, Anschriften, Tag und Art des Jubiläums von Alters- und Ehejubilaren *veröffentlichen* und an Presse, Rundfunk oder andere Medien *zum Zwecke der Veröffentlichung* übermitteln. Altersjubilare sind Einwohner, die den 70. oder einen späteren Geburtstag begehen; Ehejubilare sind Einwohner, die die goldene Hochzeit oder ein späteres Ehejubiläum begehen (§ 33 Abs. 4 SächsMG ist zu beachten).

Belz/Rimmele/Wunsch vertreten die Auffassung, daß eine Übermittlung an andere Übermittlungsempfänger unzulässig sei. Eine Ansicht, die bei verfassungskonformer Auslegung des § 33 Abs. 2 SächsMG nicht unbedingt überzeugt.

Bedenkt man nämlich, daß bei einer Übermittlung der Jubiläumsdaten an den Bürgermeister das Recht auf informationelle Selbstbestimmung der Jubilare keinesfalls mehr beeinträchtigt ist als bei einer Veröffentlichung, so ist die Übermittlung an den Bürgermeister - auch im Hinblick auf § 22 SächsMG - nicht zu beanstanden.

Aber auch wenn von dem abschließenden Charakter des § 33 Abs. 2 SächsMG ausgegangen werden sollte, halte ich die Übermittlung der Jubiläumsdaten an den Bürgermeister schon nach § 29 Abs. 1 und Abs. 7 SächsMG für zulässig. Es gehört nämlich seit alters her zu den Aufgaben eines Bürgermeisters (Landrates, Ministerpräsidenten), seinen alten Mitbürgern zu gratulieren.

Diese Rechtsauffassung wird unterstrichen durch § 4 Abs. 2 SächsMG i. V. m. §§ 13 Abs. 1, 12 Abs. 2 Nr. 2 SächsDSG, wonach die Datenübermittlung an den Bürgermeister schon deshalb zulässig ist, weil Jubiläumsdaten (gemäß § 33 Abs. 2 SächsMG) veröffentlicht werden dürfen.

Die Übermittlung der Jubiläumsdaten an den Bürgermeister hat nach *pflichtgemäßem* Ermessen zu erfolgen. Da die Jubiläumsdaten zur Aufgabenerfüllung des Bürgermeisters erforderlich sind, würde durch eine Verweigerung der Datenübermittlung gegen das Willkürverbot verstoßen. Der Bürgermeister, der seinen alten Mitbürgern gratulieren will, hat Anspruch auf die Jubiläumsdaten!

### 5.3.8 Übermittlung von Wähleranschriften aus dem Melderegister an (extremistische) politische Parteien

Nach § 33 Abs. 1 und 4 SächsMG *darf* die Meldebehörde Parteien, Wählergruppen und anderen Trägern von Wahlvorschlägen im Zusammenhang mit Wahlen zu parlamentarischen und kommunalen Vertretungskörperschaften in den *sechs* der Wahl vorangehenden Monaten Gruppenauskunft aus dem Melderegister über
- Familiennamen,
- Vornamen,
- Doktorgrad,
- gegenwärtige Anschrift

von Wahlberechtigten erteilen, für deren Zusammensetzung das Lebensalter der Betroffenen bestimmend ist und sofern die Betroffenen hiergegen nicht widersprochen haben (und wenn keine Auskunftssperre nach §§ 34 und 32 Abs. 4 SächsMG gespeichert ist oder der Betroffene für eine JVA, für ein Krankenhaus, Pflegeheim oder eine ähnliche Einrichtung i. S. v. § 20 Abs. 1 SächsMG gemeldet ist).

Nach § 33 Abs. 4 Nr. 2 SächsMG hat die Meldebehörde *zwei Monate vor Beginn der* in Abs. 1 a. a. O. genannten *Sechsmonatsfrist* auf das Widerspruchsrecht durch öffentliche Bekanntmachung hinzuweisen. Rechtsfolge der Nichteinhaltung dieser Frist ist die Unzulässigkeit von Gruppenauskünften an Parteien im Zusammenhang mit der anstehenden Wahl (Beispiel: Für die am 27. September 1998 stattfindende Bundestagswahl hätten die Meldebehörden bereits vor dem 27. Januar 1998 durch öffentliche Bekanntmachung auf das Widerspruchsrecht hinweisen müssen. Wurde diese Frist versäumt oder fand die Veröffentlichung nicht in der gebotenen Breite - also gut bemerkbar für jedermann - statt, dürfen in der verbleibenden Zeit bis zur Wahl keiner Partei Wähleranschriften mitgeteilt werden).

Über die Herausgabe von Wähleranschriften entscheidet die jeweilige Meldebehörde nach pflichtgemäßem Ermessen (die Meldebehörde „darf ...“). Dabei hat sie stets den Gleichbehandlungsgrundsatz (§ 5 Parteiengesetz) zu beachten. Entweder erhalten *alle*, also auch die von den Verfassungsschutzbehörden als extremistisch eingestuften politischen Parteien, (auf Antrag) die gewünschte Gruppenauskunft oder *keine*. Diese Auffassung findet ihre Stütze in der Rechtsprechung. Sowohl das OVG Münster (Beschl. v. 23.5.1989 - 18B 1630/89) als auch das VG Dessau (Beschl. v. 4.3.1998 - B2K 104/97) haben diese Art der Ermessensausübung bezogen auf die jeweils anstehende Wahl übereinstimmend und ausdrücklich zugunsten des Rechts auf informationelle Selbstbestimmung der Wahlberechtigten bejaht. Die Meldebehörden sind nicht gehindert, sich bei Ausübung des ihnen durch § 33 Abs. 1 SächsMG eröffneten Ermessens von den Gesichtspunkten des Datenschutzes der Wahlberechtigten leiten zu lassen, insbesondere wenn dazu im Zeitpunkt der Ermessensausübung Anlaß bestand. Beispielsweise sollten vermehrte Proteste und Widersprüche der Bürger gegen die Weitergabe ihrer personenbezogenen Daten an Parteien die Gemeinden ermutigen, ihre Entscheidung zugunsten des Rechts auf informationelle Selbstbestimmung zu treffen. Dies gilt insbesondere dann, wenn auch extremistische Parteien für die anstehende Wahl kandidieren, zumal eine Kontrolle der Einhaltung datenschutzrechtlicher Auflagen, an die solche Melderegisterauskünfte zu knüpfen sind, beim Datenempfänger kaum möglich ist (insbesondere dann, wenn sich die Partei nach der Wahl auflöst, wenn sich Verantwortliche für die in § 33 Abs. 1 Satz 4 SächsMG vorgeschriebene Löschung nicht ausmachen lassen, oder wenn die Parteiführung gleichzeitig wirtschaftliche Interessen mit Hilfe von Adreßmaterial - z. B. für einen Verlag - verfolgt).

Im Hinblick auf den jüngsten Wahlerfolg einer als extremistisch eingestuften Partei in einem Nachbarland, bei dem auch zielgruppenorientierte Melderegisterauskünfte eine bedeutsame Rolle spielten, sei den Meldebehörden eine weise und sorgfältig begründete Ermessensausübung geraten. Beispielsweise könnte ein Ratsbeschluß, generell *keiner* Partei Wähleranschriften anläßlich der bevorstehenden Wahl (oder auch für künftige Wahlen) zu übermitteln, dem Recht auf informationelle Selbstbestimmung der Wahlberechtigten ausgezeichnet Rechnung tragen. Auch muß daran gedacht werden, daß dann, wenn die in § 33 Abs. 4 Nr. 2 SächsMG vorgesehene Achtmonatsfrist zur öffentlichen Bekanntmachung der Widerspruchsmöglichkeit nicht eingehalten wurde, zumindest für die anstehende Wahl keine Wähleranschriften (an keine Partei) herausgegeben werden dürfen.

### 5.3.9 Automatisierter Abruf von Meldedaten durch die Staatsanwaltschaften des Freistaates Sachsen im On-Line-Verfahren

Im SMJus gibt es Bestrebungen, allen sächsischen Staatsanwaltschaften den Online-Zugriff auf alle sächsischen Melderegister zu ermöglichen. Die SächsMeldDÜVO sieht solche Online-Anbindungen der Staatsanwaltschaften bisher nicht vor.

Eine solche landesweite Online-Anbindung jeder sächsischen Staatsanwaltschaft an alle Melderegister in Sachsen wäre (anders als in den Stadtstaaten, wo es lediglich ein Melderegister gibt) nur mit unverhältnismäßigem Aufwand für Aufbau und Wartung eines solchen Netzes (es gibt in Sachsen z. B. ca. 30 unterschiedliche Arten von Einwohnersoftware) realisierbar. Befremdet hat mich das Ansinnen des SMJus, zur Vereinfachung der technischen Anbindung ein zentrales Melderegister (auf Landes- oder Regierungsbezirksebene) einzurichten, auf das vom zentralen Rechner der Justiz zugegriffen werden könnte. Nicht ohne Grund hat man das Zentrale Einwohnermelderegister (ZER) der DDR nach der Wende aufgelöst. Das SächsMG bestimmt deshalb, daß die Meldebehörden die Gemeinden sind, die das Melderegister zu führen haben.

Nicht zuletzt wegen der mit Online-Anbindungen einhergehenden besonderen Gefährdung des Rechts auf informationelle Selbstbestimmung rate ich dringend von einer Forcierung des Anliegens des SMJus ab.

## 5.4 Personenstandswesen

### Ausstellung von Personenstandsurkunden an Rechtsanwälte

Durch eine Eingabe erfuhr ich, daß ein Standesamt Rechtsanwälten, die ein „rechtliches Interesse“ an Personenstandsdaten glaubhaft machten, *stets* Personenstands*urkunden* zur Verfügung gestellt hat.

Dabei wurde übersehen, daß §§ 61 Abs. 1 PStG, 86 Abs. 1 DA mehrere Möglichkeiten vorsieht, nämlich

- Einsicht in Personenstandsbücher
- Durchsicht von Personenstandsbüchern
- Auskunft aus Personenstandsbüchern
- Erteilung von Personenstandsurkunden.

Bei einer Entscheidung, auf welche Weise dem Ersuchen des Rechtsanwaltes entsprochen werden soll, ist der Verhältnismäßigkeitsgrundsatz zu beachten. Danach muß eine Maßnahme geeignet, erforderlich und angemessen sein. In aller Regel dürfte eine standesamtliche Bestätigung über den aktuellen Namen des Betroffenen für den Auskunftsbegehrenden ausreichen. Die Erteilung von Personenstandsurkunden, in denen meist mehr Daten als erforderlich eingetragen sind, dürfte daher ein Ausnahmefall sein.

Auf meine diesbezügliche Beratung hat das Standesamt prompt reagiert. Dem Ersuchen von Rechtsanwälten wird künftig in der Regel mit standesamtlichen Bestätigungen über den aktuellen Namen der Betroffenen entsprochen. Die Erteilung von Personenstandsurkunden erfolgt nur noch in absoluten Ausnahmefällen.

## 5.5 Kommunale Selbstverwaltung

### 5.5.1 Offenlegung der Einkommens- und Vermögensverhältnisse bei Stundungsanträgen

Petenten beschwerten sich, daß sie bei Antrag auf Stundung der Abwassergebühren vor der Gemeinde ihre Einkommens- und Vermögenssituation in allen Einzelheiten schildern mußten.

Meinen Feststellungen zufolge orientieren sich die Gemeinden an einer Musterrichtlinie über die Stundung von Wasser- und Abwasserbeiträgen, die vom SMI erarbeitet und vom SSG publiziert und zur Anwendung empfohlen wurde. Darin werden einige Angaben von den Betroffenen verlangt, deren Erforderlichkeit ich aus datenschutzrechtlicher Sicht in Frage stelle.

Z. B. halte ich die Frage nach den im Haushalt lebenden Personen mit eigenem Einkommen (netto-monatlich) ebenso für problematisch wie das Kriterium „monatliches Familieneinkommen“. Auch die Frage nach dem *Grund* (Gefängnis, Psychiatrie, Krebskrankenhaus?) der vorübergehend abwesenden zum Haushalt gehörenden Personen dürfte gegen das Übermaßverbot verstoßen.

Wegen der grundsätzlichen Bedeutung habe ich mich mit dem SMI und dem SSG in Verbindung gesetzt, um für alle Anwender der Richtlinie Rechtssicherheit zu erreichen. Ich gehe davon aus, daß das Erörterungsergebnis zu gegebener Zeit ebenfalls durch den SSG veröffentlicht wird.

Selbstverständlich haben die Schuldner im für die Entscheidung über den Stundungsantrag erforderlichen Umfang ihre persönlichen Verhältnisse hinreichend darzulegen, um § 3 Abs. 1 Nr. 5 SächsKAG i. V. m. § 222 AO zu entsprechen. Dies geschieht zweckmäßigerweise durch Einreichung eines Liquiditätsstatus, aus dem sich eine Gegenüberstellung der flüssigen bzw. kurzfristig realisierbaren Vermögenswerte und der rückständigen bzw. kurzfristig fälligen Verpflichtungen ergibt. Nur bei Beitragsschulden von größerem Umfang kann eine Vermögensübersicht angebracht sein, verbunden mit Ausführungen darüber, aus welchen Gründen die Verwertung von Vermögensteilen zwecks sofortiger Entrichtung der Beitragsschuld nicht zumutbar ist (vgl. BFH, 13.4.61, BStBl. III, S. 292).

Die Musterrichtlinie samt Stundungsantragsformular nimmt auf diese Gegebenheiten nicht hinreichend Rücksicht. Gemäß Nr. III 1 haben die Betroffenen in jedem Fall - also unabhängig von der Höhe der Beitragsschuld - sämtliche Fragen wahrheitsgemäß und vollständig zu beantworten *und durch Nachweise zu belegen*. Dies halte ich für unverhältnismäßig.

Bis zu einer endgültigen Klärung rate ich deshalb, die Datenerhebung - gemessen am konkreten Einzelfall - auf das jeweils erforderliche Maß zu reduzieren. Bei der Beratung von Stundungsanträgen im Gemeinderat sollten die Ratsmitglieder eindringlich über ihre Verschwiegenheitspflichten belehrt werden.

### 5.5.2 Unbefugte Preisgabe von personenbezogenen Daten über Petenten durch ein Stadtratsmitglied

Bei einer öffentlichen Parteiveranstaltung veröffentlichte ein Stadtratsmitglied einen Lageplan, den er in seiner Eigenschaft als Berichterstatter des städtischen Petitionsausschusses zu bearbeiten hatte. Der in der Parteiversammlung vorgezeigte Lageplan wies neben der Petitionsnummer die Häuser von vier Petenten auf, die dort farblich und namentlich gekennzeichnet waren. Das Stadtratsmitglied nutzte diesen Lageplan für politische Zwecke, indem er in der Versammlung der Partei durch Hinweis auf die Lage der Häuser der Petenten den aus seiner Sicht wahren Grund für die Einreichung der Petition, nämlich die Wahrung der eigenen Wohnruhe, darlegen wollte.

Es widerspricht in jeder Hinsicht datenschutzrechtlichen Grundsätzen, wenn ein Stadtratsmitglied in seiner Eigenschaft als Berichterstatter zu einer Petition Namen von Petenten öffentlich preisgibt, die sich vertrauensvoll in ihrer Angelegenheit an den städtischen Petitionsausschuß gewandt haben.

Durch die Veröffentlichung personenbezogener Daten der Petenten verstieß das Stadtratsmitglied gegen seine Geheimhaltungspflichten (§ 37 Abs. 2 SächsGemO). Angelegenheiten, die ihrer Natur nach nur in nicht-öffentlichen Ausschußsitzungen behandelt werden können, wie es z. B. bei Petitionen der Fall ist, sind nicht für die Öffentlichkeit bestimmt und insofern vertraulich zu behandeln. Petenten müssen darauf vertrauen können, daß ihre Anliegen nicht für parteipolitische Zwecke zweckentfremdet werden. Das Recht des Einzelnen auf informationelle Selbstbestimmung beinhaltet auch das Recht, zu bestimmen, wer wann welche Daten über seine Person erhält. Die unbefugte Preisgabe von personenbezogenen Daten, wie sie hier erfolgte, läßt sich mit Artikel 33 SächsVerf nicht vereinbaren. Es gibt keine gesetzliche Grundlage, welche eine Veröffentlichung von Daten der Petenten in einer Versammlung einer Partei gerechtfertigt hätte. Sie war Folge einer unzulässigen Verknüpfung der Ausschußtätigkeit des Stadtratsmitglieds mit der ihm als Mitglied seiner Fraktion im Stadtrat sicherlich auch obliegenden öffentlichen politischen Betätigung. Der Berichterstatter einer Petition muß sich über deren Inhalt und politische Wertung jeder öffentlichen persönlichen Äußerung enthalten. Ferner sollte ein Mitglied des Stadtrates nur in solchen Petitionsangelegenheiten tätig werden, zu denen eine eigene politische Affinität nicht besteht. Nur so kann der Eindruck vermieden werden, die Petition werde nicht sachlich neutral behandelt.

Da ich unter Berücksichtigung der einsichtigen Stellungnahme des Stadtratsmitglieds davon ausgehen konnte, daß er die Belange des Datenschutzes bei seiner Tätigkeit als Stadtratsmitglied künftig beachten wird, hielt ich eine förmliche Beanstandung gemäß § 26 SächsDSG für nicht erforderlich.

### 5.5.3 Grenzüberschreitende kommunale Zusammenarbeit (Staatsvertrag Brandenburg - Sachsen)

Der Entwurf eines Staatsvertrags zwischen dem Land Brandenburg und dem Freistaat Sachsen über die grenzüberschreitende kommunale Zusammenarbeit in Zweckverbänden und durch Zweckvereinbarungen legt in Art. 2 fest:

*„Soweit in diesem Staatsvertrag nichts anderes geregelt ist, gilt*

1. *für Zweckverbände das Recht der kommunalen Zusammenarbeit des Landes, in dem der Zweckverband seinen Sitz hat oder haben soll,*
2. *für Zweckvereinbarungen das Recht der kommunalen Zusammenarbeit des Landes, dem die Körperschaft angehört, der durch die Vereinbarung die Erfüllung oder Durchführung der Aufgabe übertragen worden ist oder werden soll.*“

Zur Klarstellung hatte ich angeregt, anstelle der Beschränkung auf das „*Recht der kommunalen Zusammenarbeit*“ allgemein auf das *Recht des jeweiligen Sitzlandes* abzustellen, wie es in den entsprechenden Staatsverträgen mit Bayern und Sachsen-Anhalt geregelt ist. Davon wäre auch das Datenschutzrecht umfaßt und somit eindeutig auch die Zuständigkeit des Landesbeauftragten für den Datenschutz geregelt.

Auch wenn das SMI meinen Vorschlag nicht aufgegriffen hat, gehe ich davon aus, daß mit dem Sitzlandprinzip neben dem Datenschutzrecht allgemein auch die Zuständigkeit des jeweiligen Landesbeauftragten für den Datenschutz geregelt ist. Befindet sich der Sitz eines länderübergreifenden Zweckverbandes beispielsweise in Brandenburg, so handelt es sich um eine öffentliche Stelle Brandenburgs in der allerdings auch sächsische Daten verarbeitet werden; es gilt aber das Datenschutzrecht des Landes Brandenburg mit der Folge brandenburgischer Kontrollbefugnis und umgekehrt.

### 5.5.4 Firmenpräsentation durch eine Gemeinde im Internet

Eine Gemeinde beabsichtigte, ihre Internetseiten um Namen, Anschriften, Telefonnummern und Öffnungszeiten von Ärzten, Notrufen, Pflegediensten und Gewerbetreibenden zu erweitern und wollte hierzu jeweils die Einwilligung der Betroffenen einholen. Sie hatte insofern keine Bedenken, weil die Daten dem Telefonbuch, der lokalen Presse oder anderen Werbungen zu entnehmen seien.

Obwohl die Daten bereits öffentlich zugänglich sind, gehört ihre Internetpräsentation nicht zu den gesetzlichen Aufgaben der Gemeinde. Nach § 2 Abs. 1 SächsGemO erfüllen die Gemeinden *in ihrem Gebiet* im Rahmen ihrer Leistungsfähigkeit alle öffentlichen Aufgaben. Die weltweite Präsentation der Namen, Anschriften, Telefonnummern ist nicht mehr von dieser (gesetzlichen) Aufgabenzuweisung gedeckt. Es läge also ein Verstoß gegen den verfassungsrechtlichen Grundsatz der Gesetzmäßigkeit der Verwaltung vor, der auch einer Einwilligung Grenzen setzt. Bei Gewerbetreibenden setzt darüber hinaus § 14 Abs. 8 GewO Grenzen, wonach eine Übermittlung (hier Veröffentlichung) nur zulässig ist, wenn der Auskunftsbegehrende ein berechtigtes Interesse an der Kenntnis der Daten glaubhaft macht. Da es keinen Auskunftsbegehrenden gibt, ist die Veröffentlichung von Gewerbetreibendendaten im Internet zwangsläufig unzulässig.

Selbstverständlich steht es jedem Betroffenen frei, sich selbst im Internet zu präsentieren.

### 5.5.5 Einrichtung eines „Bürgerbüros“

Die Stadt Coswig hat mich in vorbildlicher Weise bereits in der Planungsphase für ein neues Rathaus beteiligt, damit Datenschutzaspekte bei den Baumaßnahmen von vornherein berücksichtigt werden können. Insbesondere die beabsichtigte Einrichtung eines „Bürgerbüros“ im neuen Rathaus war Anlaß für meine datenschutzrechtliche Beratung.

Eine neue Variante bürgerorientierter Verwaltung ist die Zusammenfassung verschiedener Fachbereiche in Organisationseinheiten, die eine ganze Reihe von Aufgaben in einer Hand erledigen und dadurch dem Bürger nur einen Ansprechpartner geben. In solchen Organisationseinheiten erhalten jedoch Mitarbeiter bei der Bearbeitung der einen Aufgabe Kenntnisse, die sie für eine andere Aufgabe, die sie ebenfalls wahrnehmen, nicht haben dürfen (z. B. Sozialhilfeempfänger stellt Bauantrag oder wird zur Grundsteuer oder Gewerbesteuer veranlagt). „Bündelungsbehörden“ wie Stadtverwaltungen und Kreisverwaltungen bestehen aus vielen, aus Gründen des Datenschutzes voneinander separierten öffentlichen Stellen. Daten dürfen dort nicht frei übermittelt werden.

In kleineren Gemeinden ist dies kein neues Problem, denn dort sind seit jeher verschiedene Aufgaben, die voneinander abzugrenzen wären, auf einen oder wenige Mitarbeiter konzentriert. Datenschutz im Sinne der Abschottung von Suchgebieten ist im Kopf *eines* Mitarbeiters eben nicht zu verwirklichen.

Das Problem erlangt aber eine neue Qualität, wenn die Arbeit technikunterstützt erledigt wird. Der Zugang zu Informationen über in automatisierten Verfahren gespeicherten Daten verschiedener Sachgebiete ist sekundenschnell und umfassend möglich. Damit wächst jedoch für die Bürger die Gefahr, daß ihr Recht auf informationelle Selbstbestimmung verletzt wird. Diese Gefahr resultiert allerdings nicht nur aus der Verknüpfbarkeit von kommunalen Datenbeständen. Vielmehr bereitet die erforderliche Abschottung der einzelnen Bürgerbüro-Arbeitsplätze enorme Probleme, nicht zuletzt finanzieller Art. Wie kann wirkungsvoll verhindert werden, daß Bürger, die in der Wartezone warten oder die an verschiedenen Schreibtischen „bedient“ (beraten, belehrt) werden, nichts von den Problemen der anderen erfahren? Sicher kann man mit Stellwänden, Zimmerpflanzen, Geräuschkulissen wie z. B. Springbrunnen das Risiko des Mithörens reduzieren. Dabei wächst jedoch die Gefahr der Unübersichtlichkeit. Erfolgt die Sachbearbeitung nämlich in einzelnen Büroräumen, kann dem Recht auf informationelle Selbstbestimmung anders als in einem als Großraumbüro angelegten Bürgeramt, auch bei kurzfristigem Verlassen des Zimmers, durch Abschließen der Tür Rechnung getragen werden. Auf dem Schreibtisch befindliche personenbezogene Unterlagen oder ein nicht abgeschalteter PC sind dadurch vor unbefugtem Zugriff sicherer als im durch Trennwände u. ä. unübersichtlichen Großraumbüro.

Den planenden Architekt sowie die verantwortlichen städtischen Bediensteten konnte ich überzeugen, daß die erforderliche Abwägung der verfassungsrechtlich verbrieften Rechte der Stadt (Organisationshoheit - Art. 82 Abs. 2 SächsVerf) und der betroffenen Bürger (Recht auf informationelle Selbstbestimmung - Art. 33 SächsVerf) im

Wege der praktischen Konkordanz zugunsten des Persönlichkeitsrechts ausfallen muß. Von dem Vorhaben, ein Bürgerbüro als Großraumbüro einzurichten, habe ich dringend abgeraten.

### 5.5.6 Beauftragung eines Inkassobüros mit der Vorbereitung von Vollstreckungsmaßnahmen der Gemeinden

Die Creditreform Dresden beabsichtigt den sächsischen Gemeinden anzubieten, ihnen beim Einzug ihrer privatrechtlichen und öffentlich-rechtlichen Forderungen einschließlich Mahnverfahren und bei der Vorbereitung von Vollstreckungsmaßnahmen behilflich zu sein. U.a. beruft sie sich auf § 87 SächsGemO, wonach die Gemeinde die Kassengeschäfte ganz oder zum Teil von einer Stelle außerhalb der Gemeindeverwaltung besorgen lassen kann, wenn die ordnungsgemäße und sichere Erledigung und die Prüfung nach den für die Gemeinde geltenden Vorschriften gewährleistet sind.

In der gegenwärtigen Meinungsbildungsphase habe ich eine Umfrage bei den anderen Landesbeauftragten für den Datenschutz gestartet und befinde mich mit dem SMI im Dialog.

Vorsorglich habe ich folgendes zu bedenken gegeben: Öffentlich-rechtlichen Forderungen im Zusammenhang mit Vollstreckungen liegen regelmäßig sensible Daten zugrunde, die tief in die Privatsphäre der Betroffenen - insbesondere in deren finanzielle Verhältnisse - eindringen und die vielfach besonderen Amtsgeheimnissen (z. B. Steuergeheimnis, Sozialgeheimnis, Betriebs- und Geschäftsgeheimnisse) unterliegen, so daß eine Auftragsvergabe an private Inkassobüros nach meinem Dafürhalten wohl rechtswidrig sein dürfte.

Daß solche Informationen für Inkassobüros, die gleichzeitig, wie die Creditreform, Kreditauskunfteien sind, in der Gesamtschau ihres Geschäftszwecks solcher Unternehmen von unschätzbarem Wert wären, ist ein weiteres Indiz für eine besondere Inkompatibilität. Die nach § 87 SächsGemO vorgeschriebene „ordnungsgemäße und sichere Erledigung“ scheint mir deshalb nicht gewährleistet zu sein. Denn die Daten aus dem Inkassogeschäft wandern mit Uhrwerkssicherheit in die Datensammlung der Auskunftei, die bei der Creditreform zentral in Neuß/Rhein geführt wird. Man denke daran, daß wegen rückständiger Gewerbesteuer in einen Gewerbebetrieb vollstreckt wird und dabei die wesentlichen Kreditverhältnisse des Betriebes zutage treten.

Außerdem vertrete ich die Auffassung, daß Vollstreckungen (einschließlich deren Vorbereitung) nach dem Sächsischen Verwaltungsvollstreckungsgesetz (SächsVwVG) zum Kernbereich hoheitsrechtlicher Verwaltung gehören und nicht auf private Inkassobüros übertragen werden können. Repression ist ausschließlich staatliche Aufgabe; sie kann ohne klare gesetzliche Vorschrift nicht auf irgendwelche Private übertragen werden.

Aus diesen Gründen heraus habe ich erhebliche Vorbehalte gegen eine Übertragung der in Rede stehenden behördlichen Aufgaben auf die Creditreform.

Im übrigen sind die Kommunen gut beraten, ihre Forderungen insbesondere bei Ortsansässigen selbst einzutreiben: Nur so kann mit dem nötigen Nachdruck und - je nach Fallkonstellation - mit der nötigen Sensibilität (z. B. inbezug auf Stundungen oder die Gefährdung von Arbeitsplätzen) vollstreckt werden.

### 5.5.7 Unbefugtes Kopieren einer Feuerwehrmitgliederliste durch einen städtischen Bediensteten

Ein städtischer Bediensteter wurde von der Wehrleitung einer Freiwilligen Feuerwehr dabei ertappt, als er in den Diensträumen der Feuerwehr eine Mitgliederliste kopierte, nachdem er sich mit dem Schlüssel, den er vom Bürgermeisteramt erhalten hatte, Zugang zu den Unterlagen verschafft hatte.

Die zur Stellungnahme aufgeforderte Stadtverwaltung bestätigte den Vorfall und teilte mit, daß der Bedienstete *„zum einen von dem Stadtfeuerwehrausschuß und zum anderen durch die zuständige Sachbearbeiterin im Ordnungsamt der Stadt beauftragt“* worden war, die Mitgliederliste zum Zwecke der Einladung zur Gesamthauptversammlung inklusive der Wahl zum Stadtbrandmeister vorzulegen. Der städtische Bedienstete, der gleichzeitig „Kamerad“ der Freiwilligen Feuerwehr sei, besitze einen Schlüssel zum Schrank und sei legitimiert, die Unterlagen einzusehen.

Wegen der völlig gegensätzlichen Ausführungen der Wehrleitung und der Gemeinde zu dem „Vorfall“, habe ich zunächst *im Interesse des Gemeindefriedens* eine unbürokratische Beilegung des Konflikts - allerdings fruchtlos - angeregt. Die Stadtverwaltung hielt wenig flexibel daran fest, daß der städtische Bedienstete jederzeit auf die feuerwehrinternen Unterlagen zugreifen dürfe. Dabei hat sie entscheidende datenschutzrechtliche Aspekte übersehen.

Zwar obliegt der vorbeugende und abwehrende Brandschutz gemäß § 2 SächsBrandSchG den *Gemeinden*. Die Freiwillige Feuerwehr ist gemäß § 8 Abs. 1 SächsBrandSchG eine *Einrichtung der Gemeinde* ohne eigene Rechtspersönlichkeit. Daraus folgt, daß die Freiwillige Feuerwehr der Gemeinde Unterlagen, die für deren Aufgabenerfüllung nach dem SächsBrandSchG und der Feuerwehrsatzung erforderlich sind, nicht vorenthalten darf.

Jedoch hätte die Beschaffung von Mitgliederdaten der Freiwilligen Feuerwehr zur Vorbereitung einer Versammlung/Wahl nicht über den Kopf der Wehrleitung hinweg erfolgen dürfen. Die Freiwillige Feuerwehr ist nämlich datenschutzrechtlich (unter Beachtung des funktionalen Stellenbegriffs) eine eigenständige „speichernde“ bzw. „datenverarbeitende“ Stelle und damit verantwortliche „Herrin der Daten“ (vgl. §§ 2 Abs. 1, 3 Abs. 3 SächsDSG). Sie ist insbesondere verpflichtet, sämtliche personellen, technischen und organisatorischen Maßnahmen zur Gewährleistung des Datenschutzes zu treffen (§ 9 SächsDSG). Diese Verantwortung der Freiwilligen Feuerwehr wird jedoch ad absurdum geführt, wenn die Wehrleitung nicht mehr wissen kann, wer sich wann aus welchem Anlaß welche Daten aus ihren Unterlagen besorgt hat. Die (heimliche) Datenbeschaffung durch den städtischen Bediensteten ist daher ohne Mitwirkung der Wehrleitung rechtswidrig. Selbstverständlich hat die Freiwillige Feuerwehr

auf begründete Anforderung der Stadt zur Erfüllung feuerwehrrechtlicher Aufgaben die *erforderlichen* Daten unter den Voraussetzungen des § 13 SächsDSG zu übermitteln.

Die Stadtverwaltung hat inzwischen organisatorisch sichergestellt, daß künftig ausschließlich die Wehrleitung der Freiwilligen Feuerwehr Zugriff auf die Mitgliederdaten hat.

### 5.5.8 Behandlung von Behördenpost in der kommunalen Poststelle

Nach Art. 28 Abs. 2 GG, Art. 82 Abs. 2 SächsVerf obliegt den Gemeinden im Rahmen ihres Selbstverwaltungsrechts u. a. die Organisationshoheit, aufgrund derer die Behandlung von Behördenpost z. B. in einer Dienstanweisung geregelt werden kann.

Wiederholt fielen mir Postordnungen auf, die undifferenziert vorsehen, daß mit Ausnahme von erkennbarer Privatpost sämtliche Postsendungen in einer zentralen Poststelle geöffnet und nach der Registrierung zumeist durch Boten oder durch Ablage in unverschlossenen Abholfächern an die zuständigen kommunalen Ämter weitergeleitet werden. Solchermaßen behandelte Dienstpost mit personenbezogenem Inhalt, der häufig auch besonderen Amtsgeheimnissen (z. B. Personalgeheimnis, Steuergeheimnis, Sozialgeheimnis) unterliegt, führt die Pflicht, die nach § 9 Abs. 2 SächsDSG erforderlichen Maßnahmen zur Gewährleistung des Datenschutzes zu treffen, ad absurdum.

Ich habe deshalb stets dafür plädiert, eingehende Behördenpost grundsätzlich ungeöffnet an die einzelnen Fachbereiche weiterzuleiten. Zumindest sollte aber geregelt werden, daß erkennbar für sensible Bereiche bestimmte Post, wie z. B. an Steueramt, Sozialamt, Jugendamt, Personalstelle, Standesamt (siehe hier auch § 22 Abs. 2 Satz 2, letzter Halbsatz DA), Einwohner-/Paßamt und den behördlichen Datenschutzbeauftragten stets ungeöffnet weitergeleitet wird. Eine Öffnung in der zentralen Poststelle kommt allenfalls für Dienstpost in Betracht, die äußerlich keinem Fachbereich zugeordnet werden kann. In solchen Fällen ist jedoch dafür Sorge zu tragen, daß die in der Poststelle (ausnahmsweise) geöffnete Post auf dem Weg zur zuständigen Stelle vor unbefugtem Zugriff gesichert wird (vgl. § 9 Abs. 2 Nr. 2 SächsDSG). Offene Abholfächer sind denkbar ungeeignet und werden von mir beanstandet.

### 5.5.9 Dezentrale Postöffnung in den einzelnen Dezernaten eines Landratsamtes

Ein Landratsamt beabsichtigte, den Vorschlag aus 3/14.8 umzusetzen und die für die Dezernate Gesundheitswesen, Jugend und Soziales eingehende Post nicht mehr in der zentralen Poststelle zu öffnen, sondern sie verschlossen den betreffenden Dezernaten zuzuleiten. Das Landratsamt befürchtete jedoch, daß bei einer solchen Verfahrensweise der Eingangsstempel auf einem Schriftstück vor Gericht keinen Beweiswert mehr habe. Dazu habe ich folgendes gesagt:

Ein Schriftstück ist an dem Tag zugegangen, an dem es in die Verfügungsgewalt des Adressaten gelangt. Behörden dokumentieren dieses Datum durch einen Posteingangsstempel auf dem Schriftstück oder - falls der Brief ungeöffnet weitergeleitet wird - auf dem Umschlag. Das so dokumentierte Datum beweist den Tag des Zugangs, es sei denn, das Datum ist verfälscht oder gibt nicht den wirklichen Eingangszeitpunkt wieder (z. B. falsch eingestellter Eingangsstempel, Blockierung der Klappe des Nachtbriefkastens, der für den Posteinwurf nach Dienstschluß vorgesehen ist). Dies dürfte die Ausnahme sein und kann in der Regel nachgeprüft und durch eine Datumsberichtigung korrigiert werden.

Macht ein Betroffener für den früheren Zugang Gründe geltend, die nicht nachprüfbar sind, und ist das Eingangsdatum entscheidend für einen Rechtsvorteil oder eine Fristwahrung, so ist zugunsten des Betroffenen der rechtzeitige Eingang anzunehmen, wenn die Gründe glaubhaft gemacht werden (Kopp, Kommentar zum Verwaltungsverfahrensgesetz, 6. Auflage 1996, Rdnr. 30 ff. zu § 31 und Rdnr. 12 zu § 32 mit zahlreichen Hinweisen auf die Rechtsprechung zur Fristwahrung).

Der Beweiswert eines in der zentralen Poststelle angebrachten Eingangsstempels ist nicht höher als der im Dezernat angebrachte. Da jedoch der Tag des Eingangs in der zentralen Poststelle maßgebend ist, muß organisatorisch sichergestellt werden, daß die für ein Dezernat bestimmte Post dieses Eingangsdatum erhält. Die Post muß also noch am Eingangstag dem Dezernat zugehen, dort geöffnet und dann mit dem Eingangsstempel versehen werden. Falls dies aus örtlichen oder personellen Gründen generell oder im Ausnahmefall nicht möglich ist, müßte das tatsächliche Eingangsdatum durch Abstempeln der Umschläge in der zentralen Poststelle festgehalten werden. Bei Fristsachen wären die abgestempelten Umschläge zu den Akten zu nehmen. Fehlt der Umschlag und wird von einem Betroffenen ein früherer Zugang geltend gemacht, kann ich mir vorstellen, daß im Streitfalle die Behörde dies gegen sich gelten lassen muß.

### 5.5.10 Öffnen von für die Verwaltungsgemeinschaft bestimmte Behördenpost durch den Bürgermeister einer Mitgliedsgemeinde

Einige Gemeinden haben sich zu einer Verwaltungsgemeinschaft zusammengeschlossen und einer leistungsfähigen Stadt das Melde- und Paßwesen, das Gewerbe- sowie das Standesamtswesen zur selbständigen Aufgabenerledigung übertragen.

Eingehende Behördenpost, die zwar (irrtümlich?) an eine Mitgliedsgemeinde adressiert, jedoch durch die Zusätze wie „Einwohnermeldeamt“, „Paßamt“, „Gewerbeamt“, „Standesamt“ erkennbar für die die Aufgaben erledigende Stadt bestimmt war, wurde dennoch durch den Bürgermeister geöffnet, zur Kenntnis genommen und anschließend an die zuständige Stelle weitergeleitet. Ein Öffnen der Standesamtspost durch den Bürgermeister war schon im Hinblick auf § 22 Abs. 2 DA rechtswidrig, wonach die Post dem Standesamt *ungeöffnet* zuzuleiten ist.

Der von mir beratene Bürgermeister zeigte sich zunächst uneinsichtig und öffnete - mit Ausnahme der Standesamtspost - weiterhin die erkennbar nicht für seine Gemein-

de bestimmte Post; schließlich sei „*im deutschen Rechtsstaat alles erlaubt, was nicht ausdrücklich per Gesetz verboten ist*“. Hier irrte der Bürgermeister - und zwar grundsätzlich.

Erst meine Hinweise auf Art. 3 Abs. 3 SächsVerf, wonach die vollziehende Gewalt an *Gesetz und Recht* gebunden ist und die daraus resultierenden Grundsätze
- Vorrang des Gesetzes = kein Handeln gegen ein Gesetz
- Vorbehalt des Gesetzes = kein Handeln ohne Gesetz
und auf Art. 10 GG, Art. 27 SächsVerf wonach das unbefugte Öffnen von Post unzulässig und nach § 202 Abs. 1 StGB unter Strafe gestellt ist, brachten den Bürgermeister schließlich zur Räson.

### 5.5.11 Offene Zustellung von Behördenpost einer Gemeinde

Ein Petent teilte mit, sein minderjähriger Sohn sei verdächtigt worden, ein Buswartehäuschen beschädigt zu haben. Deshalb sei er von der Gemeinde zu einer Anhörung vorgeladen worden. Pikanterweise sei die „Vorladung“ offen, d. h. ohne Umschlag einem Nachbarn, also einem unbeteiligten Dritten, zur Weiterleitung an den Petenten ausgehändigt worden.

Die Zustellung dieses offenen Schreibens ist ein Verstoß gegen § 9 Abs. 2 Nr. 2 SächsDSG, wonach es u. a. zu verhindern gilt, daß Datenträger unbefugt gelesen werden. Ich habe die Gemeinde aufgefordert, künftig von offenen Zustellungen über unbeteiligte Dritte abzusehen und die im Zusammenhang mit den „Vorladungen“ angefallenen personenbezogenen Daten, die zur Aufgabenerfüllung der Gemeindeverwaltung nicht (mehr) erforderlich sind, zu löschen (§ 19 Abs. 2 Nr. 2 SächsDSG).

Zudem ist es Aufgabe der Polizei und nicht der Gemeinde, Straftaten aufzuklären. Wenn die Gemeinde als (privater) Eigentümer des Buswartehäuschens klären will, ob und gegen wen ihr Schadensersatzforderungen zustehen, so darf sie das tun, hat aber obrigkeitliche Methoden, z. B. „Vorladungen“ zu unterlassen.

Die Gemeinde hat mir für die Zukunft eine ordnungsgemäße Zustellung ihrer Schreiben zugesagt.

## 5.6 Baurecht; Wohnungswesen

#### Veröffentlichung personenbezogener Daten im Enteignungsverfahren

Ein Petent beklagte sich, im Zusammenhang mit einem Enteignungsverfahren sei sein voller Name und seine Adresse im Amtsblatt der Gemeinde veröffentlicht worden.

Nach § 108 Abs. 5 Satz 1 BauGB ist die Einleitung des Enteignungsverfahrens (§§ 104 ff. BauGB) u. a. unter Bezeichnung des betroffenen Grundstücks und des im Grundbuch eingetragenen Eigentümers ortsüblich bekanntzumachen. Dies dient vor allem der Interessenwahrung von Inhabern eines nicht im Grundbuch eingetragenen

Rechts oder eines das Grundstück belastenden Rechts (z. B. durch Erbschaft, Zuschlag im Zwangsversteigerungsverfahren, ein obligatorisches Vorkaufsrecht, Besitz- oder Nutzungsrechte aus Miete oder Pacht).

Für die Bekanntgabe des Namens des im Grundbuch eingetragenen Eigentümers ist § 108 Abs. 5 BauGB eine ausreichende Grundlage. Die Bekanntgabe der Anschrift ist unzulässig. Sie ist weder gesetzlich normiert noch erforderlich, um das betroffene Grundstück und seinen Eigentümer hinreichend klar zu benennen.

## 5.7 Statistikwesen

### 5.7.1 EG-Fremdenverkehrsstatistik

Durch einen Zeitungsartikel wurde ich darauf aufmerksam, daß das Statistische Landesamt angefangen hatte, eine Befragung durchzuführen, bei der zufällig ausgewählte Haushalte telefonisch darüber befragt wurden, ob sie Privat- oder Dienstreisen durchführten und wie lange diese jeweils dauerten.

Als ich von dem Vorgang Kenntnis erhielt, war das Statistische Landesamt gerade dabei, Daten statistisch zu erfassen, die gemäß (Teil C des Anhanges) der EU-Richtlinie zur Fremdenverkehrsstatistik (Richtlinie 95/57/EG über die Erhebung statistischer Daten im Bereich des Tourismus vom 23. November 1995; Amtsblatt der Europäischen Gemeinschaften Nr. L 291/32) der EG-Kommission zur Verfügung zu stellen sind.

Diese Richtlinie ist - wie leider viele - vertragswidrig nicht in deutsches Recht umgesetzt worden. Daher stellt sie keine ausreichende Rechtsgrundlage für Grundrechtseingriffe und damit auch für die Erhebung und Weiterverarbeitung personenbezogener Daten dar. Nach der Rechtsprechung des Europäischen Gerichtshofs kann sich eine innerstaatliche Behörde nicht zu Lasten eines Einzelnen auf eine Bestimmung einer noch nicht umgesetzten Richtlinie berufen (sondern nur auf die innerstaatliche Rechtsvorschrift, mittels welcher die Richtlinie umgesetzt wird, vgl. Europäischer Gerichtshof Slg. 1987, S. 3969, 3985 f. - Kolpinghuis Nijmegen). Das bedeutet insbesondere: Amtliche Statistiken dürfen in Deutschland nicht unmittelbar, d. h. ohne Transformationsakt, auf der Grundlage einer EG-Richtlinie durchgeführt werden.

Das SMI hat sich meiner Rechtsauffassung angeschlossen und das Statistische Landesamt angewiesen, die Erhebung endgültig einzustellen.

Über den BfD war der Hintergrund der Angelegenheit zu erfahren, und der ist befremdlich genug:
Die betreffende Statistik geht mit dem genannten Teil C des Erhebungsprogrammes über das hinaus, was wir in Deutschland auf der Grundlage des Beherbergungsstatistikgesetzes zu erfassen gewohnt sind und was, wie mir scheint, erst recht für eine EU-weite Betrachtung des Fremdenverkehrswesens voll ausgereicht hätte. Ich darf mir dieses laienhafte Urteil erlauben, denn es wird von der Bundesregierung, also auf

der Grundlage des nötigen Sachverstandes, geteilt: Sie hat sich im Rat der EU gegen die Durchführung einer so ausgedehnten Statistik ausgesprochen und folgerichtig die von ihr nicht gewollte Richtlinie nicht umgesetzt. Bundeskanzler Kohl hat in seiner Rede im Deutschen Bundestag am 18. Juni 1998 diese Richtlinie als ein "besonders absurdes Beispiel" einer Fehlentwicklung bezeichntet, hin zur Überregulierung und unnötigen Bürokratie im vereinten Europa. Statt die Richtlinie umzusetzen, hat man folgendes gemacht: Der Bund hat, vertreten durch das Statistische Bundesamt, mit dem Statistischen Amt der EG, EUROSTAT, einen Vertrag geschlossen, in dem er sich zur Lieferung von Daten verpflichtet hat, und zwar gegen von der EG zu zahlendes Entgelt! Daraufhin hat das Statistische Bundesamt die Beschaffung dieser Daten (sc. privatrechtlich) ausgeschrieben, und das Statistische Landesamt Nordrhein-Westfalen hat als günstigster Anbieter den Zuschlag erhalten. Wie es heißt, hat dann das Land Nordrhein-Westfalen, vertreten durch das Statistische Landesamt, aufgrund lediglich mündlichen Vertragsschlusses die anderen statistischen Landesämter für deren örtlichen Zuständigkeitsbereich als Subunternehmer zweiter Stufe gewonnen; in dieser Eigenschaft und auf dieser Rechtsgrundlage war also das Statistische Landesamt des Freistaates tätig geworden! Man glaubt es kaum ...

Zur Verteidigung dieser Vorgehensweise beruft man sich auf Art. 5 Abs. 1 der genannten Richtlinie, nämlich daß die Mitgliedsstaaten abweichend von Art. 1 nicht selbst eine Statistik durchführen, sondern „auf bestehende Daten, Quellen und Systeme zurückgreifen“. Diese „kreative“ Überlegung, gegen die der BfD nichts einzuwenden hat, ist nichts als ein Umgehungsgeschäft: Um die Statistik formell nicht selber durchführen zu müssen, sorgt der Bund für das Stattfinden einer Datensammlung, auf die er dann, als auf eine scheinbar von der statistischen Tätigkeit des Bundes unabhängig schon *bestehende* zurückgreifen kann. Gegen diese Aktion würde ich nichts einwenden, wäre sie tatsächlich in vollprivatisierter Form durchgeführt worden (vgl. 4/5.7.3). Dies ist jedoch gerade nicht geschehen. Denn Statistik-Behörden werden, wenn sie in ihrem räumlichen Zuständigkeitsbereich einer Tätigkeit nachgehen, die genau in ihren sachlichen Zuständigkeitsbereich fällt, nun einmal nicht fiskalisch tätig, sofern diese Tätigkeit darin besteht, in ein Grundrecht einzugreifen. Und letzteres ist nun einmal, wie wir alle seit dem Volkszählungsurteil wissen, beim Sammeln personenbezogener Daten durch Statistik-Behörden der Fall.

Allerdings läßt sich dagegen einwenden, daß die Erhebung - natürlich - auf freiwilliger Grundlage stattgefunden hat. Nur: Sowohl das Bundesstatistikgesetz - und das reicht in diesem Falle schon aus, da es sich ja um eine verkappte Bundesstatistik handelt! - als auch mit vielen anderen Landesstatistikgesetzen das Sächsische Statistikgesetz folgen einem Verfassungsverständnis, welches die Erhebung personenbezogener Daten auf freiwilliger Grundlage im Bereich der amtlichen Statistik für etwas so wichtiges hält, daß insoweit der *Vorbehalt des Gesetzes* gilt (vgl. §§ 5 Abs. 1, 15 Abs. 1 Satz 1 BStatG, §§ 6 Abs. 3 Satz 1, Abs. 6 Satz 2, 11 Abs. 1, 17 Abs. 6 SächsStatG).

Mit anderen Worten: Eine Behörde, die auf dem Gebiet ihrer ureigenen Zuständigkeit, also auf dem Gebiet, auf dem sie öffentliche Gewalt ausübt, grundrechtseinschränkend tätig wird, kann sich nicht darauf berufen, diese Tätigkeit diene der

Einziehung von Einkünften, sei ausschließlich „fiskalischer“ Natur, und deswegen sei sie insoweit nicht an die Rechtsvorschriften gebunden, die für Grundrechtseinschränkungen dieser Art allgemein und insbesondere für die betreffende Behörde gelten.

An meine Kollegen im Bund sowie Nordrhein-Westfalen, welche sich mit diesen Praktiken einverstanden erklärt haben, kann ich nur appellieren, dieser Verwilderung der Sitten auf dem Gebiet der amtlichen Statistik mit mir entschieden entgegenzutreten. Es kann nicht angehen, daß durch scheinbare - weil nämlich verdeckte - Privatisierungen der amtlichen Statistik der Schutz des Grundrechts auf informationelle Selbstbestimmung auf diesem Gebiet ausgehöhlt wird. Abgesehen von wettbewerbsrechtlichen Bedenken sollte man auch folgendes überlegen: Wenn das Statistische Bundesamt bei dergleichen Tätigkeiten, also bei der Sammlung personenbezogener Daten, nicht mehr an das Bundesstatistikgesetz gebunden ist, dann ist eigentlich nicht einzusehen, warum das Bundesamt dann noch an öffentliches Datenschutzrecht, nämlich den zweiten Abschnitt des Bundesdatenschutzgesetzes gebunden sein und insbesondere der Kontrolle des BfD unterliegen sollte ...

### 5.7.2 Bundesstatistik zur Einkommensverwendung

Das Ausländeramt eines Kreises hat sich an mich gewandt, als es vom Statistischen Landesamt um die Übermittlung von Anschriften von Ausländern ersucht worden war. Die Zweifel der Behörde haben sich als berechtigt erwiesen:

Das Statistische Landesamt wollte die Daten für die Durchführung einer bestimmten Statistik verwenden, nämlich für die in den neuen Bundesländern zum zweitenmal durchgeführte sog. „Einkommens- und Verbrauchsstichprobe“. Rechtsgrundlage dieser Befragung zu Einkünften, Verbrauchsgewohnheiten, Vermögensbildung und Ausstattung der Haushalte mit bestimmten Geräten ist das Gesetz über die Statistik der Wirtschaftsrechnungen privater Haushalte vom 11. Januar 1961 (BGBl. I S. 18, BGBl. III S. 708-6), ein altes Gesetz, das in seinem Grundbestand kaum geändert worden ist.

Eine Rechtsgrundlage dafür, die Ausländereigenschaft von Angehörigen der befragten Haushalte *als Erhebungsmerkmal* im technischen Sinne des Statistikrechtes zu *erheben*, bietet das Gesetz dem Statistischen Landesamt und dem Statistischen Bundesamt nicht; auch ein etwa ergänzend heranzuziehendes anderes Statistikgesetz enthält keine Ermächtigung dazu. Denn: Zwar sind gemäß § 1 Abs. 1 Nr. 2 dieses Gesetzes Erhebungen bei Haushalten *aller* Bevölkerungskreise durchzuführen. Das Gesetz sieht damit aber nicht die Zugehörigkeit zu diesem oder jenem Bevölkerungskreis als Erhebungsmerkmal vor, sondern es schreibt vor, daß alle Bevölkerungskreise in der Stichprobe vorkommen müssen.
Auch das in § 2 Abs. 2 des Gesetzes genannte Erhebungsmerkmal ‘wirtschaftliche und soziale Verhältnisse des Haushalts’ deckt die Erhebung der Ausländereigenschaft oder im einzelnen der Zugehörigkeit zu den Staatsangehörigkeits-Arten „Deutsch, EU, sonstige, ohne“ nach den Maßstäben des verfassungsrechtlichen Bestimmtheits-

grundsatzes nicht mehr: Bei Bevölkerungsstatistiken, also Statistiken, bei denen die Daten nicht von Unternehmen und Betrieben, sondern von der allgemeinen Bevölkerung erhoben werden, ist insoweit ein vergleichsweise strengerer Maßstab anzulegen - so einleuchtend die amtliche Begründung zu § 10 Abs. 1 des Bundesstatistikgesetzes 1987 (BT-Dr 10/5345 vom 17. April 1986, S. 17), zustimmend zitiert vom Bundesverwaltungsgericht in seinem Urteil vom 11. Dezember 1990 - 1 C 52/88, NJW 1991, 1246, 1246/1247.

Eine Berücksichtigung der Ausländereigenschaft als Hilfsmerkmal, also zur Sicherung der Repräsentativität der Stichprobe, ist hingegen zulässig. Insoweit bietet § 1 Abs. 1 Nr. 2 des Gesetzes über die Statistik der Wirtschaftsrechnungen privater Haushalte dem Statistischen Landesamt eine Erhebungsbefugnis. Hintergrund ist, daß die Auskunftsbereitschaft je nach Haushaltstyp (z. B. Rentner, 'Single', Ausländer) sehr unterschiedlich ist.

Da es sich um eine Bundesstatistik handelt, kommt gemäß § 15 Abs. 1 BStatG eine auf Einwilligung gestützte Datenverarbeitung - freiwillige Auskunftserteilung, vgl. § 4 des Gesetzes - als hinreichende Rechtsgrundlage einer Datenerhebung nicht in Betracht. Dies gilt auch für diejenigen Bundesländer, die für Landes- und Kommunalstatistiken im Falle fehlender Auskunftspflicht auf das Erfordernis einer Rechtsvorschrift, welche die Durchführung der betreffenden einzelnen Statistik anordnet, verzichten.

Ersucht das Statistische Landesamt eine andere Behörde um Übermittlung von Namen und Anschriften von Ausländern, bedarf diese Behörde einer Übermittlungsbefugnis.

Es gibt keine Vorschrift, die es Ausländerbehörden erlaubt, solche Daten dem Statistischen Landesamt zu übermitteln. Weder das Statistikrecht noch das Ausländerrecht enthalten eine solche Erlaubnis. Auch die ersatzweise heranzuziehende Vorschrift des § 13 Abs. 1 SächsDSG bietet keine Grundlage, da keiner der in § 13 Abs. 1 Nr. 2 vorausgesetzten Verarbeitungszwecke des § 12 Abs. 1 bis 4 SächsDSG vorliegt.

Nach anfänglichem Zögern hat mir das Statistische Landesamt zugesagt, bei der Durchführung der Statistik bis auf weiteres die Staatsangehörigkeit nicht mehr als Erhebungsmerkmal zu verarbeiten.

Vom Statistischen Bundesamt, dem ich die Sachlage dargelegt habe, weil ja die gesamte einschlägige Bundesstatistik betroffen ist, liegt mir noch keine Reaktion vor. Weil das Bundesstatistikgesetz (in § 15 Abs. 1 Satz 1) für die gesamte Bundesstatistik vorschreibt, daß Statistiken auch dann einer Rechtsvorschrift als Rechtsgrundlage bedürfen, wenn sie ohne Auskunftspflicht durchgeführt werden, kann man sich auch in denjenigen Bundesländern, welche für ihr eigenes Landesstatistikrecht, anders als Sachsen, noch nicht diesen strengeren rechtsstaatlichen Standard erreicht haben, also für ohne Auskunftspflicht durchgeführte Statistiken eine Rechtsvorschrift nicht verlangen, nicht damit beruhigen, daß die Statistik (gemäß § 4 des o. g. Gesetzes) auf freiwilliger Grundlage durchgeführt wird.

### 5.7.3 Aggregierungserfordernisse der Statistik im Verwaltungsvollzug

Eine im Geschäftsbereich des SMI angeordnete *Statistik im Verwaltungsvollzug* gab Anlaß, die unter 5/5.7.12 angestellten Überlegungen zu denjenigen Statistiken im Verwaltungsvollzug weiterzuführen, die mit der Weitergabe von Daten von der unteren zu einer oberen oder obersten Verwaltungsbehörde verbunden sind.
Wie gesetzlich angeordnete Sekundärstatistiken arbeiten auch solche Statistiken im Verwaltungsvollzug, die durch Verwaltungsvorschrift gewissermaßen institutionalisiert sind, meist mit sogenannten Zählkarten oder Zählblättern, d. h. mit Erhebungsbögen, die der sachbearbeitende Bedienstete auf der Grundlage einer Auswertung der durch die Erledigung seiner Vorgänge anfallenden, also bereits erhobenen Daten ausfüllt. Ist die betreffende Statistik nicht durch Rechtsvorschrift angeordnet, werden die Zählkarten - die natürlich zunehmend durch maschinell verwertbare Datenträger abgelöst werden - nicht notwendig vom Statistischen Landesamt gesammelt und verarbeitet. Vielmehr kann dies auch innerhalb der betreffenden Fachverwaltung selbst geschehen.

Dann müssen meiner Auffassung nach jedoch folgende Regeln eingehalten werden:

1. Einzeldatensätze, auch wenn sie frei von unmittelbar identifizierenden Merkmalen wie Namen und Anschriften sind, dürfen an die nächsthöhere Behörde nicht übermittelt werden. Diese darf nur aggregierte Daten erhalten. Das folgt aus dem Gebot der frühestmöglichen - statistikunschädlichen - Anonymisierung, wie schon 5/5.7.12 dargelegt. Dieses Gebot ist nur eine Anwendung des verfassungsrechtlichen Verhältnismäßigkeitsgrundsatzes.

2. Hingegen ist es meiner Auffassung nach erlaubt, daß die Behörde, die für die Bearbeitung eines Vorganges im Verwaltungsvollzug instantiell zuständig war und ihn gemäß dem in der ‘Zählkarte’ vorgegebenen Erhebungs-Programm statistisch ausgewertet hat, die Zählkarte, also datenschutzrechtlich gesprochen den betreffenden Einzeldatensatz, bei sich vorrätig hält. Sie kann dann für diesen Datenbestand das tun, was in der amtlichen Statistik in den Statistikämtern üblich ist: So weit, wie statistikunschädlich möglich ist, anonymisierte Einzeldatensätze vorhalten für Auswertungen - also Merkmals-Kombinations-Feststellungen, an die man aufgrund der Standard-Fragestellungen zunächst bei der Auswertung (Aggregierung) nicht gedacht hat.
   Diese Doppel-Speicherung personenbezogener Daten ist durch § 12 Abs. 3 Satz 1 SächsDSG eindeutig gedeckt.

3. Bei übergeordneten Behörden darf das jedoch nicht stattfinden. Denn das wäre eine *Speicherung personenbezogener Daten*, die nicht erforderlich wäre: Zu Zwecken des bloßen Verwaltungsvollzuges dürften sie dort nicht gespeichert sein, weil die Behörde als bloße Aufsichts-Behörde für den Verwaltungsvollzug die Daten nur in einzelnen Fällen aufsichtlicher Tätigkeit benötigte, also gerade nicht in der für eine Statistik kennzeichnenden Vollständigkeit (sei diese Vollständig-

keit auch nur diejenige einer Stichprobe). Für die Erreichung von Zwecken, für die man hingegen gerade Statistiken braucht, also für die Gewinnung von Kenntnissen über Massenerscheinungen, für die Gewinnung des Überblickes, also für die gerade übergeordneten Behörden zukommenden Aufgaben, bedarf es jedoch einer dort zusätzlich stattfindenden Speicherung der einzelnen 'Zählkarten'-Daten gerade nicht.
Das bedeutet: Die vorgesetzte Behörde darf nicht das, was das Statistische Landesamt darf und was für die bei ihr zu bearbeitenden Vorgänge auch die für diese instantiell zuständige untere Behörde darf, nämlich die Einzeldatensätze, die im Wege des 'Zählkarten'-Verfahrens aus den Vorgangsbearbeitungs-Daten herausgezogen sind, für künftige statistische Auswertungen vorhalten.
Andernfalls entstünde in einer ausschließlich dem Verwaltungsvollzug dienenden Stelle eine Statistik-Nebenbehörde.
§ 7 Abs. 1 SächsStatG ist nicht zwingend auf eine Nutzungserlaubnis beschränkt, sondern erlaubt grundsätzlich auch Übermittlungen an die übergeordnete Behörde und eine dort stattfindende Speicherung. Allerdings ist § 7 Abs. 1 SächsStatG, wie auch § 12 Abs. 3 Satz 1 SächsDSG, was Statistiken im Verwaltungsvollzug betrifft, verfassungskonform so auszulegen, daß diese Vorschriften eine Speicherung und Übermittlung nur im Rahmen des Erforderlichen erlauben.
Erforderlich ist jedoch nur, daß die untergeordnete Behörde der übergeordneten Behörde auch ausnahmsweise Aggregationsergebnisse mitteilt, welche die übliche Mindestzahl von drei unterschreiten, die also personenbeziehbar sind. Solche Daten muß die übergeordnete Behörde bekommen und auch aufbewahren dürfen. Mehr ist andererseits jedoch nicht für die Erfüllung der Aufgaben der übergeordneten Behörde, nämlich Aufsicht auszuüben und Übersicht über die tatsächlichen Verhältnisse zu gewinnen, erforderlich.

Das SMI ist jedenfalls in dem konkreten Fall im Ergebnis meinen Überlegungen gefolgt und hat darauf verzichtet, bei der betreffenden Statistik eine Mehrfertigung des Zählkarten-Datensatzes, der vom Statistischen Landesamt zu verarbeiten ist, für das zuständige Regierungspräsidium vorzusehen.

### 5.7.4 Mietspiegel

Mehrere Gemeinden haben mich an der Vorbereitung einer Mietspiegelsatzung beteiligt. Hierbei war ich mit zwei Problemen befaßt:

1. Eine sehr kleine Gemeinde beabsichtigte die Erstellung einer Mietspiegels. Hierfür fehlte ihr die notwendige Rechtsgrundlage.
   Empirische Mietspiegel werden durch Verarbeitung empirischer Einzeldaten erstellt. Soweit die Gemeinde die Daten neu bei einzelnen Mietvertragsparteien erhebt, handelt es sich um die Verarbeitung personenbezogener Daten durch eine öffentliche Stelle. Hierfür ist eine Rechtsgrundlage erforderlich.
   Wie ich in 5/5.7.2 dargelegt habe, ist die Datenerhebung zur Erstellung empirischer Mietspiegel als Statistik im Rechtssinne aufzufassen. § 8 SächsStatG regelt die Voraussetzungen, unter denen die Durchführung einer Kommunalstatistik zulässig ist. Danach können die Gemeinden zur Wahrnehmung ihrer Aufgaben Kommunalstatistiken durchführen. Die Aufgabe, die hier wahrgenommen wird,

ist in § 2 Abs. 5 Satz 1 des Gesetzes zur Regelung der Miethöhe (MHG) beschrieben. Danach sollen die Gemeinden, soweit hierfür ein Bedürfnis besteht und dies mit einem für sie vertretbaren Aufwand möglich ist, Mietspiegel erstellen.
Wann ein Bedürfnis besteht, richtet sich in erster Linie nach der Gemeindegröße. Wesentlich sind laut der unter Beteiligung des SMI und mehrerer Behörden, Städte und Institutionen vom Institut für Stadt-, Regional- und Wohnforschung GmbH (kurz: GEWOS) erstellten Arbeitshilfe zur Erstellung von Mietspiegeln in Sachsen der Gesamtbestand mietspiegelrelevanter Wohnungen und die Zahl der Einwohner. Danach sollen in einer Gemeinde mindestens 1200 mietspiegelrelevante Wohnungen vorhanden sein oder mindestens 20.000 Einwohner leben. Laut Auskunft der GEWOS wurde davon ausgegangen, daß eine Gemeinde mit weniger als 20.000 Einwohnern keine 1200 mietspiegelrelevanten Wohnungen haben könne. Primär abzustellen sei auf die Anzahl der Wohnungen; die Einwohnerzahl biete hierfür einen Anhaltspunkt.
Gemeinden, die keine 1200 mietspiegelrelevanten Wohnungen oder die nicht mindestens 20.000 Einwohner haben, haben kein Bedürfnis, Mietspiegel zu erstellen. Damit fehlt es an einer Aufgabenzuweisung nach § 2 Abs. 5 Satz 1 MHG und damit auch an einer Ermächtigung zur Durchführung einer Kommunalstatistik nach § 8 Abs. 1 Satz 1 SächsStatG.

2. Gemäß § 8 Abs. 1 Satz 2 SächsStatG werden die Gemeinden ermächtigt, Kommunalstatistiken (hierzu zählt, wie bereits erwähnt, die Datenerhebung zur Erstellung empirischer Mietspiegel) durch Satzung anzuordnen. An der Vorbereitung der Satzung ist gemäß § 8 Abs. 3 SächsStatG der Sächsische Datenschutzbeauftragte zu beteiligen.
An den Satzungsentwürfen fiel mir auf, daß die Gemeinden bei Festlegung der Erhebungsmerkmale den Grundsatz der Verhältnismäßigkeit nicht in ausreichendem Maße beachten:
Die mietpreisbildenden Faktoren nennt § 2 Abs. 1 Nr. 2 MHG. Dies sind Art, Größe, Ausstattung, Beschaffenheit und Lage der Wohnung. Diese einzelnen Merkmale müssen, um aussagekräftig zu sein, verschiedene Merkmalsausprägungen aufweisen. So sollte z. B. unter „Beschaffenheit der Wohnung“ danach gefragt werden, ob die Ausstattungsmerkmale Bad, Sammelheizung und WC vorhanden sind. Mancher Satzungsentwurf beschränkt sich hier auf zu wenige Merkmalsausprägungen.
Unter dem Gesichtspunkt der Verhältnismäßigkeit ist darauf zu achten, daß die Daten für den mit der Erhebung verfolgten Zweck geeignet und erforderlich sind. Das kann bedeuten, daß eine Datenerhebung auch umfangreicher als ursprünglich beabsichtigt durchgeführt werden muß, um nicht den gesamten Zweck zu verfehlen und die Datenerhebung deshalb unzulässig werden zu lassen. Ein Weniger an Daten muß also nicht immer das datenschutzrechtlich Erforderliche sein.

### 5.7.5 Standard-Verkehrs-Untersuchung der TU Dresden in Zusammenarbeit mit sächsischen Gemeinden

Schon seit den siebziger Jahren hat die TU Dresden, genauer gesagt die Fakultät Verkehrswissenschaften „Friedrich List“, in regelmäßigen Abständen auf dem Gebiet

der DDR und jetzt der neuen Bundesländer in Zusammenarbeit mit ausgewählten Städten für deren Gebiet Untersuchungen dazu durchgeführt, welche Personenkreise zu welcher Zeit welche Wege mittels welchen Verkehrsmittels zurücklegen, um damit Erkenntnisse für die Verkehrsplanung zu gewinnen.

Dazu werden von Haushalten für alle Haushaltsmitglieder Angaben über die genauen Zeiten sowie mindestens straßengenau bestimmten Ausgangs- und Zielpunkte der Wege und über sonstige für die Mobilität mehr oder weniger wichtigen Eigenschaften der Person erfragt.

1. Nachdem der Übergangsbonus des § 25 SächsStatG Mitte 1995 ausgelaufen ist, mußten die TU Dresden und die zu beteiligenden Städte, was Sachsen betrifft, für ihren neuen Durchgang im Jahr 1998 die Untersuchung auf rechtsstaatliche Füße stellen. Das bedeutete zunächst, daß entschieden werden mußte, ob die Erhebung als amtliche - kommunale - Statistik oder aber in vollständig privater Rechtsform durchgeführt werden sollte (dazu ausführlich schon früher 4/5.7.3).

   Zittau, Plauen und Chemnitz haben sich für die öffentlich-rechtliche, Leipzig hat sich für die vollständig privatrechtliche Form entschieden. Damit hat sich die Messestadt für diese Datenerhebung von den unmittelbaren Vorgaben des Statistikrechtes freigemacht. Insbesondere bedarf sie keiner kommunalen Statistiksatzung als Rechtsgrundlage, sie muß auch aus statistikrechtlichen, letztlich verfassungsrechtlichen Gründen nicht sichern, daß nur Daten erhoben werden, für die tatsächlich verkehrsplanerischer Bedarf besteht (dazu unten [3]). Die Frage, inwieweit die Stadt die Daten Dritten übermitteln darf, stellt sich gar nicht, weil die Daten, solange sie Personenbezug aufweisen, gar nicht an die Kommune gelangen dürfen; denn sonst handelte es sich ja um eine Umgehung des Statistikrechts (vgl. 4. TB a.a.O., Fallgruppe 1).

   Allerdings: Wie im 4. TB bereits ausgeführt, darf bei dieser Verfahrensweise die Kommune in keiner Weise als Interessent oder Auftraggeber der Datensammlung in Erscheinung treten; eine geräuschlose Erwähnung in Haushaltsplänen ist unschädlich, weil die befragten Bevölkerungskreise diese Einzelheiten nicht erfahren, jedenfalls in ihrem Antwortverhalten dadurch unbeeinflußt bleiben.

   Die TU Dresden hat deutlich zu erkennen gegeben, daß ihr die andere Rechtsform, bei der die Kommune zumindest als Auftraggeber oder sogar als diejenige Stelle in Erscheinung tritt, welche die Erhebung selbst durchführt, eindeutig lieber ist. Verspricht sie sich doch von einer solchen amtlichen Erscheinungsweise eine größere Teilnahmebereitschaft der Bevölkerung.
   Denn wohlgemerkt: Die Erhebung soll ohne Auskunftspflicht durchgeführt werden. Aber auch eine amtliche Statistik *ohne* Auskunftspflicht bedarf nach sächsischem Statistikrecht - wie nach dem des Bundes und auch anderer Länder wie z. B. Hessen und Thüringen - einer Rechtsvorschrift als Rechtsgrundlage (vgl. § 6 Abs. 3 Satz 1, Abs. 6 Satz 2, § 11 Abs. 1, § 17 Abs. 6 SächsStatG).

   Das andere hauptsächliche Erfordernis einer (amtlichen) kommunalen Statistik ist, daß die Durchführung einer den besonderen gesetzlichen Anforderungen genügenden kommunalen Statistikstelle vorbehalten ist (§ 9 Abs. 1 Satz 1

SächsStatG). Dies dient der verfassungsrechtlich gebotenen Sicherung der strikten Zweckbindung von Statistik-Daten, soweit diese nicht völlig frei von Personenbezug sind.

2. Dieses letztere Erfordernis kann die Kommune durch Teil-Privatisierung ihrer Statistik umgehen. Sie muß dafür sorgen, daß sie selbst gar nicht, in keiner der Phasen der Durchführung einer amtlichen Statistik (vgl. § 1 Abs. 1 Satz 1, a. E., SächsStatG), an Einzelangaben herankommt, daß sie vielmehr nur Auswertungen bekommt, die hinreichend anonymisiert sind, im Regelfall also solche, in denen keine Tabellenwerte kleiner als drei vorkommen; vgl. dazu ausführlicher im 4. TB a. a. O. Fallgruppe 2, S. 80.

   Diese Art der Durchführung wäre der TU Dresden auch recht gewesen. Insbesondere deswegen, weil sie die Programme zur Auswertung der durch Befragung zu erhebenden Daten entwickelt hat und weiterentwickeln will. Außerdem hat sie ein natürliches, ihrer Aufgabe entsprechendes Interesse daran, die Daten, und zwar als Einzelangaben, auch zur Beantwortung von Fragestellungen auszuwerten, die über den Bedarf der kommunalen Verkehrsplaner hinausgehen.

   Und wegen dieses notwendig gegebenen Interesses der Hochschule an den Einzelangaben wäre es nicht zulässig, wenn die TU zugleich als Auftragsdatenverarbeiter (a. a. O., Fallgruppe 3) oder auch als Funktionsübernehmer (a. a. O., Fallgruppe 2) in die Durchführung einer - dadurch teilprivatisierten - amtlichen Statistik eingeschaltet würde. Denn der TU darf nicht im Wege der Auftragsdatenverarbeitung oder auch der Funktionsübertragung der Umgang mit Daten ermöglicht werden, die ihr nicht auch gemäß § 19 Abs. 5 SächsStatG (i. V. m. Abs. 9) zur Verwendung in der Forschung überlassen werden dürften. Daher muß die von der Kommune benötigte Verarbeitung der Daten, soweit sich diese auf kleinräumigere Einheiten als das Gesamtgebiet der betreffenden Stadt, also Verkehrsbezirke, Straßen oder Blockseiten, beziehen, ausschließlich bei der Kommune selbst, d. h. in deren kommunaler Statistikstelle, stattfinden.

   Aufgrund dessen war die ursprüngliche Abgrenzung der Arbeitsteilung zwischen Kommune und TU Dresden zu ändern, d. h. der ursprünglich vorgesehene Vertrag dazu umzugestalten.

   Das Statistische Landesamt, welches gemäß § 8 Abs. 3 SächsStatG ebenso wie meine Behörde an der Vorbereitung kommunaler Statistiksatzungen zu beteiligen ist, wie auch dessen Aufsichtsbehörde, das SMI (vgl. § 3 Abs. 1 Satz 1 SächsStatG), haben meine Auffassung unterstützt.

   Konkret handelt es sich um folgendes Anonymisierungs-Problem: Im Falle der Stadt Dresden sollte eine Stichprobe von mindestens 420 Haushalten gezogen werden, von denen jeweils sechs in einem der 70 Verkehrsbezirke, in die das gesamte Stadtgebiet eingeteilt wird, wohnhaft sind. Angesichts der recht detaillierten Erhebungsmerkmale war der für eine Übermittlung an eine Hochschule notwendige Anonymisierungsgrad gemäß § 19 Abs. 5 SächsStatG erst erreicht,

wenn der Bezug auf einen räumlichen Bereich, der kleiner als das gesamte Gebiet der Stadt Dresden ist, gänzlich getilgt ist.

Die TU Dresden hat erklärt, ihr sei mit unterschiedslos auf das Gesamtgebiet der Stadt bezogenen Datensätzen ausreichend gedient.

3. Weitere Fragen hat das von der TU Dresden vorgesehene Erhebungsprogramm aufgeworfen.

Für alle Bestandteile des Erhebungsprogramms, also alle Erhebungsmerkmale, muß ein objektiver Informationsbedarf bestehen. Die Daten müssen benötigt werden, d. h. dienlich sein zur Aufgabenerfüllung (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 Entscheidungen innerhalb des Rahmens der Planungshoheit.
Alle diese Formulierungen drücken aus, was sich ergibt, wenn man den verfassungsrechtlichen Grundsatz der Verhältnismäßigkeit, hier dessen beide Teilerfordernisse der Geeignetheit und Erforderlichkeit, auf den besonderen Verwaltungszweck einer Statistik anwendet: Sammlung und Weiterverarbeitung von Daten zum Zweck der Statistik haben einen weniger engen, weniger konkreten Zweckbezug als die Datenverarbeitung zu Zwecken des Verwaltungsvollzuges. Im Unterschied zur Verarbeitung personenbezogener Daten, die zu Zwecken des Verwaltungsvollzuges stattfindet, darf diejenige, die zu Statistikzwecken stattfindet, in dem Sinne auf Vorrat stattfinden, daß man bei ihrer Durchführung noch nicht genau wissen muß, für welche bestimmte Aufgabe die öffentliche Verwaltung sie alsbald benötigt (BVerfGE 65, 1, 47 f.). Die Vielfalt der Verwendungs- und Verknüpfungsmöglichkeiten personenbezogener Daten ist, wie das Bundesverfassungsgericht (a. a. O. S. 48) formuliert hat, bei der Statistik von der Natur der Sache her nicht im voraus bestimmbar. Es wird Wissen über Massenerscheinungen von Amts wegen in allgemeiner Vorausschau bereitgestellt.
Gleichwohl muß die Informationsbeschaffung einem *„einleuchtenden, zur Erfüllung legitimer Staatsaufgaben [„Staat“ hier im weiten Sinne der ‘öffentlichen Gewalt’] angestrebten Zweck“ dienlich sein* (BVerfGE a. a. O. S. 54/55); sie muß *„als Hilfe zur Erfüllung öffentlicher Aufgaben erfolgen“* (a. a. O. S. 48).

Bei Erhebungen, die im Vergleich zu sehr allgemein gehaltenen Statistiken wie etwa Volkszählungen einen im wesentlichen abschließend zu benennenden Zweck haben, muß aber die Dienlichkeit der einzelnen Merkmale für die Verwendung plausibel gemacht werden.

Es war für meine Behörde eine bemerkenswerte Erfahrung, daß diejenigen, die den Fragebogen entworfen haben oder die mittels seiner zu gewinnenden Ergebnisse nutzen wollen, auch beim besten Willen keineswegs immer die Zweckdienlichkeit aller Erhebungsmerkmale zu vermitteln in der Lage sind. Erst ein von der TU zusätzlich hinzugezogener, eher theoretisch arbeitender Wissenschaftler konnte zu manchen Merkmalen dem Laien eine Ahnung davon verschaffen, inwiefern sie der städtischen Verkehrsplanung dienlich sein können.

Konkret ging es um die Merkmale
- Stellung im Beruf, mit Merkmalsausprägungen wie Arbeiter, Beamter, Selbständiger,
- Schulabschluß, z. B. ob Abitur, sowie
- Berufsausbildung, z. B. ob Facharbeiter oder Meister,

aber auch darum, ob das Geschlecht oder bestehender Mutterschaftsurlaub erheblich sein könnten.

Ich habe mich überzeugen lassen, daß es wohl geschlechtsspezifische Unterschiede bei der Verfügbarkeit von Pkw in Haushalten gibt, mit zu erwartenden Verschiebungen in der Zukunft, die bestimmte Veränderungen berechenbar machen. Und ebenso, daß die Reichweite des Pendelns zwischen Wohnung und Arbeitsstätte von der Stellung im Beruf, dem Schulabschluß oder der Berufsausbildung statistisch abhängig ist, und daß dies je nach Wohnquartieren und Gebieten mit verschiedenen Arbeitsstätten, z. B. Produktionsstätten, Behörden, privatwirtschaftlichen Dienstleistungszentren usw. zu Möglichkeiten der Berechnung künftiger Verkehrsströme führt.

Was mir auf diese Weise in der Theorie halbwegs deutlich geworden war, das wollte ich dann aber gerne in der praktischen Anwendung vorgeführt bekommen. Denn die kommunale Statistik hat, wenn als nicht rein privatrechtliche durchgeführt (dann bin ich nicht zuständig), den Zwecken der Kommune, nicht denen der Wissenschaft dienlich zu sein. Und da die Untersuchung ja bereits in den neunziger Jahren zweimal mit diesen Erhebungsmerkmalen durchgeführt worden war, mußte dieses Merkmal ja schon durch die Stadtplaner verwendet worden sein.

Mein Verdacht, daß dies möglicherweise doch noch gar nicht geschehen war, hat sich weitgehend bestätigt: Nach einigen vergeblichen Anläufen eines Nachweises der Verwendung der betreffenden Merkmale mußte die Stadt Dresden - sie war wie so oft das ‘Versuchskaninchen’, und bei den anderen beteiligten Städten wird es keinen Deut besser sein - eingestehen, daß sie die drei oben aufgeführten Merkmale bisher bei ihrer verkehrsplanerischen Tätigkeit nicht verwendet hatte. Ein schönes Beispiel für die nur angeblich wissenschaftliche Verkehrsplanung - und das in Dresden, wo jeder Laie den Verkehrsplanern Beine machen könnte!

Daraus durfte ich aber nicht Rechtswidrigkeit dieses Teils des vorgesehenen Erhebungsprogramms folgern. Es wäre zwar nicht rechtmäßig, wenn die Kommune mit Bedacht statistische Daten erhöbe, von denen absehbar ist, daß sie in Zukunft von ihnen weiterhin keinerlei Gebrauch machen wird. Aber ich habe es zur Voraussetzung einer Zustimmung zu diesem Teil des Erhebungsprogramms gemacht, daß die betreffenden Kommunen mir zugesagt haben, die bei der für 1998 vorgesehenen Befragung anfallenden Daten gerade zu diesen drei Erhebungsmerkmalen auch tatsächlich und konkret für Verkehrsplanungszwecke zu benutzen. Sollte diese Zusage nicht eingehalten werden, könnte man für die nächste Erhebung nicht mehr davon ausgehen, daß insoweit ein plausibler objektiver Informationsbedarf bestünde.

### 5.7.6 Scheinstatistik: Verkehrserhebung in der Umgebung einer industriellen Anlage

Ein Petent hat sich an mich gewandt, weil das städtische Umweltamt auf der Straße, an der sein Betrieb liegt, eine Verkehrszählung durchgeführt habe. Hierbei seien neben der Uhrzeit und dem Fahrzeugtyp auch das vollständige amtliche Kennzeichen der Fahrzeuge, die die Zufahrt zum Betriebsgelände benutzten, erfaßt worden.

Der Verdacht, daß diese Datenerhebung keine Verkehrszählung im landläufigen Sinne gewesen war, hat sich dann bald bestätigt. Das Amt hatte prüfen wollen, ob die mit der Betriebsgenehmigung verbundene Auflage eingehalten wurde, die Anlage werktags nicht vor 6.00 Uhr zu betreiben. Die Datenerhebung diente, auch wenn die Ergebnisse tabellarisch dargestellt wurden (Anzahl der Kraftfahrzeuge verschiedener Arten je Zeitabschnitt), demnach nicht statistischen Zwecken. Denn hier ging es nicht um die Gewinnung und Auswertung empirischer Daten über Massenerscheinungen zur Deckung eines den Zwecken von Planung und ähnlichen allgemeinen Überlegungen dienenden Informationsbedarfes. Vielmehr handelte es sich um eine Datenerhebung zur Prüfung, ob in diesem konkreten Einzelfall behördliche Maßnahmen gegenüber dem Betreiber der Anlage zu ergreifen waren oder nicht.
Die Zulässigkeit der Datenerhebung war demnach nicht nach Statistikrecht zu beurteilen. Da spezialgesetzliche Vorschriften, gerade auch im hier einschlägigen Bundesimmissionsschutzgesetz, fehlen, war als Auffangmaßstab das Sächsische Datenschutzgesetz heranzuziehen.

Gemäß § 11 Abs. 1 SächsDSG ist das *Erheben* personenbezogener Daten nur zulässig, wenn ihre Kenntnis zur Erfüllung der Aufgaben der erhebenden Stelle geeignet und erforderlich ist. Hier war festzustellen, wann die Anlage morgens üblicherweise in Betrieb genommen wurde. Zum Betrieb gehörte auch der An- und Abtransport von Gütern durch LKW. Da mag die Beobachtung, inwieweit LKW und auch PKW die Zufahrt zum Betriebsgelände benutzen, eine geeignete Maßnahme gewesen sein. Dazu war es aber nicht erforderlich, die amtlichen Kennzeichen der die Zufahrt benutzenden Kraftfahrzeuge zu erfassen und damit personenbezogene Daten zu erheben. Denn die Kennzeichen haben selbst keinen Aussagewert darüber, zu welcher Uhrzeit die Anlage in Betrieb genommen worden ist. (Dies galt insbesondere für die Erhebung der Kennzeichen der Privatfahrzeuge der Arbeitnehmer des Betriebes.) Mit Hilfe der Angabe der Kfz-Kennzeichen hätte man zwar im sich noch gar nicht abzeichnenden - Bestreitensfalle nachweisen können, daß man tatsächlich Kraftfahrzeuge beobachtet hatte, welche die Zufahrt benutzten. Für das entscheidende Moment, nämlich die Uhrzeit, hätte sich daraus jedoch noch kein Beweis ergeben.

Im allgemeinen werden dergleichen Angaben von Behörden im verwaltungsgerichtlichen Verfahren auch nicht bezweifelt. Auch hätte die Behörde erst einmal - unter Umständen auch gerade um diese Zeit in der Frühe - gemäß § 52 Abs. 2 Satz 1 BimSchG eine Auskunft des Betreibers der Anlage verlangen können, z. B. durch einen Telefonanruf. Oder sie hätte sich am Werkstor melden und offen nachfragen können.

Jedenfalls: Eine Strichliste über Kfz-Verkehr, der die Anlage anfuhr oder von ihr wegfuhr, hätte ausgereicht, um Beobachtungen darüber festzuhalten, wann die Anlage in Betrieb genommen worden war.

Stattdessen waren jedoch personenbezogene Daten auch *gespeichert* worden. Zulässig wäre dies gemäß § 12 Abs. 1 SächsDSG dann gewesen, wenn es zur Erfüllung der Aufgaben der öffentlichen Stelle erforderlich und die Daten nicht in unzulässiger Weise erhoben worden wären. Da hier, wie gezeigt, die Datenerhebung unzulässig gewesen war, war eine Speicherung nicht durch § 12 Abs. 1 SächsDSG erlaubt.

Die Speicherung war auch nicht etwa nach § 12 Abs. 5 SächsDSG ausnahmsweise erlaubt:

Die bei der Beobachtung der Zufahrt zum Betriebsgelände angefertigten Aufzeichnungen sind Bestandteil einer Akte geworden. Eine Speicherung der Kennzeichen wäre dann zulässig gewesen, wenn diese Aufzeichnungen derart mit Aufzeichnungen weiterer personenbezogener Daten verbunden gewesen wären, daß eine Trennung nicht oder nur mit unverhältnismäßigem Aufwand möglich gewesen wäre. Das war hier nicht der Fall; eine Trennung wäre möglich gewesen. Diese hätte so aussehen können, daß eine Kopie, auf der die Kennzeichen geschwärzt sind, erstellt und in der Akte verblieben wäre.
Folge der Rechtswidrigkeit der Speicherung der Daten in der Akte war: Die Blätter, auf denen die Kennzeichen aufgezeichnet sind, wären gemäß § 20 Abs. 3 Satz 1 SächsDSG gesondert aufzubewahren gewesen. Das ergibt sich aus folgendem: Da eine Speicherung der Kennzeichen unzulässig war und ist, die Akte, in der diese Daten sich befinden, aber vollständig bleiben muß, dürfen die Daten gemäß § 19 Abs. 2 SächsDSG erst gelöscht werden, wenn die gesamte Akte zur Aufgabenerfüllung nicht mehr erforderlich ist. Bis dahin sind sie gemäß § 20 Abs. 2 Satz 1 SächsDSG zu sperren. Gesperrte personenbezogene Daten sind nach § 20 Abs. 3 Satz 1 SächsDSG gesondert aufzubewahren.

Alles in allem ein sehr lehrreicher Fall.

## 5.8 Archivwesen

### 5.8.1 Psychiatrische Unterlagen in falschen Händen

Eine Eingabe hat gezeigt, wie nützlich die Altdatenregelung des § 35 SächsDSG weiterhin ist:

Eine Petentin hatte vergeblich versucht, für die Zwecke eines Rehabilitierungsverfahrens nach dem 2. SED-Unrechtsbereinigungsgesetz an ärztliche Aufzeichnungen aus ihrer psychiatrischen Behandlung in den 70er und 80er Jahren heranzukommen.

Die Universitätsklinik verfügte nur über zum Teil unerschlossene Alt-Unterlagen. Der Arzt, der die Petentin seinerzeit als Universitätsbediensteter behandelt hatte, hatte sich inzwischen mit eigener Praxis niedergelassen und erklärte - wahrheitsgemäß -, die Unterlagen nicht zu haben, aber er könne die Unterlagen, im Unterschied zur Petentin, in der Universitätsklinik bekommen, wenn die Petentin ihm unterschreibe, daß sie bei ihm in Behandlung sei und er deswegen die sie betreffenden Aufzeichnungen benötige. Gerade dies wollte die Petentin verständlicherweise nicht unterschreiben, weil sie eben kein Vertrauen in den Arzt hatte, der sie seinerzeit behandelt hatte. Sie kam nicht weiter und wandte sich schließlich an mich. Meine Behörde konnte ihr helfen:

Gemäß § 35 Abs. 1 i. V. m. § 24 Abs. 1 Satz 1 SächsDSG konnte der Sächsische Datenschutzbeauftragte in der Arztpraxis - in diesem Fall auch einmal unangekündigt - Auskunft darüber verlangen, was der Arzt an Unterlagen aus seiner Tätigkeit in der Universitätsklinik vor dem 3. Oktober 1990 mitgenommen hatte. Es stellte sich heraus, daß er vor allem ein Findbuch hatte mitgehen lassen, in dem seit den 60er Jahren für jeden Jahrgang die Neuzugänge an Patienten mit dem Aktenzeichen der dazu geführten Unterlagen verzeichnet worden waren. Da mir der Beginn der Behandlung bekannt war, war das Aktenzeichen bei scheinbar zufälligem Blättern in dem Findbuch schnell gefunden. Nach einem Gespräch mit der Leitung der Universitätsklinik, die schilderte, wie es seinerzeit zu den unkontrollierten Entnahmen von Unterlagen gekommen war, konnte ich im Keller der Klinik die Bestände an Alt-Unterlagen besichtigen - und die Akte der Petentin rasch ausfindig machen.

Der Universitätsklinik wurde dann eröffnet, daß bei der Kontrolle auch eine ganz bestimmte Akte gesucht worden sei und daß sich die betroffene Person vermutlich bald mit einem Akteneinsichtsgesuch melden werde.
Dem folgte ein längeres Gespräch, in dem versucht werden mußte, den Psychiater davon zu überzeugen, daß er die Unterlagen, vor allem das Patientenverzeichnis, weil sie als Universitätsklinik-Unterlagen entstanden waren, herauszurücken hatte.

Inzwischen hat die Übergabe der Unterlagen an die Universitätsklinik stattgefunden, hat die Petentin ihre Akte eingesehen - und habe ich den Sachverhalt der Staatsanwaltschaft unterbreitet, denn es liegt ein meines Erachtens unzweifelhafter Verstoß gegen den Straftatbestand des § 35 Abs. 5 SächsDSG vor.

Länger zurückliegende ärztliche Aufzeichnungen der Psychiatrie haben eine ungleich höhere Bedeutung als in anderen Bereichen der Medizin. Der Psychiater hat das Patientenverzeichnis und damit den Schlüssel zu größeren Beständen an Patientenunterlagen an sich gebracht. Dies hat ihm einen unberechtigten Wettbewerbsvorteil verschafft. Für die Einstellung, mit der er gehandelt hat, ist es bezeichnend, daß er der Petentin auf deren Frage nicht deren Aktenzeichen herausgesucht und mitgeteilt hat, sondern sein Wissen zu privatem „Herrschaftswissen“ gemacht hat - was § 35 SächsDSG gerade verhindern soll.

### 5.8.2 Einsichtnahme von Sicherheitsbehörden in archivierte melderechtsfremde Daten

Wie ich erfahren habe, haben Nachrichtendienste, Polizei und Staatsanwaltschaften in einzelnen Fällen versucht, Zugang zu archivierten melderechtsfremden Altdaten (z. B. aus den alten Kreismeldedateien) zu erhalten.

Soweit alte Meldedaten gemäß § 5 Abs. 5 Satz 1 (i. V. m. § 13 Abs. 3 Satz 1) SächsArchG von einem Archiv übernommen worden, also im Rechtssinne Archivgut geworden sind, unterliegt die Einsichtnahme in die in den Unterlagen vorhandenen personenbezogenen Daten ausschließlich Archivrecht.

Danach gilt folgendes:
Archivgut darf erst nach Ablauf der in § 10 Abs. 1 SächsArchG genannten Schutzfristen benutzt werden. Diese Schutzfristen sind sehr lang; im Regelfall wird Archivgut erst 30 Jahre nach Entstehung der Unterlagen für die Benutzung freigegeben. Für personenbezogenes Archivgut, d. h. Akten und Daten, die sich auf eine natürliche Person beziehen, können sich diese Fristen noch verlängern (vgl. § 10 Abs. 1 Satz 3 und 4 SächsArchG).

Die Schutzfristenregelung des § 10 Abs. 1 SächsArchG enthält ein Übermittlungsverbot:
Bis zum Ablauf der Schutzfristen darf das Archiv die Benutzung der betreffenden Unterlagen nicht zulassen, d. h. datenschutzrechtlich gesprochen, es darf keine in den Unterlagen enthaltenen Daten übermitteln.
Das gilt für kommunale wie für staatliche Archive gleichermaßen (vgl. § 13 Abs. 3 Satz 1 SächsArchG).

Dieses Übermittlungsverbot wird nicht durch die in anderen Rechtsvorschriften geregelten Erhebungs- und Übermittlungsbefugnisse verdrängt:

a) Einer Einsichtnahme des Landesamtes für Verfassungsschutz vor Ablauf der Schutzfristen steht die ausdrückliche Regelung des § 13 Abs. 1 Nr. 3 SächsVSG entgegen. Danach unterbleibt die Übermittlung von Informationen, zu der das Archiv nach den §§ 10 und 11 SächsVSG grundsätzlich verpflichtet ist, wenn besondere gesetzliche Übermittlungsregelungen entgegenstehen. Darunter fällt das Übermittlungsverbot des § 10 SächsArchG.
b) Das gleiche gilt für Einsichtnahmeersuchen des Bundesamtes für Verfassungsschutz gemäß § 23 Nr. 3 BVerfSchG i. V. m. § 10 Abs. 3 Satz 1, Abs. 1 SächsArchG sowie des Militärischen Abschirmdienstes gemäß § 12 MADG i. V. m. § 10 Abs. 3 Satz 1, Abs. 1 SächsArchG.
c) Ähnlich ist die Rechtslage für Einsichtnahmeersuchen des Bundesnachrichtendienstes. Zwar hat der Bundesnachrichtendienst gemäß § 2 Abs. 1 BND-Gesetz grundsätzlich im Rahmen des für die Erfüllung seiner gesetzlichen Aufgaben Erforderlichen eine grundsätzliche Erhebungsbefugnis. Der BND darf gemäß § 8 Abs. 3 Satz 1 BND-Gesetz diese Erhebung auch dadurch durchführen, daß er Behörden jeder Art und die Übermittlung der von ihm benötigten personenbezogenen Daten ersucht. Nichtsdestoweniger gilt jedoch auch im Falle des BND ein

Verbot für andere Behörden, dem Bundesnachrichtendienst Nachrichten zu übermitteln, wenn besondere gesetzliche Übermittlungsregelungen entgegenstehen: § 23 Nr. 3, 2. Halbsatz Bundesverfassungsschutzgesetz i. V. m. § 10 BND-Gesetz.

Einer Benutzung des Archivgutes vor Ablauf der festgelegten Schutzfristen ist in den vorstehenden Fällen nur möglich bei einer Verkürzung der festgelegten Fristen. Eine Verkürzung kann gemäß § 10 Abs. 4 Satz 1 SächsArchG erfolgen, wenn im Einzelfall ein öffentliches Interesse an einer Verkürzung gegeben ist. Bei personenbezogenem Archivgut ist eine Verkürzung allerdings nur zulässig für bestimmte Forschungsvorhaben (§ 10 Abs. 4 Satz 2 SächsArchG). Nachforschungen von Sicherheitsbehörden sind selbstverständlich keine Forschungsvorhaben in diesem Sinne.

Soweit sich das Archivgut ausschließlich auf Amtsträger in Ausübung ihrer Ämter in dem weiten Sinne des § 10 Abs. 2 Satz 3, 2. Halbsatz SächsArchG bezieht, sind die dem Persönlichkeitsrechtsschutz dienenden Schutzfristen nach dem Gesetz gar nicht anwendbar. Aber auch die allgemeinen Schutzfristen stellen für solches Archivgut kein Zugangshindernis dar, insoweit sie gemäß § 10 Abs. 2 Satz 2 SächsArchG für DDR-Altdaten nicht gelten; der Berufung auf öffentliches Interesse zur Begründung einer Schutzfristverkürzung (gemäß § 10 Abs. 4 Satz 1 SächsArchG) bedürfte es insoweit also nicht.

Der Meinungsaustausch zur Frage des Datenzugangs für Polizei und Staatsanwaltschaft ist noch nicht abgeschlossen. Der umfassenden Erhebungsbefugnis der Staatsanwaltschaft und Polizei zur Strafverfolgung gemäß § 161 Satz 1 StPO steht das für die Dauer der Schutzfristen geltende Übermittlungsverbot des § 10 Abs. 1 SächsArchG entgegen.
Über die Frage, wie die beiden Normen sich zueinander verhalten, befinde ich mich mit dem SMI, dem SMJus, der Generalstaatsanwaltschaft, dem Landesamt für Verfassungsschutz und dem Landeskriminalamt im Gespräch.
Bis zu einer abschließenden Meinungsbildung habe ich darum gebeten, Staatsanwaltschaft und Polizei keine Einsicht in die Unterlagen zu gewähren.

### 5.8.3 Der Weg ins Archiv als „Einbahnstraße“ für personenbezogene Daten

1. Ein Kommunalarchiv, das über Meldekarten aus der Zeit des Dritten Reiches verfügt, hat angefragt, ob es diese dem Internationalen Suchdienst (ISD) in Arolsen überlassen dürfe, der ein Interesse an der Übernahme der Unterlagen bekundet habe. (Zum ISD vgl. bereits früher unter 2/5.8.4 und 3/5.3.3.1.)
   Ich habe dem Kommunalarchiv mit Zustimmung des SMI folgendes mitgeteilt:

   Die Überlassung der archivierten Meldekarten an den Suchdienst wäre archivrechtlich gesehen eine Veräußerung des Archivgutes. Eine solche Veräußerung ist, solange die Archivwürdigkeit gegeben ist, gemäß § 8 Abs. 4 i. V. m. § 13 Abs. 3 Satz 1 SächsArchG verboten. Archivwürdig sind die Unterlagen jedenfalls so lange, wie der ISD die in den Unterlagen enthaltenen Daten für die Erfüllung seiner Aufgabe (Suchtätigkeit) benötigt.

Daneben können die Unterlagen auch aus anderen Gründen archivwürdig sein. Hierzu zählt alles, was ihnen gemäß § 2 Abs. 3 SächsArchG einen bleibenden Wert für - erstens - Gesetzgebung, Rechtsprechung, Regierung und Verwaltung, für - zweitens - Wissenschaft und Forschung oder - drittens - für die Sicherung berechtigter Belange betroffener Personen und Institutionen oder Dritter zukommen läßt.
Solange die Unterlagen archivwürdig sind, besteht eine Aufbewahrungspflicht des Archivs (§ 4 Abs. 2 Satz 1 i. V. m. § 2 Abs. 4, § 13 Abs. 1 SächsArchG).
Benötigte der ISD die Unterlagen für seine Aufgabenerfüllung gar nicht mehr und entfiele darüber hinaus sogar die Archivwürdigkeit insgesamt, dann fehlte es an der Befugnis zur Übermittlung der in ihnen enthaltenen personbezogenen Daten, die für eine Überlassung der Unterlagen erforderlich wäre, solange nicht alle archivrechtlichen Schutzfristen abgelaufen sind. Denn die Übermittlung wäre nicht *Aufgabe* des Archivs, und der ISD benötigte die Daten ja nicht mehr zur Erfüllung seiner Aufgaben - mit der Folge, daß die Voraussetzungen des § 13 Abs. 1 Nr. 1 SächsDSG nicht erfüllt sein könnten.

Kurz: Die Unterlagen dürfen daher einem Dritten, auch einer Einrichtung wie dem ISD, nicht überlassen werden. Der ISD darf sie aber nach Maßgabe der §§ 13 i. V. m. 9 und 10 SächsArchG nutzen.

2. Das Kommunalarchiv hat außerdem gefragt, unter welchen Voraussetzungen es die Unterlagen vernichten dürfe. Diese Frage ist folgendermaßen zu beantworten:

   Erst wenn die Archivwürdigkeit der Unterlagen weggefallen ist, sind die Archive gemäß § 8 Abs. 2 (i. V. m. § 13 Abs. 3 Satz 1) SächsArchG befugt, diese Unterlagen zu vernichten: § 8 Abs. 2 SächsArchG läßt sich nicht anders verstehen, als daß die ursprünglich gegeben gewesene Archivwürdigkeit im Laufe der Zeit auch einmal wegfallen kann, das heißt im Lichte der dann vorhandenen Erkenntnisse der Archivbehörde (denn ein Archiv einer öffentlichen Stelle ist eine Behörde!) nicht mehr besteht. Bei den ersten beiden Fallgruppen des § 2 Abs. 3 SächsArchG wird dies wohl recht selten vorkommen; dagegen dann, wenn sich die Archivwürdigkeit ausschließlich nach der dritten Fallgruppe der Vorschrift begründet, vermutlich gar nicht so selten. (Im vorliegenden Fall habe ich darauf hingewiesen, daß die Archivfachleute des SMI den Wert, den Meldeunterlagen dieser Art für die Wissenschaft haben, sehr hoch einschätzen.)

   Die Vernichtungs-Befugnis nach § 8 Abs. 2 SächsArchG ist rein archivrechtlich zu verstehen. Daher gilt: Wird die Archivwürdigkeit der Unterlagen verneint, ist eine weitere Aufbewahrung durch das Archiv nicht mehr erforderlich. Damit ist aber noch keine vollständige Aussage über den weiteren Verbleib der Unterlagen getroffen.

   Bei der Frage nach dem endgültigen Verbleib sind (a) die möglicherweise bestehenden Interessen öffentlicher Stellen und Privater an der Nutzung dieser Unterlagen zu berücksichtigen sowie (b) die datenschutzrechtlichen Interessen der Betroffenen:

Der Weg ins Archiv ist eine ‘Einbahnstraße’. Hier werden die Unterlagen so lange aufbewahrt, bis auch das letzte berechtigte Interesse an ihnen erloschen ist, d. h. bis die Unterlagen nicht mehr archivwürdig sind. Danach gibt es kein schützenswertes Interesse von Behörden und Privaten an der Nutzung des Inhalts der Unterlagen mehr. Von daher gesehen fehlt es an einer Grundlage für eine weitere Aufbewahrung durch das Archiv und auch, wie oben gezeigt, für eine Übergabe der Unterlagen an eine dritte Stelle, die an den Daten interessiert sein könnte.
Weiterhin sind die datenschutzrechtlichen Regelungen zu Gunsten der Betroffenen zu berücksichtigen. Dies gilt so lange, wie die dem Schutz des Persönlichkeitsrechts dienenden Schutzfristen des SächsArchG (§ 10 Abs. 1 Satz 3 und 4) noch nicht abgelaufen sind.

Maßgebliche Regelung ist § 19 SächsDSG. Danach sind personenbezogene Daten in Dateien zu löschen, wenn ihre Kenntnis für die speichernde Stelle zur Erfüllung ihrer Aufgaben nicht mehr erforderlich ist (§ 19 Abs. 1 Nr. 2 SächsDSG). Personenbezogene Daten in Akten sind zu löschen, wenn die speichernde Stelle im Einzelfall feststellt, daß die gesamte Akte zur Aufgabenerfüllung nicht mehr erforderlich ist (§ 19 Abs. 2 SächsDSG). Speichernde Stelle ist das Archiv. Dessen Aufgabe ist das Archivieren archivwürdiger Unterlagen. Ist die Archivwürdigkeit entfallen, ist die Aufgabe in diesem Sinne erfüllt. Die Daten sind daher zu löschen, d. h. die Unterlagen sind zu vernichten. Anderes gilt nur, wenn ein Fall des § 19 Abs. 4 SächsDSG vorliegt:
Der Tatbestand des § 19 Abs. 4 Nr. 1 SächsDSG kann jedoch nicht erfüllt sein: Schutzwürdige Interessen des Betroffenen an der Aufbewahrung wurden schon bei Prüfung der Archivwürdigkeit berücksichtigt (vgl. § 2 Abs. 3, 3. Fallgruppe SächsArchG).
Aber auch der Tatbestand des § 19 Abs. 4 Nr. 2 SächsDSG scheidet aus: Ist der Löschungstatbestand des § 19 Abs. 2 erfüllt, kann dieser 2. Ausnahmetatbestand des § 19 Abs. 4 schon begrifflich nicht erfüllt sein (vgl. auch Auernhammer, Bundesdatenschutzgesetz, Kommentar, Rdnr. 27 zu § 20 BDSG mit dessen ähnlicher Regelung in Abs. 3 Nr. 3).

Zusammenfassend gilt also: Die Unterlagen sind, solange der Personenbezug im datenschutzrechtlichen Sinne nicht durch Ablauf der dem Persönlichkeitsschutz dienenden archivrechtlichen Fristen entfallen ist, bei Wegfall der Archivwürdigkeit zu vernichten.

### 5.8.4 Behinderung des Zugangs der zeitgeschichtlichen Forschung zu noch nicht archivierten Altdaten

In § 5 Abs. 2 Satz 2 SächsArchG hat der Sächsische Gesetzgeber seinen entschiedenen Willen zum Ausdruck gebracht, daß die durch Geschichtsforschung und Geschichtsdarstellung stattfindende Aufarbeitung des KPD/SED-Regimes ohne Verzögerung möglich sein soll.

Daraus folgt, daß der Zugang zu Unterlagen aus dieser Zeit, auch wenn es sich um personenbezogene Daten handelt, nicht dadurch erschwert werden soll, daß die Un-

terlagen nicht archiviert werden. Werden die Unterlagen nicht archiviert, ist Zugang zu in ihnen enthaltenen personenbezogenen Daten zu Forschungszwecken nach § 12 Abs. 2 Nr. 4 SächsDSG (i. V. m. § 15 Abs. 1 Nr. 2 oder auch § 13 Abs. 1 SächsDSG) zu gewähren, statt nach § 10 Abs. 4 Satz 2 SächsArchG.

Der Unterschied zwischen beiden Regelungen ist beträchtlich. Die Forschung hat nach sächsischem Archivrecht einen erheblich weitergehenden Zugang zu Unterlagen mit personenbezogenen Daten als nach SächsDSG. Ich habe das bereits früher unter 3/5.8.2 nachdrücklich geltend gemacht. Vergleicht man im einzelnen, ergibt sich folgendes Bild:

- Nach § 10 Abs. 4 Satz 2 SächsArchG sind bei der Abwägung mit dem öffentlichen/wissenschaftlichen Interesse an der Durchführung des Forschungsvorhabens nur die *schutzwürdigen* Belange des Betroffenen zu berücksichtigen, nach § 12 Abs. 2 Nr. 4 SächsDSG dagegen jegliches Interesse des Betroffenen.

- § 10 Abs. 4 Satz 2 SächsArchG verlangt nur, daß die personenbezogenen Daten für das wissenschaftliche Vorhaben zweckdienlich, förderlich sind; dies geschieht durch das Wort „für“, synonym mit ‘zum Zweck’. Demgegenüber verlangt § 12 Abs. 2 Nr. 4 SächsDSG - enger - die Erforderlichkeit der Verwendung des Datums für die wissenschaftliche Forschung.

- Amtsträgern in Ausübung ihrer Ämter kommen die persönlichkeitsbezogenen Schutzfristen des § 10 Abs. 1 Satz 3 SächsArchG gemäß Abs. 2 Satz 3 derselben Vorschrift in keinem Fall zugute. Demgegenüber ist bei der Anwendung des § 12 Abs. 2 Nr. 4 SächsDSG durchaus bei der Interessenabwägung ein Schutzinteresse des Bediensteten nicht völlig ausgeschlossen.

- Im Falle der Übermittlung an private Forschungtreibende, also bei Anwendung des § 15 Abs. 1 Nr. 2 SächsDSG nähert sich das allgemeine Datenschutzrecht dem Archivrecht möglicherweise an, indem es auf die Schutzwürdigkeit des Interesses des Betroffenen am Unterbleiben der Übermittlung abstellt, wobei man jedoch Zweifel haben muß, ob diese Regelung auch im Bereich des Tatbestandes des § 12 Abs. 2 Nr. 4 SächsDSG Anwendung finden soll. Jedenfalls wird man in diesen Fällen aber kaum die Hürde des § 15 Abs. 3 SächsDSG überwinden können, weil es typisch für archivierte Unterlagen ist, daß nicht alle Betroffenen mit ihrer aktuellen oder halbwegs aktuellen Anschrift bekannt sind, so daß man zu der doch recht engen Ausnahmevorschrift zu Gunsten *schwerwiegender öffentlicher oder privater Belange* Zuflucht nehmen müßte.

- Sofern sich die Übermittlung zu Forschungszwecken nach § 13 Abs. 1 SächsDSG bestimmen sollte, käme die an Daten interessierte forschungsbetreibende öffentliche Stelle sogar in den Genuß der in § 13 Abs. 2 Satz 2 für den Regelfall der übermittelnden Stelle eingeräumten Erleichterung. Wie § 10 Abs. 4 Satz 2 SächsArchG zeigt, paßt dies für den Fall der Übermittlung aus archivierten oder zu archivierenden Daten jedoch schlecht: Die bereichsspezifische Regelung des Archivgesetzes paßt entschieden besser, weil das Archiv - als Behörde - durchaus

gerade das Metier, die Aufgaben auf der Seite des Übermittlungsempfängers, also eben auf Seiten der Forschungstreibenden im Prinzip doch recht gut beurteilen kann, weswegen insofern die strengere, weil eben spezifischere Regelung des Archivgesetzes auch angemessen und zum Zweck des Grundrechtsschutzes geboten ist.

Aufgrund dessen wird man sagen müssen, daß es der Wille des Sächsischen Archivgesetzgebers ist, daß alle Daten, die unter § 4 Abs. 2 Satz 2 und 3 SächsArchG fallen, also die personenbezogenen Daten in den Unterlagen, die aus der Zeit vom 8.5.1945 bis zum 2.10.1990 bei Funktionsvorgängern der jetzigen Stellen des Freistaates und im gesamten Bereich der Staatswirtschaft und der Parteien und gesellschaftlichen Organisationen angefallen sind, der Forschung mit der in § 5 Abs. 2 SächsArchG angeordneten Kurzfristigkeit zur Verfügung stehen sollen. Wenn dem so ist, ist § 5 Abs. 1 SächsArchG nicht so auszulegen, daß Stellen des Freistaates Sachsen Unterlagen, die unter § 4 Abs. 2 Satz 2 und 3 SächsArchG fallen, nur nach Maßgabe von § 5 Abs. 1 Satz 2 SächsArchG, also eben nicht unverzüglich dem Staatlichen Archiv anzubieten haben. Anderenfalls entzögen nämlich bloße Verwaltungsvorschriften wichtige Unterlagen weitgehend der zeitgeschichtlichen Forschung.

Ein Fall, in dem sich die noch nicht durchgeführte Archivierung forschungsbehindernd auszuwirken droht, ist unter 5.8.5, im Teil (2) beschrieben; es handelt sich um die Personalakten früherer Justizbediensteter.

Ein ganz ähnlicher Fall sind die bisher noch von den Justizvollzugsanstalten verwahrten Unterlagen ehemaliger Strafgefangener. Einigkeit besteht hier darüber, daß die Gefangenenakten von den Justizvollzugsanstalten, die sie aufbewahren, zur Erfüllung ihrer eigenen Aufgaben nicht mehr benötigt werden. Dies hätte zur Folge, daß die Justizvollzugsverwaltungen gemäß § 5 Abs. 1 Satz 1 SächsArchG verpflichtet wäre, die Gefangenenakten dem zuständigen Staatsarchiv anzubieten. Es könnte allerdings sein, daß gemäß § 5 Abs. 1 Satz 2 SächsArchG das Entstehen dieser Pflicht noch hinausgeschoben, die Anbietungspflicht also noch nicht entstanden ist, weil eine Verwaltungsvorschrift eine längere Aufbewahrungsfrist für die Justizverwaltung bestimmt. Auf eine solche Verwaltungsvorschrift, die eine 30jährige Aufbewahrung für die Personalakten der Gefangenen bestimmt, beruft sich das SMJus dann auch. Voraussetzung ist dabei jedoch, daß die Ausnahmevorschrift des § 5 Abs. 1 Satz 2 SächsArchG auch auf den Fall des § 5 Abs. 1 Satz 1 des Gesetzes anzuwenden ist. Ohne das Für und Wider dieser Auslegung hier im einzelnen zu erörtern, kann man feststellen: Eine solche Auslegung von § 5 Abs. 1 Satz 1 und 2 SächsArchG ist sinnvoll, aber nach dem Wortlaut keineswegs über jeden Zweifel erhaben. Ich habe dem für Archivrechtsfragen zuständigen SMI mitgeteilt, daß ich diese Auslegung für vorzugswürdig halte und angeregt, im Rahmen einer Novellierung des Archivgesetzes die Vorschrift insoweit klarer zu fassen.

Es fragt sich dann allerdings noch, ob die bisher praktizierte Lösung, nämlich die Unterlagen weiterhin in den Strafvollzugsanstalten zu belassen, an § 5 Abs. 2 SächsArchG scheitert.

Es leuchtet zwar sehr ein, worauf das SMJus mit Recht hinweist und womit auch seitens der staatlichen Archivverwaltung Einverständnis besteht, nämlich, daß die Strafvollzugsanstalten viel besser in der Lage sind, die wöchentlich etwa zehn bei ihnen von Trägern der Sozialversicherung eingehenden Begehren nach Auskünften aus den Haftunterlagen der ehemaligen Strafgefangenen beantworten zu können, als dies durch Bedienstete des Staatsarchivs geschehen könnte, die in Vorgänge dieser Art nicht eingearbeitet und ohnehin mit anderen Aufgaben ausgelastet sind; von den auch in der Öffentlichkeit bekannten (lösbaren) Raumproblemen der Staatsarchive ganz zu schweigen.

Vom praktischen Ergebnis her leuchtet dieser Standpunkt ohne weiteres ein. Er hat allerdings einen Haken:
§ 5 Abs. 2 Satz 1 SächsArchG ist, zwar nicht unbedingt vom Wortlaut her, aber nach der angesichts der mangelnden - hier aus Platzgründen nicht näher zu erläuternden - Eindeutigkeit des Wortlautes der historischen Auslegung so zu verstehen, daß auch die bei Gerichten, Behörden und sonstigen öffentlichen Stellen des Freistaates Sachsen selbst (vgl. § 5 Abs. 1 Satz 1 SächsArchG) vorhandenen Altdaten (Unterlagen im Sinne von § 4 Abs. 2 Satz 2 und 3) unverzüglich anzubieten sind. Die gegenwärtige Fassung des § 5 Abs. 2 SächsArchG geht nämlich zurück auf einen Antrag der Vertreter der SPD-Fraktion im Innenausschuß des Sächsischen Landtages, der damit begründet ist, die Vorschrift solle in ihrer - dann Gesetz gewordenen Formulierung - *zur effektiven Aufarbeitung der Vergangenheit einen sofortigen Zugriff auf die Unterlagen der in § 4 Abs. 2 Satz 2 und 3 genannten Stellen ermöglichen, statt erst nach evtl. 30 Jahren*, wie bis dahin im Gesetzentwurf vorgesehen. Dies ist eindeutig so zu verstehen, daß auch diejenigen Unterlagen gemeint sind, die bei Rechtsvorgängern des Freistaates Sachsen und Funktionsvorgängern der in § 4 Abs. 2 Satz 1 SächsArchG genannten Stellen - eben des Freistaates selbst - angefallen sind (vgl. § 4 Abs. 2 Satz 2 SächsArchG, am Anfang).

Zusammenfassend: § 5 Abs. 2 SächsArchG so zu verstehen, daß er ausschließlich die nicht zum Freistaat selbst gehörenden Personen und Stellen zur Anbietung verpflichtet, wäre praktisch durchaus sinnvoll. Einer solchen Regelung läge der Gedanke zugrunde, daß die Altdaten beim Staat insgesamt in guten Händen sind, sei es nun in der Archivbehörde oder aber in sonstigen Stellen des Staates, also den Fachbehörden. Damit stellt man den Sicherungsgedanken in den Vordergrund und man hätte eine ordentliche praktische Lösung für Fälle wie die Strafgefangenenakten, aber auch andere Akten, die noch benötigt werden, so z. B. Kriminalakten, noch heute benötigte Bestandteile von Personalakten weiterbeschäftigten staatlichen Personals, Akten über die Enteignung von Unternehmen, welche das LARoV hat und benutzt, auch etwa Akten der Staatlichen Vermögensverwaltung, oder auch Akten psychiatrischer Landeskrankenhäuser.
Das bedeutete, daß der Gedanke der Sicherung der Unterlagen im Vordergrund stünde. Nach § 5 Abs. 2 SächsArchG steht jedoch demgegenüber der Gedanke der Auswertung der Unterlagen und des Zuganges der Unterlagen im Vordergrund, und dieser Gedanke impliziert, daß alle Unterlagen sich im Archiv befinden sollen, als derjenigen Stelle, die gerade dafür zuständig ist, Zugang zu Unterlagen zwecks Erforschung vergangener Geschehnisse zu gewähren. Da die Sicherheit der Zugäng-

lichkeit dient, darf sie nicht zu einem die Zugänglichkeit verhindernden Faktor werden.

Der nachstehend in Abschnitt 5.8.5 unter (2) genannte Fall, aber auch die in einer kleinen Anfrage eines Landtagsabgeordneten (Drucksache 2/7490, ausgegeben am 13.1.1998) gestellte Frage nach der Verfügbarkeit der die Strafvollzugseinrichtung Bautzen II des DDR-MdI betreffenden Unterlagen zeigt, daß es dem Willen des sächsischen Gesetzgebers widerspricht, wenn die Erforschung der jüngeren Vergangenheit dadurch erschwert wird, daß die datenschutzrechtlichen Regelungen für den Zugang zu diesen Unterlagen sich statt nach Archivgesetz nach dem Sächsischen Datenschutzgesetz bestimmen, worauf sich das SMJus in seiner Antwort (vom 7. Januar 1998) auf die genannte Anfrage ausdrücklich festgelegt hat.

Als Ausweg aus diesem Dilemma habe ich dem SMI als dem für das Archivrecht zuständige Ressort vorgeschlagen, den Entwurf einer Regelung im Landtag einzubringen, welche bestimmt, daß auf Unterlagen, die unter § 4 Abs. 2 Satz 2 und 3 SächsArchG fallen und noch nicht archiviert sind, die Regelungen des § 10 Abs. 1, Abs. 2 und Abs. 4 SächsArchG entsprechend anzuwenden sind.

### 5.8.5 Zugang zu Daten zum Werdegang von DDR-Amtsträgern

Für Forschungsvorhaben zur DDR-Geschichte besteht vielfach auch Interesse daran, neben der eigentlichen Amtsführung im engeren Sinne den Werdegang von Funktionsträgern zu untersuchen.
Solches Forschungsinteresse fällt nicht aus dem Rahmen der üblichen Elitenforschung. Es fragt sich, inwieweit das Datenschutzrecht für die Erforschung der jüngeren Vergangenheit dem Grenzen setzt.

(1) Eine Anfrage, die an mich gerichtet worden ist, hat Universitätsprofessoren betroffen.

Ausgangspunkt der rechtlichen Überlegungen ist: Soweit Amtsträger in Ausübung ihres Amtes betroffen sind, gelten ganz allgemein die dem *Persönlichkeitsschutz* dienenden Schutzfristen (§ 10 Abs. 1 Satz 3 und 4 SächsArchG) gerade nicht (§ 10 Abs. 2 Satz 3, 1. Halbs. SächsArchG), weil sie insofern nicht Grundrechtsträger sind. Diese Regelung wird durch § 10 Abs. 2 Satz 3, 2. Halbs. für Unterlagen aus der Zeit zwischen dem Zusammenbruch des Dritten Reiches und der Wiedervereinigung auf die Bediensteten der Rechtsvorgänger des Freistaates Sachsen und der Funktionsvorgänger der heutigen öffentlichen Stellen im Freistaat Sachsen erstreckt (§ 4 Abs. 2 Satz 2, 1. Fallgruppe SächsArchG), eine Klarstellung, welche die logische Folge der Anerkennung der Staatlichkeit der DDR und ihrer Einrichtungen ist. (Vgl. auch schon früher unter 5/5.8, S. 108).

Zur Amtsausübung gehört bei Hochschulprofessoren der akademische Werdegang vom Anfang des Studiums an sowie das außerakademische öffentliche Wirken, und zwar in seinem Zusammenhang wie auch ggf. seinem Nicht-Zusammenhang mit dem Fach, welches der Professor - später oder gleichzeitig - vertreten hat.

Dies folgt aus den Besonderheiten des Amtes des Hochschulprofessors:
Er betreibt in (mittelbar) öffentlichem Auftrag Wissenschaft. Was die wissenschaftliche Lehre betrifft, ist er mit besonderer, durch die öffentliche Gewalt verliehener Ermächtigung tätig. In der alten Bezeichnung eines Ordinarius als *ordentlichen und öffentlichen Professors* kam dies, worauf unlängst W. Hennis noch einmal aufmerksam gemacht hat (FAZ v. 18. Februar 1998) zum Ausdruck: Die öffentlichen Professoren waren, im Unterschied zu den Privatdozenten, solche, denen der Staat ein öffentliches Amt, nämlich die wissenschaftlich freie Vertretung ihres Faches, übertragen hatte.
Daran hat sich durch neue Bezeichnungen („C 4-Professur“) nichts geändert. Unverändert ist der Hochschulprofessor in institutionalisierter Weise, nämlich durch Amtsinhaberschaft und korporationsrechtliche Stellung, zugleich in besonderer Weise Träger des Grundrechtes gemäß Artikel 5 Abs. 3 Satz 1 GG, Art. 21 der Sächsischen Verfassung und den entsprechenden Regelungen anderer Länder-Verfassungen.

Zu dieser Rechtsstellung gehören auch Lasten: Zum Wissenschaftsbetrieb gehören seit alters her notwendig Öffentlichkeit und Kritik. Zu den Regeln dieser im öffentlichen Raum stattfindenden Kritik gehört zwar, daß auf die Person des Urhebers wissenschaftlicher Lehren bezogene Argumente in der Wissenschaft letztlich nicht zählen. Aber es ist wissenschaftliche Erkenntnis, daß, trotz des Ideals der reinen Wissenschaftlichkeit, in der Realität des Wissenschaftsbetriebes die Wissenschaft doch nicht unabhängig von persönlichen Eigenheiten der Wissenschaftler (einzeln und als Gruppe) betrieben wird. Dies ist Gegenstand der historisch und soziologisch arbeitenden Wissenschaftsforschung (vgl. dazu unter rechtlichem Gesichtspunkt H.-H. Trute, Die Forschung zwischen grundrechtlicher Freiheit und staatlicher Institutionalisierung, Tübingen 1994, S. 70 ff., 87). Auch dabei geht es um Gesetzmäßigkeiten. Diese lassen sich jedoch mit der für die Wissenschaft erforderlichen Überprüfbarkeit oft nur anhand einzelner Personen aufzeigen, die für die betreffenden Fachkreise nicht anonym darstellbar sind (vgl. schon früher 5/5.8 unter [1]): In Fachkreisen kennt man sich eben auch heute noch, auch über die Grenzen von Staaten und Generationen hinweg.

Soweit es um den DDR-Wissenschaftsbetrieb geht, kommt noch ein Weiteres hinzu: Die DDR hatte die Gewaltenteilung zwischen Staatsgewalt und Wissenschaftsbetrieb, die in Idee und Wirklichkeit der europäischen Universität entwickelt worden ist, weitgehend beseitigt. Dies war die logische Folge der Vorstellung von der - einen - wissenschaftlichen Weltanschauung, eben des Marxismus-Leninismus. Deswegen hatten folgerichtig parteipolitische Gegebenheiten einen hervorragenden Einfluß auf wissenschaftliche Karrieren und wissenschaftliche Inhalte; ohne Wissen der Partei oder gar gegen die Partei war mit Ausnahme einiger Refugien, z. B. in den Kirchen, eine wissenschaftliche Karriere nicht möglich, mag dies auch heute von dem einen oder anderen verharmlost werden. Manche muten uns sogar zu, sich trotz wissenschaftlicher Karriere unter den Augen der SED zu Widerständlern zu stilisieren. Kommen dann noch Westreisen, weltweite Kontakte oder gar Spezialaufträge für die Herrschenden der DDR hinzu, ist das unerträglich, wenn nicht lächerlich.

Unter den Bedingungen des damals staatlich-weltanschaulich politisierten Wissenschaftsbetriebes sind daher für die Wissenschaftsforschung der DDR auch solche Umstände von Bedeutung, die unter anderen Voraussetzungen, nämlich bei Gewaltenteilung zwischen dem Kernbereich des Staates, insbesondere der Exekutive, und dem öffentlich-rechtlich organisierten Wissenschaftsbetrieb, nicht von vornherein bedeutungsvoll, sondern allenfalls in - systemwidrigen - Ausnahmefällen von Belang sind.

Konkret bedeutet das: Mitgliedschaft und Funktionsausübung in den gesellschaftlichen Massenorganisationen - wie sie ja in der Regel auf Personalfragebögen der DDR anzugeben waren -, erst recht natürlich etwa eine Tätigkeit in der SED-Grundorganisation an der Hochschule, unterliegen nicht den dem Persönlichkeitsschutz dienenden Schutzfristen des Archivrechts. Dasselbe gilt für Tätigkeiten, die darauf hinweisen, daß es gerade an einer facheinschlägigen Praxis gefehlt und eher politisches Wohlverhalten die Grundlage für die Berufung in wissenschaftliche Ämter gewesen ist.

Die vorstehenden Überlegungen sind unabhängig von den Besonderheiten des sächsischen Rechtes, insbesondere des Sächsischen Archivgesetzes. Denn die Grenzen des Persönlichkeitsschutzes für Amtsträger müssen durch Auslegung des Verfassungsrechts gewonnen werden.

(2) Ähnliches gilt für den Werdegang von DDR-Richtern und -Staatsanwälten.

Zu diesem Thema hat sich ein Assistent an der Universität Halle an mich gewandt, der eine Arbeit über „Die theologischen Fakultäten in der DDR als Problem der Kirchen- und Hochschulpolitik des SED-Staates bis zu ihrer Umwandlung in Sektionen 1970/71“ verfaßt und in diesem Zusammenhang politische Strafverfahren gegen christliche Studenten und auch das bekannte Strafverfahren gegen den Leipziger Studentenpfarrer Siegfried Schmutzler von 1957 untersucht.

In seiner Arbeit wollte der Verfasser zu Staatsanwälten und Richtern, die an den von ihm dargestellten politischen Strafverfahren maßgeblich beteiligt gewesen sind, den Vornamen, das Geburts- und ggf. auch das Todesjahr angeben können. Da die Personalakten dieser Bediensteten der DDR-Justiz offenbar noch nicht archiviert sind, sondern noch von der jetzigen Justizverwaltung aufbewahrt werden, hatte er sich mit der Bitte um Auskunft an die Staatsanwaltschaft Leipzig und dann an das SMJus gewandt, welches unter Berufung auf § 12 Abs. 2 Nr. 4 SächsDSG die Übermittlung von Vornamen, Geburts- und Todesjahr abgelehnt hat.

Ich habe dem SMJus mitgeteilt, daß ich den von ihm eingenommenen Standpunkt im Ergebnis teile, in der Begründung jedoch nicht zustimmen kann und der Meinung bin, daß dem Forscher, falls er dies wünsche, statt dessen andere, für sein Forschungsvorhaben und die Forschung insgesamt interessantere Daten zu den betreffenden Juristen zugänglich gemacht werden müßten. Dies ergibt sich im einzelnen aus folgenden Überlegungen:

Zweckmäßigerweise kann man dabei von der Frage, nach welcher Vorschrift genau eine zu Forschungszwecken stattfindende Übermittlung von Daten über die betreffen-

den Justiz-Bediensteten zu beurteilen ist - nämlich nach Archivrecht oder aber nach § 15 Abs. 1 Nr. 2 oder auch § 13 Abs. 1 i. V. m. § 12 Abs. 2 Nr. 4 SächsDSG - zunächst einmal absehen; ausführlicher zu diesen Fragen unter 5.8.4.
Dann geht es einfach darum, welche die an den untersuchten Vorgängen beteiligten Amtsträger betreffenden Daten benötigt werden bzw. dazu dienen können, den wissenschaftlichen Gehalt der Untersuchung zu erhöhen. Unter diesem Gesichtspunkt leuchtet dann die Auffassung des SMJus ein, daß die Vornamen und das Geburtsdatum - also im wesentlichen das Alter - und vor allem auch gegebenenfalls das Todesjahr als zusätzliche Angabe keine nennenswerte Bereicherung des Informationsgehaltes der Studie darstellen können. Denn in der Tat wären diejenigen, die zu benachbarten Forschungszwecken die Arbeit auswerten und auf den in ihr enthaltenen Anfangs-Informationen aufbauend Näheres über die betreffenden Juristen in Erfahrung bringen wollten, gehalten, eigene Auskunfts- bzw. Einsichtsansprüche gegenüber der Behörde, welche die Unterlagen aufbewahrt, geltend zu machen.

Andererseits aber erhielte der Teil der Untersuchung, der sich mit den genannten Strafverfahren beschäftigt, durchaus einen zusätzlichen Informationsgehalt, wenn auf das amtliche Tätigwerden der betreffenden Staatsanwälte und Richter dadurch zusätzliches Licht fiele, daß für die Art der Amtsausübung nicht unwichtige Umstände in der die Arbeit ergänzenden Kurzbiografie wiedergegeben würden. Folgende Daten müßten meiner Meinung nach zu den in der Arbeit erwähnten, weil an den betreffenden Vorgängen beteiligten, Staatsanwälten und Richtern offengelegt werden. Dies könnte dadurch geschehen, daß man einen tabellarischen Fragebogen, den der Autor der Behörde zusenden könnte, ausfüllte:
- Juristische Tätigkeit bis 1933
- juristische Tätigkeit 1933 bis 1945: Justiz/Verwaltung/Anwalt oder sonstiges
- Opfer von Verfolgung bzw. beruflicher Zurücksetzung 1933 bis 1945
- Abschluß Jurastudium bis Mai 1945
- ordentliches Jurastudium nach 1945 abgeschlossen
- Volksrichter-Ausbildung nach 1945
- KPD/SED-Parteimitglied seit [Jahresangabe]
- Blockpartei [Angabe der Partei] seit [Jahresangabe].

Wer Staatsanwalt oder Strafrichter in politischen Prozessen, zumal solchen von so großem Bekanntheitsgrad wie dem Strafverfahren gegen Pastor Schmutzler und damit zusammenhängenden Strafverfahren gewesen ist, hat es angesichts des hochpolitisierten Justizwesens der DDR hinzunehmen, daß diese für das Verständnis seiner Amtstätigkeit grundlegenden Umstände seines Werdeganges als Bestandteile seiner Amtstätigkeit offengelegt werden. Den Schutz des Grundrechts auf informationelle Selbstbestimmung kann er als Amtsträger hinsichtlich dieser für seine gesamte Amtstätigkeit als politischer Strafjurist in der DDR prägenden Umstände nicht beanspruchen.
Einer Überlegung, inwieweit er Person der Zeitgeschichte sein könnte, bedarf es dazu nicht.

Die Antwort des SMJus steht noch aus.

## 5.9 Polizei

### 5.9.1 Novellierung des Sächsischen Polizeigesetzes

Mit seinem Urteil zum Sächsischen Polizeigesetz hatte der Sächsische Verfassungsgerichtshof einige datenschutzrechtliche Bestimmungen des Gesetzes für verfassungswidrig erklärt, andere Bestimmungen nur bei verfassungskonformer Auslegung und nach Maßgabe der vom Gericht ausgesprochenen Vorgaben für zulässig erachtet. Hierüber habe ich in 5/5.9.1 eingehend berichtet.

In die Überlegungen des Sächsischen Staatsministeriums des Innern zur Novelle des Sächsischen Polizeigesetzes wurde ich frühzeitig eingebunden. Als Ergebnis der konstrukiven Besprechungen kann ich nun hervorheben, daß die Vorgaben des Sächsischen Verfassungsgerichtshofs zur Präzisierung der Vorschriften zur Datenerhebung mit besonderen Mitteln und zur Schaffung eines ausreichenden prozeduralen Grundrechtsschutzes bei ihrer Anwendung insgesamt umgesetzt worden sind. Neben den vom Gericht gebotenen Änderungen enthält der nunmehr vorliegende Referentenentwurf der Staatsregierung zwei bedeutende neue datenschutzrelevante Befugnisregelungen: Die verdachtsunabhängigen Kontrollen und die Umnutzung von Protokolldaten.

1. In § 19 Abs. 1 Nr. 5 des Entwurfs werden verdachtsunabhängige Kontrollen im öffentlichen Straßenverkehr der Sächsischen Polizei zur Erfüllung ihrer gesetzlichen Aufgaben als Instrumentarium an die Hand gegeben.

   Ich halte diese verdachtsunabhängigen Kontrollen aus datenschutzrechtlicher Sicht unter den im Entwurf gegebenen Voraussetzungen, insbesondere in Anbetracht der verfahrenssichernden Maßnahmen (Pflicht dem Sächsischen Datenschutzbeauftragten über die Zahl und die Ergebnisse zu berichten) für verhältnismäßig:

   - Der grenzüberschreitende Verkehr zwischen dem Freistaat Sachsen und dem südlichen und östlichen außerhalb der europäischen Gemeinschaft stehenden Anrainerstaaten hat überdimensional stark zugenommen. Dies führt dazu, daß die früher üblichen und zum Teil ins einzelne gehenden Grenzkontrollen nicht mehr möglich sind, ohne einschneidend in das Grundrecht der Betroffenen auf Freizügigkeit einzugreifen. Im Kielwasser des grenzüberschreitenden Verkehrs haben sich Kriminalitätsformen entwickelt, die von den sächsischen Polizeidienststellen sowohl zum Zwecke der Gefahrenabwehr als auch zum Zwecke der Strafverfolgung ermittelt werden müssen. Als Ermittlungsansatz halte ich verdachtsunabhängige Kontrollen auf bedeutenden, letztlich dem grenzüberschreitenden Verkehr dienenden Straßen im rückwärtigen Raum der Grenze für geeignet, erforderlich und zumutbar.

   - Mit Verkehrskontrollen allein ist der Zweck, grenzüberschreitenden Kriminalitätsformen zu begegnen, nicht erfüllbar, weil die Beifahrer nicht kontrollierbar sind und der Inhalt des Fahrzeugs - bis auf die der Verkehrssicherheit dienenden Gegenstände - nicht zu untersuchen ist.

- Es handelt sich bei den im Entwurf vorgesehenen Kontrollmaßnahmen nicht um „rechtswidrige Ausgleichsmaßnahmen“, die gegen die Freizügigkeit im Sinne des Schengener Durchführungsübereinkommens gerichtet sein könnten, weil der Schutz der Außengrenze Sachsens die EG-Außengrenze betrifft, die vom Schengener Durchführungsabkommen nicht erfaßt ist.

- Dem Polizeirecht sind verhaltensunabhängige Kontrollen nicht gänzlich fremd: Ich verweise dazu auf die Lehre vom „verrufenen Ort“ sowie auf die im Luftverkehr üblichen Personen- und Gepäckkontrollen, wobei ich allerdings gewisse Unterschiede zwischen dem Straßenverkehr und den besonderen Gefahren des Luftverkehrs durchaus sehe. Wir sollten uns aber vergegenwärtigen, daß auch der Luftverkehr mittlerweile ein Massenverkehr ist, der - jedenfalls nach Erfahrungen in Deutschland - nicht einer besonderen Gefährdung ausgesetzt ist. Dies ist auf die Wirkung der Personenkontrollen zurückzuführen. Es ist erklärter Zweck der Personen- und Gepäckkontrollen im Luftverkehr, nicht nur die dem Luftverkehr selbst drohenden Gefahren zu bannen, sondern darüber hinaus auch eine Kontrolle des grenzüberschreitenden Verkehrs durchzuführen und damit dessen besondere Gefahren abzuwehren.

Unter den gegebenen Umständen findet daher diese neue Befugnisregelung im Gesetzentwurf der Staatsregierung meine grundsätzliche Unterstützung. In einem Punkt bedarf jedoch die neue Regelung einer Präzisierung im Gesetz, zumindest aber in den entsprechenden Verwaltungsvorschriften:

Im Zusammenhang mit den verdachtsunabhängigen Kontrollen bemängele ich, daß der Anknüpfungstatbestand „andere Straßen von erheblicher Bedeutung für die Kriminalität“ nicht ausreichend klar ist. Die in der Entwurfsbegründung angeführte Erläuterung „Straßen von lokaler und regionaler Bedeutung im Hinterland werden von dem Anwendungsbereich der neuen Vorschrift nicht erfaßt; dort sind polizeiliche Kontrollen weiterhin unter den bisher bereits geltenden Voraussetzungen zulässig“ erklärt nicht, wann eine Straße von Bedeutung für die grenzüberschreitende Kriminalität ist. Das Problem besteht darin, daß die (möglicherweise vorhandenen) objektiven Kriterien zur Einstufung der Straße nur von der Polizei erhoben und ausgewertet werden. Die damit zusammenhängenden Erkenntnisse werden dem Betroffenen nicht mitgeteilt. Sie sind daher letztlich zwar im gerichtlichen Verfahren nachprüfbar, aber jedenfalls durch den einzelnen Betroffenen nicht vorhersehbar. Damit erfüllt die Vorschrift nicht das verfassungsrechtliche Gebot der Normenklarheit, das darin besteht, daß grundsätzlich jede geplante hoheitsrechtliche Maßnahme durch den Einzelnen vorhersehbar sein muß.

2. Im Zusammenhang mit der vom Entwurf vorgesehenen Befugnis zum Umnutzen von Protokolldaten halte ich eine gesetzliche Fixierung dieser Nutzung, die auf den begründeten Einzelfall abstellt, für notwendig. Die Entwurfsregelung erlaubt die Umnutzung der Protokolldaten „auch zum Zweck der Abwehr von Gefahren für Leben, Gesundheit oder Freiheit einer Person oder für bedeutende fremde Sach- oder Vermögenswerte sowie zur vorbeugenden Bekämpfung von Straftaten

von erheblicher Bedeutung“ - mithin zu einem nahezu generalklauselartig umschriebenen Gefahrenabwehrzweck.

Eine Präzisierung dieser Vorschrift ist wünschenswert; die Nutzung von Protokolldaten sollte nur im schriftlich zu begründenden Einzelfall stattfinden, auch darüber ist dem Datenschutzbeauftragten zu berichten. Denn die Protokolldaten haben den Zweck, den Datenschutz zu ermöglichen; deshalb sollte ihre Nutzung zu anderen Zwecken dem Datenschutzbeauftragten zumindest zur Kenntnis gelangen. Damit wäre ein hinreichender Grundrechtsschutz (Stichwort: „Grundrechtsschutz durch Verfahren“) gewährleistet. Da die Nutzung von Protokolldaten zum Zwecke der Polizeiarbeit nur ein seltener Ausnahmefall bleiben dürfte, wäre der mit der Berichtspflicht verbundene Verwaltungsaufwand gering.

### 5.9.2 Gesetz über die Erprobung einer sächsischen Sicherheitswacht (Sächsisches Sicherheitswachterprobungsgesetz - SächsSWEG)

Über die datenschutzrechtlichen Anforderungen, die an ein Gesetz zum Einsatz einer Sicherheitswacht zu stellen sind, habe ich in 5/5.9.2 berichtet. Meine Empfehlungen wurden vollständig in das inzwischen in Kraft getretene Gesetz eingearbeitet und in der zugehörigen Verwaltungsvorschrift des SMI nochmals konkretisiert. Hervorzuheben ist hierbei, daß die von den Angehörigen der sächsischen Sicherheitswacht erhobenen und von ihnen schriftlich fixierten Daten unverzüglich, spätestens jedoch zum jeweiligen Dienstende, der für die Sicherheitswacht zuständigen Polizeidienststelle weiterzuleiten sind. Eine darüber hinausgehende Datenspeicherung ist nicht zulässig. Auch werden die Angehörigen der sächsischen Sicherheitswacht durch die Verwaltungsvorschrift verpflichtet, zu Kontrollzwecken ihre Eingriffsmaßnahmen schriftlich zu dokumentieren und diese Schriftstücke unverzüglich der Polizeidienststelle weiterzuleiten. Kopien dieser Dokumente dürfen bei der Sicherheitswacht nicht verbleiben. Die Verwaltungsvorschrift stellt ferner klar, daß für die Datenübermittlung der Polizeidienststelle an die Sicherheitswacht die Aufgabenzuweisung nach § 2 SächsSWEG maßgebend ist: Damit wird gewährleistet, daß nur solche polizeilichen Daten in die Hände der Sicherheitswacht gelangen, die dem - auch zeitlich - begrenzten Aufgabenbereich der Sicherheitswacht unterfallen können.

Das Beispiel des SächsSWEG und seiner Verwaltungsvorschrift zeigt, daß im Dialog auch auf in der Öffentlichkeit kontrovers diskutierten und brisanten neuartigen Regelungsgebieten eine datenschutzgerechte Normgestaltung zu erzielen ist.

### 5.9.3 Initiativermittlungen im Rahmen der Bekämpfung der Organisierten Kriminalität

In 5/5.9.10 habe ich die Voraussetzungen aufgeführt, unter denen Initativermittlungen, also Ermittlungen ohne Anfangsverdacht, im Bereich der organisierten Kriminalität datenschutzrechtlich zulässig sein können. Zu dieser Thematik habe ich

mit dem SMI und dem SMJus im Berichtszeitraum einige Besprechungen geführt, dabei habe ich folgende Auffassung vertreten:

Die Polizeigesetze der Länder regeln die Aufgaben und Befugnisse der (Landes-) Polizei auf dem Gebiet der Gefahrenabwehr. Die Strafprozeßordnung hingegen enthält als Bundesgesetz die für die (Landes-)Polizei maßgeblichen Vorschriften zur Strafverfolgung, denn insofern hat der Bund seine Kompetenz zur konkurrierenden Gesetzgebung auf den Gebieten des „Strafrechts“ und des „Gerichtlichen Verfahrens“ (Art. 74 Nr. 1 GG) wahrgenommen. Zum „Gerichtlichen Verfahren“ zählen auch die Aufgaben und Befugnisse der Polizei im Ermittlungsverfahren. Ferner ist Gegenstand der ausschließlichen Gesetzgebung des Bundes „die Zusammenarbeit des Bundes und der Länder ... in der Kriminalpolizei ... sowie ... die internationale Verbrechensbekämpfung“ (Art. 73 GG). Die klassische Unterscheidung zwischen den Bereichen der Gefahrenabwehr und der Strafverfolgung wird durch Aufgabenumschreibungen wie „Vorfeldbeobachtung“, „vorbeugende Verbrechensbekämpfung“ und „Initiativermittlungen“ vermischt. Die Datenverarbeitung der Polizei auf diesen wichtigen Feldern muß jedoch klaren Rechtsvorschriften zugeordnet werden können. Hauptzweck der mit dem Begriff der vorbeugenden Straftatenbekämpfung umschriebenen Datenverarbeitung ist die Vorbereitung auf die künftige Strafverfolgung. Dies ist eine Aufgabe die der Kriminalpolizei nach der Rechtsprechung des Bundesverwaltungsgerichts durch die Strafprozeßordnung zugewiesen ist. Verdachtsgewinnung, Verdachtssteuerung und Verdachtsverdichtung sollen in erster Linie Strafverfahren ermöglichen und erleichtern. Die Daten dienen folglich nicht der Gefahrenabwehr. Denn mit reiner Gefahrenabwehr wäre es nicht zu vereinbaren, die Gefahr zu beobachten und es zuzulassen, daß die Gefahr sich konkretisiert und - vor allem - sich steigert. Oftmals wird die Vergrößerung des Gefahrenpotentials regelmäßig in den Dienst einer Erleichterung späterer Überführung gestellt. Oder: Die Gefahr wird nicht bekämpft, um es statt dessen zu einer - in den Folgen zwar gebändigten, weil überwachten - Straftat (meist also ein Versuch) und danach zu einer Verurteilung kommen zu lassen. Dieses risikoreiche Verhalten muß nach meiner Überzeugung der Verfahrensherrschaft der Staatsanwaltschaft unterstellt werden (§§ 160 f. StPO). Soweit die vorsorgende Informationssammlung kriminalistisch geboten ist, sind die Rechtsgrundlagen in der StPO zu schaffen. Schon die erste Prüfung eines Sachverhaltes auf (auch künftige, sich entwickelnde) strafrechtliche Relevanz muß Aufgabe der Staatsanwaltschaft sein. Nur sie kann das rechtsstaatlich gebotene Legalitätsprinzip (im Gegensatz zum polizeirechtlichen Opportunitätsprinzip) sichern.

Vor diesem Hintergrund halte ich eine grundsätzliche Neuorientierung für erforderlich. Meine Gespräche mit dem SMI und dem SMJus werde ich fortsetzen. Gegenstand der Gespräche wird auch die Frage sein, ob bundesgesetzliche Regelungen für den Bereich der Vorfeldbeobachtungen erforderlich und zweckmäßig sind. Zuvor sollten auf untergesetzlicher Ebene Arbeitsanweisungen entwickelt werden, die sicherstellen, daß immer, bevor die Polizei eine personenbezogene Datenerhebung zum Endzweck strafrechtlicher Verfolgung durchführt, die Verfahrensherrschaft der Staatsanwaltschaft gesichert ist. Daneben müssen inhaltliche Datenverarbeitungsregeln statuiert werden, die denen in meinem 5. Tätigkeitsbericht genannten Forderungen genügen.

### 5.9.4 Videoüberwachung des öffentlichen Verkehrsraums

Die Zulässigkeit des polizeilichen Einsatzes der Videotechnik im öffentlichen Verkehrsraum habe ich in 5/5.9.8 am Beispiel des Leipziger Hauptbahnhofes erörtert. Ein Projekt der Polizeidirektion Dresden, in der Vorweihnachtszeit für die Dauer von zwei Wochen eine Videoüberwachung der gesamten Prager Straße durchzuführen, veranlaßte mich, die datenschutzrechtliche Zulässigkeit dieser besonderen Art polizeilicher Datenerhebung eingehend und grundsätzlich zu prüfen.

Beim erwähnten Dresdner Projekt war vorgesehen, den gesamten Bereich der Einkaufszone der Prager Straße zu erfassen. Damit stellte sich die Frage, ob die Erhebungsvoraussetzungen des § 38 Abs. 2 SächsPolG - anders als in Leipzig am Bahnhofsvorplatz - überhaupt erfüllt werden konnten. Schließlich knüpft die Vorschrift über ihre Verweisung auf § 19 Abs. 1 Nr. 3 SächsPolG an eine besondere objektbezogene Gefahrensituation an, die beim Leipziger Bahnhofsvorplatz konkret gegeben, für die gesamte Prager Straße aber wohl kaum zu begründen war. Diese rechtlichen Bedenken konnten im vorliegenden Fall durch die Darlegung der Polizeidirektion Dresden ausgeräumt werden, wonach die Kriminalitätsschwerpunkte in der Prager Straße durchaus zu lokalisieren sind, und zwar objektbezogen auf ein Kaufhaus und eine Imbißeinrichtung.

Das Dresdner Videoprojekt hat deutlich gemacht, auf welche generellen rechtlichen Schwierigkeiten Videoüberwachungen im öffentlichen Verkehrsraum stoßen:

Zunächst ist zu beachten, daß die von der Datenerhebungsnorm des § 38 Abs. 2 SächsPolG in Bezug genommene Vorschrift des § 19 Abs. 1 Nr. 3 SächsPolG nicht primär auf die Bekämpfung von Kriminalitätsschwerpunkten, sondern vielmehr auf die Erhaltung der Funktionsfähigkeit wichtiger Einrichtungen zielt.

Kann im Leipziger Fall wegen des dort noch begründbaren Objektbezuges der Gefahrensituation die Videoaufnahme auf die genannten Rechtsvorschriften gestützt werden, besteht kaum noch rechtlicher Begründungsspielraum, wenn es darum geht, Kriminalitätsschwerpunkte, die sich im *offenen Verkehrsraum* (auf Straßen und Plätzen) gebildet haben, mittels Videotechnik zu überwachen. In diesen Fällen ist ein Objektbezug (Funktionsfähigkeit von *Einrichtungen*) im Sinne des § 19 Abs. 1 Nr. 3 SächsPolG nicht mehr zu konstruieren; eine sonstige bereichsspezifische polizeirechtliche Erhebungsgrundlage ist nicht ersichtlich.

Sollten die Erfahrungen aus den Projekten Leipzig und Dresden belegen, daß die (präventive) Kriminalitätsbekämpfung mittels Videoeinsatzes entscheidend effektiviert werden kann, wird es unumgänglich sein, tragfähige Rechtsgrundlagen für die Überwachung des offenen Verkehrsraums zu schaffen. Als Lösung käme in Betracht, den Anwendungsbereich der Datenerhebungsnorm des § 38 Abs. 2 SächsPolG um eine Verweisung auf § 19 Abs. 1 Nr. 2 SächsPolG zu erweitern. Damit wäre der von den Videomaßnahmen Leipzig und Dresden ins Visier genommene Personenkreis, nämlich Personen, die Straftaten verabreden, vorbereiten oder verüben, erfaßt - und zwar, ohne daß das zusätzliche Tatbestandserfordernis der Objekt-

bezogenheit hinzutreten müßte. Die in Aussicht genommene Novellierung des Sächsischen Polizeigesetzes böte Gelegenheit, den Videoeinsatz zur Bekämpfung von Kriminaliätsschwerpunkten gesetzlich umfassend abzusichern. Bis zu einer - mit großer Sicherheit zu erwartenden - entsprechenden gesetzlichen Regelung halte ich es allerdings für vertretbar, den Probebetrieb zu gestatten. Diese Zeitspanne sollte genutzt werden, um eine verläßliche Evaluierung der durch den Einsatz der Videotechnik gesammelten Erfahrungen zur Kriminalitätsentwicklung durchzuführen.

Aus gegebenem Anlaß weise ich darauf hin, daß es sich beim Einsatz der Videotechnik rechtlich nicht nur um ein „bloßes Beobachten von Personen“ handelt, sondern um eine Alternative des § 38 Abs. 2 SächsPolG, mithin um „Bildaufnahmen“, an die dieselben strengen Voraussetzungen zu stellen sind wie an „Bildaufzeichnungen“. An dieser gesetzlichen Gleichstellung wird zugleich deutlich, daß nicht erst das Speichern, sondern bereits das Erheben ein perönlichkeitsrechtsrelevanter Vorgang beim Einsatz der Videotechnik ist.

Wie mir das SMI inzwischen mitteilen konnte, ist beabsichtigt, bei der anstehenden Novellierung des Sächsischen Polizeigesetzes eine tragfähige Rechtsgrundlage für die Videoüberwachung öffentlichen Verkehrsraums zu schaffen.

### 5.9.5 Datenschutzrechtliche Zuständigkeit bei der Videoüberwachung der Deutschen Bahn AG

Wie bereits im Bahnhof Dresden Neustadt im Probebetrieb praktiziert, wird die Deutsche Bahn AG in einigen sächsischen Bahnhöfen Videoüberwachungsanlagen nach dem sogenannten „3-S-Konzept“ installieren, die von der Deutschen Bahn AG, der sächsischen Polizei und dem Bundesgrenzschutz gemeinsam genutzt werden können.

Das Zusammenwirken dieser Stellen wirft die Frage nach der datenschutzrechtlichen Kontrollzuständigkeit auf. Insbesondere ist zu prüfen, ob die Zuständigkeit des Berliner Datenschutzbeauftragten als Aufsichtsbehörde gemäß § 38 BDSG für die Deutsche Bahn AG, die im Zusammenhang mit der Diskussion um die Bahn-Card angenommen worden sei, auch für die Videoüberwachung der Deutschen Bahn AG auf Bahnhöfen gilt. Nach meiner Auffassung, die ich im Arbeitskreis Sicherheit der Datenschutzbeauftragten des Bundes und der Länder zur Diskussion gestellt habe, nimmt die Deutsche Bahn AG bei der Videoüberwachung von Bahnhöfen eine öffentliche Aufgabe wahr, weil die ungehinderte Benutzung von Verkehrseinrichtungen zur Daseinsvorsorge zählt. Aus diesem Grunde ist auf die Videoüberwachung der Deutschen Bahn AG das Sächsische Datenschutzgesetz anzuwenden. Das Hausrecht der Bahnhofsbetreiber sehe ich durch Grundrechte - hier insbesondere die Freizügigkeit und das Recht auf informationelle Selbstbestimmung - begrenzt. Für Eingriffe in diese Grundrechte ist daher eine tragfähige Rechtsgrundlage erforderlich, die es für die Videoüberwachung auf Bahnhöfen bisher nicht gibt.

Im Gespräch mit der Deutschen Bahn AG und den beteiligten Sicherheitsbehörden werde ich eine einvernehmliche Lösung des Problems anstreben.

### 5.9.6 Videoüberwachung des Autobahnverkehrs durch die Polizei

In 5/5.9.9 habe ich empfohlen, die Videoüberwachung des Autobahnverkehrs in einer Dienstanweisung datenschutzgerecht zu regeln. Meine Empfehlungen hat das SMI in seiner Verwaltungsvorschrift zur Überwachung des Straßenverkehrs inzwischen umgesetzt. Hervorzuheben ist, daß die von mir kritisierten „Aufzeichnungsbücher", die zusammen mit den automatisierten Vorkommnisberichten die Gefahr der Doppelspeicherung bargen, nicht mehr fortgeführt werden dürfen.

## 5.10 Verfassungsschutz

**Landesamt für Verfassungsschutz**

Bei meinen im Berichtszeitraum durchgeführten Kontrollen im Landesamt für Verfassungsschutz habe ich wie in den Vorjahren ein ausgeprägtes Bewußtsein für datenschutzrechtliche Problemkreise festgestellt.

Die vereinzelt aufgetretenen Schwierigkeiten bei der Zusammenführung bislang manuell geführter, in Akten gespeicherter Informationsbestände im Zusammenhang mit der Einführung des amtsinternen Informationssystems ISIS (vgl. 5/5.10) traten nur noch vereinzelt auf. Ich habe mich aber davon überzeugen können, daß in dieser Umstellungsphase die aufgetretenen Probleme in ihrer Struktur durch das Datenschutzreferat des Amtes erkannt worden sind und durch geeignete Arbeitsanweisungen minimiert werden konnten, so daß ich bei meiner Kontrolltätigkeit keine Beanstandungen aussprechen mußte.

Wie bisher erhielt ich gemäß § 8 Abs. 2 SächsVSG durch das SMI und das LfV frühzeitig Gelegenheit, die datenschutzrechtliche Zulässigkeit neuer automatisierter Dateien vorab zu prüfen.
In einem Fall sah das technische Konzept des LfV vor, Texte einzuscannen und schließlich auf CD zu archivieren. Das grundsätzliche datenschutzrechtliche Problem liegt bei dieser Technikanwendung darin, daß die auf der CD gespeicherten recherchefähigen Personendaten nicht gemäß den individuell zu vergebenden Fristen gezielt gelöscht werden können. Ich habe daher empfohlen, bei künftigen Anwendungen prinzipiell magneto-optische Datenträger einzusetzen, die eine differenzierte Umsetzung der Löschungsfristen ermöglichen.
Im zugrundeliegenden Fall hatte das LfV allerdings zusätzliche Sicherungen durch Verwendungsbeschränkungen veranlaßt, so daß - auch wegen der geringen Eingriffstiefe der Datenverarbeitung - die Anwendung datenschutzrechtlicher Anforderungen in ausreichendem Maße genügte.

## 5.11 Landessystemkonzept / Landesnetz

### InfoHighway / kommunale Intranetze

Nach einer abschließenden Kostenabschätzung und der Erarbeitung eines Pflichtenheftes ist der „InfoHighway“ mittlerweile zur Ausschreibung gelangt. Datenschutzmaßnahmen werden in einem noch zu erstellenden Sicherheitskonzept festgeschrieben. Dieses Konzept geht von einem zweistufigen Aufbau aus, der sich bereits in der Ausschreibung wiederfindet. Neben einer Grundsicherung wird vom Auftragnehmer noch das Angebot verschiedener optionaler Sicherheitsdienste verlangt, auf die die Ressorts anwendungsspezifisch zurückgreifen können. Ich werde die Umsetzung begleiten und darauf achten, daß die guten Vorsätze auch in die Tat umgesetzt werden.

Neben dem von mir über mehrere Jahre begleiteten Vorhaben des InfoHighway in der Landesverwaltung wird auch in der Kommunalverwaltung der Ruf nach interkommunalen Netzen immer lauter. Die SAKD hat deshalb in Zusammenarbeit mit den Spitzenverbänden innerhalb einer Arbeitsgemeinschaft „Interkommunale Kommunikation“ vier Arbeitskreise gegründet, die sich zum einen mit der interkommunalen Kommunikation, zum anderen mit der Kommunikation Bürger - Kommune befassen. Ich begleite mit meinen Mitarbeitern aktiv deren Arbeit und begrüße diese Koordination und Bündelung der kommunalen Aktivitäten, da hier ansonsten - stärker noch als in der Landesverwaltung - die Gefahr der Zersplitterung und des (auch datenschutzrechtlichen) Wildwuchses besteht.

## 5.12 Ausländerwesen

### 5.12.1 Verwendung eines bundeseinheitlichen Formulars einer Verpflichtungserklärung gemäß § 84 AuslG

Angehörige bestimmter Staaten, die in die Bundesrepublik Deutschland einreisen wollen, haben im Visumverfahren zusammen mit dem Visumantrag der zuständigen Auslandsvertretung eine Verpflichtungserklärung gemäß § 84 AuslG vorzulegen, in der sich ein Dritter der Ausländerbehörde oder einer Auslandsvertretung gegenüber verpflichtet hat, die Kosten für den Lebensunterhalt eines Ausländers zu tragen. Auf Grund dieser Verpflichtung hat dieser „Einladende“ grundsätzlich sämtliche öffentlichen Mittel zu erstatten, die für den Lebensunterhalt des Ausländers einschließlich der Versorgung mit Wohnraum und der Versorgung im Krankheitsfalle und bei Pflegebedürftigkeit aufgewendet werden. Die Verpflichtungserklärung bedarf der Schriftform.

Die sächsischen Ausländerbehörden verwenden ein bundeseinheitliches Formular einer Verpflichtungserklärung nach § 84 AuslG. Die Verwendung dieses Formulars stößt bei mir überwiegend auf folgende datenschutzrechtliche Bedenken:

Der „Einladende“ hat das Original der Verpflichtungserklärung dem Ausländer zur Vorlage bei der zuständigen Auslandsvertretung zu übersenden; da er in der Verpflichtungserklärung zum Nachweis, daß er seiner Verpflichtung nachkommen

kann, u. a. die genaue Höhe seines Einkommens/Vermögens angeben soll, erfährt der Ausländer somit verfahrensbedingt die finanziellen Verhältnisse. Gleiches gilt für die zuständige Auslandsvertretung. Dies ist meines Erachtens nicht erforderlich, zumal nur die Ausländerbehörde die Bonitätsprüfung abschließend wahrnehmen kann. Auf die Angabe der finanziellen Verhältnisse in der Verpflichtungserklärung kann dann verzichtet werden. Ein Vermerk der Ausländerbehörde auf der Verpflichtungserklärung über die Bonität des „Einladenden", z. B. durch eine bloße Kennzeichnung mit „Ja" oder „Nein", würde genügen.

Ich teilte dem SMI mit, daß eine Reihe von Ländern auf die im Formular vorgesehene Form der Bonitätsprüfung aus datenschutzrechtlichen Gründen verzichtet. Zwischenzeitlich übersandte mir das SMI die vom BMI überarbeiteten Hinweise zur Verwendung des bundeseinheitlichen Formulars der Verpflichtungserklärung zur datenschutzrechtlichen Prüfung. Diese sehen nunmehr vor, daß die Ausländerbehörde eine Bonitätsprüfung vornimmt und lediglich das Ergebnis auf dem Formular vermerkt, wobei in der Regel die Abgabe einer Stellungnahme über die Glaubhaftmachung/den Nachweis der Bonität durch die Ausländerbehörde ausreiche und auf Detailangaben zu Wohn-, Einkommens-, und Vermögensverhältnisse im Regelfall verzichtet werden soll. Es handelt sich hierbei um einen Schritt in die richtige Richtung.

### 5.12.2 Übermittlung von Dokumenten zur Vorbereitung der Paßersatzbeschaffung bei ausreisepflichtigen Ausländern

Der Sächsiche Ausländerbeauftragte bat mich um Prüfung des nachfolgenden Sachverhalts:

Ein tunesischer Bürger, der sich in der Bundesrepublik Deutschland aufhält, vermutete einen datenschutzrechtlichen Verstoß, weil sein Militärausweis, der zu Beginn seines Asylverfahrens als sein einziges Identifikationspapier einbehalten wurde, an das tunesische Generalkonsulat in Berlin weitergeleitet wurde.

Meine Prüfung ergab, daß der tunesische Staatsbürger vollziehbar ausreisepflichtig war. Da er keinen Reisepaß besaß, waren geeignete Paßbeschaffungsmaßnahmen erforderlich. Sowohl eine freiwillige Ausreise des abgelehnten Asylbewerbers als auch dessen Abschiebung kann nur mit einem gültigen Heimreisedokument erfolgen. Nachdem der tunesische Staatsbürger seiner Mitwirkungspflicht bei der Paßbeschaffung gemäß § 15 Abs. 2 Nr. 6 AsylVfG nicht nachgekommen war, traf die Zentrale Ausländerbehörde im Regierungspräsidium Chemnitz die weiteren erforderlichen Maßnahmen zur Paßbeschaffung.

Gemäß § 43 b AsylVfG hat der BMI oder die von ihm bestimmte Stelle für die Beschaffung der Heimreisedokumente im Wege der Amtshilfe Sorge zu tragen. Durch Anordnung des BMI wurde der Bundesgrenzschutz als die dafür zuständige Stelle bestimmt. Die Zentrale Ausländerbehörde durfte daher aus datenschutzrechtlicher Sicht den Militärausweis, der ihr vom Bundesamt für die Anerkennung ausländischer Flüchtlinge nach Ablehnung des Asylantrags zugesandt worden war, als sein einziges Originalidentifikationspapier, das u. a. dem Nachweis seiner tunesischen Staatsangehörigkeit diente, an die Grenzschutzdirektion Koblenz als Grundlage

für die Paßbeschaffung weiterleiten. Die mit der Weiterleitung des Militärausweises verbundene Datenübermittlung ist gemäß §§ 13, 12 Abs. 1 bis 4 SächsDSG zulässig, zumal sie zur Paßbeschaffung erforderlich war.

Die Grenzschutzdirektion Koblenz, für deren datenschutzrechtliche Kontrolle der BfD zuständig ist, hat dann offensichtlich den Militärausweis an das tunesische Generalkonsulat in Berlin zur Ausstellung der für die Ausreise des tunesischen Staatsbürgers erforderlichen Heimreisedokumente gesandt. Auch diese Maßnahme ist aus datenschutzrechtlicher Sicht zulässig, zumal der Petent vollziehbar ausreisepflichtig war. Rechtsgrundlage einer mit der Übersendung des Militärausweises an das tunesische Generalkonsulat verbundenen Datenübermittlung ist § 17 BDSG.

Die spätere Heirat des tunesischen Staatsbürgers, die ggf. (bei Heirat einer deutschen Staatsangehörigen) einen Anspruch auf Erteilung einer Aufenthaltsgenehmigung begründen würde, hatte keinen Einfluß auf die Rechtmäßigkeit der Weitergabe des Militärausweises an die Grenzschutzdirektion Koblenz und von dieser an das tunesische Generalkonsulat, zumal die Heirat einige Zeit nach Abschluß der Maßnahme erfolgte. Vor seiner Heirat war er, wie oben ausgeführt, vollziehbar ausreisepflichtig, so daß die davor getroffenen Paßbeschaffungsmaßnahmen rechtmäßig waren.

Die Verwendung des Militärausweises im Rahmen der Paßbeschaffung hätte der tunesische Staatsbürger im *konkreten* Fall vermeiden können, wenn er seiner diesbezüglichen Mitwirkungspflicht nachgekommen wäre.

Die Ausländerbehörden haben sich korrekt verhalten.

### 5.12.3 Löschungsfristen von Ausschreibungen über ausgewiesene Ausländer im Schengener Informationssystem (SIS)

Der Datenschutzbeauftragte eines anderen Landes teilte mir folgende dort festgelegten Löschungsfristen von Ausschreibungen über ausgewiesene Ausländer im Schengener Informationssystem mit: Abschiebung nach § 49 AuslG und Ermessensausweisung nach §§ 45, 46 AuslG: Drei Jahre; Regel-Ausweisung nach § 47 Abs. 2 AuslG: Fünf Jahre; Ist-Ausweisung nach § 47 Abs. 1 AuslG: Acht Jahre.

Dies war für mich Anlaß, die sächsische Praxis festzustellen.

Das SMI teilte mit, daß die im Rahmen des Schengener Informationssystems zu bearbeitenden Ausweisungen und Abschiebungen von Ausländern nach §§ 45-47, 49 AuslG vom Landeskriminalamt regelmäßig nach *drei* Jahren gelöscht werden. Die Prüffrist nach Art. 112 Abs. 1 Satz 2 des Schengener Durchführungsübereinkommens ist somit grundsätzlich identisch mit der Löschungsfrist der Daten. Die Löschung unterbleibt lediglich in den Fällen, in denen von der zuständigen Ausländerbehörde eine Auschreibungsverlängerung beantragt wird. Die Dauer der Fristverlängerung richtet sich dabei nach den Umständen des Einzelfalls.

Die sächsische Verfahrensweise entspricht den Vorgaben des Art. 112 des Schengener Durchführungsabkommens.

## 5.13 Wahlrecht

### Bundestagswahl 1998 - Gewinnung von Wahlhelfern

Verschiedene Gemeinden wenden sich derzeit an sächsische Behörden mit der Bitte um namentliche Nennung von Bediensteten, die als Wahlvorstand oder als Wahlhelfer eingesetzt werden können.

§ 31 Abs. 1 SächsDSG läßt die Übermittlung von Beschäftigtendaten u. a. nur dann zu, soweit ein Gesetz dies vorsieht.

Während in § 8 Abs. 6 SächsWahlG und in § 10 Abs. 2 KomWG die Körperschaften und sonstigen juristischen Personen des öffentlichen Rechts *verpflichtet* werden, unter gewissen Voraussetzungen Beschäftigtendaten zwecks Bildung der Wahlvorstände auf Antrag der Bürgermeister zu übermitteln, fehlen solche Vorschriften im Bundeswahlrecht, so daß eine Datenübermittlung anläßlich der Bundestagswahl nur auf freiwilliger Basis erfolgen darf. Auf die Entschließung der 49. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 9./10. März 1995 in Bremen zum Datenschutz bei Wahlen, dort insbesondere die Nr. 3 (abgedruckt unter Nr. 16.2.14 des 3. Tätigkeitsberichts) weise ich hin.

## 5.14 Sonstiges

### 5.14.1 Stellungnahme zur Novellierung des Sächsischen Vermessungsgesetzes

Zu einem Referentenentwurf zum Gesetz über die Landesvermessung und das Liegenschaftskataster im Freistaat Sachsen, der Umstrukturierungen und Neuerungen, insbesondere die vollständige Übertragung der örtlichen Katastervermessungen auf Öffentlich bestellte Vermessungsingenieure (ÖbV) enthält, habe ich mich vor allem zu den vorgesehenen regelmäßigen Datenübermittlungen und automatisierten Abrufverfahren aus dem Liegenschaftskataster geäußert.

Als besonders problematisch erachte ich § 24 Abs. 6 des Entwurfs. Danach sollen Gerichte und Behörden (dazu zählen insbesondere auch die untereinander konkurrierenden ÖbV) ermächtigt werden, für den Betroffenen nachteilige Sachverhalte dem Landesvermessungsamt mitzuteilen, *„soweit hierdurch schutzwürdige Belange des betroffenen Öffentlich bestellten Vermessungsingenieurs nicht beeinträchtigt werden oder das öffentliche Interesse das Geheimhaltungsinteresse des Öffentlich bestellten Vermessungsingenieurs überwiegt.“*

Aus grundsätzlichen Erwägungen - Schutz vor Denunziation - habe ich gebeten, auf diese Bestimmung zu verzichten, zumal die erforderlichen Datenübermittlungen bereits durch das SächsDSG ausreichend legitimiert sind.

Des weiteren habe ich darauf hingewiesen, daß die in § 31 Nr. 3 vorgesehene Ermächtigungsgrundlage zur regelmäßigen Datenübermittlung und über automati-

sierte Abrufverfahren gemessen an § 8 Abs. 1 SächsDSG als formelle Ermächtigung nicht ausreicht.

Hierzu bedarf es eines formellen Gesetzes. Materielle Gesetze wie Rechtsverordnungen und Satzungen reichen dazu nicht aus.

Deshalb sollte im Gesetz selbst an geeigneter Stelle eine Bestimmung aufgenommen werden, die Anlaß, Zweck, Datenempfänger, Datenumfang und technisch-organisatorische Maßnahmen zur Gewährleistung des Datenschutzes ausreichend normenklar regelt.

Einen Teil meiner Vorschläge hat das SMI in seinen überarbeiteten Referentenentwurf aufgenommen. Die Ermächtigungsgrundlage zur regelmäßigen Datenübermittlung aus dem Liegenschaftskataster an Behörden und sonstige öffentliche Stellen bzw. zur Einrichtung automatisierter Abrufverfahren aus diesen ist in § 18 Abs. 9 nun normenklar geregelt. Das SMI ist nach § 31 Nr. 3 nur noch ermächtigt, durch Rechtsverordnung die Rahmenbedingungen zu regeln, wobei der Übermittlungszweck, die Datenempfänger, der Datenumfang und die zur Gewährleistung des Datenschutzes notwendigen technischen und organisatorischen Maßnahmen festzulegen sind.

### 5.14.2 Nutzung von Stasi-Unterlagen

Das SMF fragte mich, ob es zulässig sei, die zur Überprüfung auf MfS-Mitarbeit von Bediensteten erhaltenen Bescheide des Bundesbeauftragten für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR (BStU) auch für andere Zwecke zu nutzen.

Den Hintergrund bildete der Fall eines sächsischen Hochschulbediensteten, dessen Arbeitsverhältnis seit über einem Jahr aufgelöst war und der - wie sich erst jetzt anhand eines BStU-Berichts herausstellte - entgegen den Angaben bei seiner Einstellung früher inoffizieller Mitarbeiter der Stasi war. Dabei waren seine ruhegehaltsfähigen Vordienstzeiten neu festzulegen, was zur Folge hatte, daß die bislang überzahlten Ruhebezüge zurückgefordert werden mußten. Somit war zu klären, in welchem Umfang der Überprüfungsbescheid des BStU für eine zivilrechtliche Klage des früheren Dienstherrn auf Rückforderung zuviel gezahlter Ruhebezüge verwendet werden darf.

Ich vertrete hierzu folgende Auffassung: Nach § 20 Abs. 1 Nr. 9 StUG ist die Verwendung von Unterlagen für die Fragen der Versorgung von Stasi-Angehörigen zulässig. Die frühere Beschäftigungsbehörde hätte als zuständige Stelle im Sinne des § 19 Abs. 2 StUG auch nach Beendigung des Beschäftigungsverhältnisses die Möglichkeit, ein entsprechendes Ersuchen - und zwar auch ohne Einwilligung des Betroffenen - an den BStU zu richten, wenn dies zur Erfüllung ihrer Aufgaben erforderlich ist. Die rückwirkende Feststellung der Beschäftigungszeiten früherer Bediensteter gehört zu den Aufgaben des Dienstherrn.

Zu bedenken wäre lediglich, ob die beim Dienstherrn eingegangenen BStU-Berichte in ihrer detaillierten Ausgestaltung für die Feststellung der Beschäftigungszeiten herangezogen werden dürfen - wäre doch ein BStU-Bescheid, der auf ein nach § 20 Abs. 1 Nr. 9 StUG gestütztes Ersuchen ergeht, auf die *Rahmendaten* der MfS-Mitarbeit zu beschränken. Etwaige im BStU-Bescheid aufgeführte Einzelheiten zur MfS-Mitarbeit (z. B. Zahl der Berichte, Zeit des letzten Treffs) können aber im Streitfall zur Begründung zivilrechtlicher Rückzahlungsansprüche durchaus erforderlich sein, z. B. um den subjektiven Unrechtsgehalt einer falschen Erklärung bei der Einstellung zu belegen.

Gegen die Verwendung der Rahmendaten der MfS-Zugehörigkeit zur Festsetzung der Beschäftigungszeiten bestehen daher im Hinblick auf § 20 Abs. 1 Nr. 9 StUG keine datenschutzrechtlichen Bedenken.

# 6 Finanzen

## 6.1 Mitteilung des Gesamtschuldenstandes durch das Finanzamt an Drittschuldner

Wer beim Finanzamt Schulden hat, muß damit rechnen, daß seine eigenen Außenstände gepfändet und eingezogen werden.

Solche Pfändungs- und Einziehungsverfügungen an Drittschuldner offenbaren regelmäßig den aktuellen Gesamtbetrag der geschuldeten Steuern und Abgaben des Schuldners. Ein Petent beklagte sich, daß seine Mieter und Geschäftspartner, die ihm Geld schuldeten und nun an das Finanzamt zahlen mußten, damit Kenntnis über die Höhe seiner Verpflichtungen gegenüber dem Finanzamt erlangten.

Über Jahrzehnte hatte der Bundesfinanzhof - als oberstes Gericht in Steuersachen - in seiner Rechtsprechung verlangt, daß die beizutreibenden Beträge nach Grund und Höhe und bei Steuern, die für bestimmte Zeiträume erhoben werden, auch nach Zeiträumen anzugeben waren. Durch das Steuerbereinigungsgesetz 1986 wurde zwar § 309 Abs. 2 AO dahingehend geändert, daß nun in der Pfändungsverfügung an den Drittschuldner auf die Angabe von Steuerarten und Zeiträumen verzichtet wird. Jedoch ist nach wie vor der beizutreibende Geldbetrag in einer Summe zu bezeichnen. Somit ist die Angabe des Gesamtschuldenstandes in der Pfändungsverfügung an den Drittschuldner gesetzlich vorgeschrieben.

Dies ist aus datenschutzrechtlicher Sicht alles andere als eine befriedigende Lösung. Eine weitergehende datenschutzgerechtere Anpassung durch den Bundesgesetzgeber ist allerdings zur Zeit nicht zu erwarten.

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

In 5/6.6 habe ich bereits auf die Unzulässigkeit von Veröffentlichungen der Steuerberaterkammer des Freistaates Sachsen über Verurteilungen und strafbewehrte Unterlassungserklärungen in ihrer Mitteilungsschrift hingewiesen.

Die sächsische Steuerberaterkammer hat daraufhin zunächst auf entsprechende Veröffentlichungen verzichtet, allerdings die Veröffentlichungspraxis unter Berufung auf ein Urteil des LG Kiel sowie auf einen mehrheitlichen Beschluß der Berufsreferenten des Bundes und der Länder im Sommer 1997 wieder aufgenommen. Ein Verstoß gegen § 15 Abs. 1 Nr. 1 SächsDSG liege angeblich nicht vor. Die von der sächsischen Steuerberaterkammer erklärte Bereitschaft, sich bei zukünftigen Veröffentlichungen eines Wettbewerbsstörers nur noch auf dessen vollständigen Namen sowie den Ort des Sitzes seiner Firma zu beschränken und auf die Angabe der vollständigen Anschrift zu verzichten, reicht insofern nicht aus, als es in Zeiten elektronischer Telefonbücher ein leichtes ist, die übrigen Angaben zu erhalten.

Mit den erneuten Veröffentlichungen der sächsischen Steuerberaterkammer in ihren Kammermitteilungen erhält eine unbestimmte Zahl unbeteiligter Dritter - und keinesfalls nur Kammermitglieder - Kenntnis von einer gegen den Betroffenen ergriffenen Maßnahme. Demgegenüber bleibt es der Kammer und ihren Mitgliedern sozusagen als „milderes Mittel“ weiterhin unbenommen, in Einzelfällen bei konkreten Anhaltspunkten für eine unzulässige Berufsausübung Ermittlungen durchzuführen und entsprechende Maßnahmen einzuleiten. Dies reicht offensichtlich aus, mißbräuchliche Berufsausübung im Steuerhilfebereich zu verhindern, denn nach meiner Kenntnis nehmen nicht alle Steuerberaterkammern solche Veröffentlichungen vor.

Die von der Steuerberaterkammer des Freistaates Sachsen vertretene Auffassung steht mit geltendem Datenschutzrecht nicht in Einklang. Nach § 4 Abs. 1 SächsDSG ist die Verarbeitung personenbezogener Daten u. a. nur dann zulässig, wenn eine Rechtsvorschrift dies ausdrücklich erlaubt. Eine die Praxis der Kammer rechtfertigende Übermittlungsvorschrift gibt es jedoch nicht.

§ 76 StBerG regelt lediglich die gesetzliche Aufgabenzuweisung, nicht jedoch eine datenschutzrechtliche Befugnis. Jeder Eingriff in das verfassungsrechtlich garantierte Recht auf informationelle Selbstbestimmung erfordert aber eine normenklare Rechtsgrundlage (BVerfGE 65, 44).

Auch § 23 UWG scheidet als generelle Bekanntmachungsnorm für die fraglichen Fälle aus. Sämtliche Fallgruppen dieser Vorschrift setzen voraus, daß das *Gericht* die Bekanntmachung des Urteils, in dem das wettbewerbswidrige Verhalten sanktioniert wird, ausdrücklich anordnet. Wegen des Richtervorbehalts läßt sich diese Regelung auch nicht auf sonstige Fälle analog anwenden, in denen das Gericht eine entsprechende Anordnung nicht verfügt oder es gar kein gerichtliches Verfahren gegeben hat.

Auch der von der Steuerberaterkammer angeführte Verweis auf § 15 Abs. 1 Nr. 1 SächsDSG greift letztlich nicht. Denn die Voraussetzungen, unter denen eine öffentliche Stelle personenbezogene Daten an Personen und Stellen außerhalb des öffentlichen Bereichs übermitteln darf, sind ersichtlich nicht erfüllt:

Die Übermittlung personenbezogener Daten an Personen und Stellen außerhalb des öffentlichen Bereichs läßt § 15 Abs. 1 SächsDSG u. a. zu, soweit dies zur Aufgabenerfüllung der übermittelnden Stelle erforderlich ist. Erforderlich ist eine Übermittlung aber nur dann, wenn ohne sie eine Aufgabe nicht oder nur mangelhaft erfüllt werden kann. Dabei ist wegen des bei Eingriffen in das sich aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 2 GG, Art. 33 SächsVerf ergebende Recht auf informationelle Selbstbestimmung zu beachtenden Grundsatzes der Verhältnismäßigkeit ein strenger Maßstab anzulegen.

Die von der Kammer geübte Veröffentlichungspraxis läßt sich auch nicht auf die angeführte Entscheidung des LG Kiel (LG Kiel, Beschluß vom 11. Januar 1995, AZ 60 299/94) stützen, da sich diese nicht mit der sächsischen Rechtslage befaßt und für uns nicht bindend ist.

Vor allem aber geht der Hinweis auf die Erörterung der Berufsreferenten des Bundes und der Länder an der Problematik vorbei, weil auch ein mehrheitlicher Beschluß dieser Runde eine fehlende gesetzliche Grundlage nicht zu ersetzen vermag.

Die sächsische Steuerberaterkammer hat ihre Veröffentlichungspraxis (vorerst) wegen fehlender Rechtsgrundlage wieder eingestellt und gebeten, mich für die Schaffung einer solchen einzusetzen. Das SMF habe ich entsprechend unterrichtet.

## 6.3 Werbungskosten für Auslandsstudienreisen - Aufforderung des Finanzamts an den Steuerpflichtigen, Namen und Anschriften der Mitreisenden mitzuteilen

In 5/6.2 erläuterte ich, warum ich die Aufforderung der Finanzämter an den Steuerpflichtigen oder ggf. an den Reiseveranstalter, die Namen und Anschriften der übrigen Reiseteilnehmer zur Anerkennung der Reisekosten für Auslandsstudienreisen als Werbungskosten mitzuteilen, datenschutzrechtlich für bedenklich halte.
Das SMF hält entgegen meiner Rechtsauffassung die Ermittlung von Namen und Anschrift der übrigen Reiseteilnehmer beim Steuerpflichtigen oder ggf. beim Reiseveranstalter als Prüfungsgrundlage auch in Zukunft für erforderlich und für zulässig.

Eine Änderung der von mir kritisierten Verfahrensweise bei der Prüfung der Voraussetzungen für eine Anerkennung von Auslandsstudienreisen als Betriebsausgaben/ Werbungskosten ist wünschenswert. Ein Betroffener könnte dies im Klagewege erzwingen.

## 6.4 Datenschutz bei Außenprüfungen der Finanzbehörden in Arztpraxen

Bei der Prüfung von Arztpraxen verlangen die Finanzämter in bestimmten Fällen u. a. die Patientennamen, die nach meinem Dafürhalten eindeutig dem Auskunftsverweigerungsrecht der Ärzte gemäß § 102 Abs. 1 Nr. 3c AO unterliegen.

Meine Auffassung zu § 102 Abs. 1 Nr. 3c AO stützt sich auf die Rechtsprechung zu § 53 Abs. 1 Nr. 3 StPO (Zeugnisverweigerungsrecht der Ärzte), der § 102 Abs. 1 Nr. 3c AO entspricht, wonach sowohl Name und Anschrift als auch die Tatsache der Behandlung eines Patienten unter das Zeugnisverweigerungsrecht des Arztes fallen.

Die obersten Finanzbehörden des Bundes und der Länder vertreten hingegen die Auffassung, daß das Auskunftsverweigerungsrecht der Ärzte im Besteuerungsverfahren die Patientennamen nicht mit umfasse. Sie haben dies mit der Gesetzessystematik des § 102 AO begründet. Da in § 102 Abs. 1 Nr. 2 AO (Auskunftsverweigerungsrecht der Abgeordneten) im Gegensatz zu § 102 Abs. 1 Nr. 3c AO ausdrücklich erwähnt wird, daß auch die Auskunft „über die Personen“ verweigert werden könne, würde sich das Auskunfsverweigerungsrecht der Ärzte wegen Fehlens der Worte „über die Personen“ nicht auf Namen und Anschriften ihrer Patienten erstrecken.

Ich habe dem SMF mitgeteilt, daß die Auffassung der obersten Finanzbehörden des Bundes und der Länder zu § 102 Abs. 1 Nr. 3c AO unter Verweis auf die „Gesetzessystematik“ des § 102 AO, die letztlich mit der des § 53 StPO identisch ist, nicht haltbar sei.

Gleichwohl hält das SMF nach wie vor an der Auffassung fest, daß der Patientenname nicht dem Auskunftsverweigerungsrecht der Ärzte gegenüber den Finanzbehörden unterliegt. Das Problem wird weiter bundesweit erörtert. Die Sächsische Landesärztekammer habe ich informiert.

## 6.5 Führen von Fahrtenbüchern durch Ärzte für steuerliche Zwecke

Die Problematik, die ich unter Punkt 6.4 (Datenschutz bei Außenprüfungen der Finanzbehörden in Arztpraxen) aufzeigte, zieht sich wie ein roter Faden durch die Verwaltungspraxis der Finanzbehörden. Diese fordern nicht nur die Angabe des Patientennamens im Rahmen von Außenprüfungen, sondern auch bei der Führung von Fahrtenbüchern durch Ärzte für steuerliche Zwecke.

Pressemeldungen und einer Petition entnahm ich, daß Ärzte ab dem 1. Januar 1998 in ihre Fahrtenbücher neben Reisezweck, Reiseziel, Reiseroute, Datum und Kilometerstand ohne Ausnahme auch den Patientennamen eintragen müssen, um eine pauschalierte Besteuerung des privaten Nutzungsanteils des zum Betriebsvermögen gehörenden Fahrzeugs zu vermeiden. Allerdings ist diese Anforderung einer Rechtsvorschrift nicht zu entnehmen. Dem SMF teilte ich meine datenschutzrechtlichen Bedenken mit:

Die Forderung der Finanzbehörden läßt die ärztliche Schweigepflicht, deren Verletzung mit Strafe bedroht ist, unberücksichtigt und ist daher datenschutzrechtlich nicht haltbar.

Die ärztliche Schweigepflicht wird durch § 102 AO nicht eingeschränkt. Der Patientenname und die Tatsache der Behandlung unterliegen in der gesamten deutschen Rechtsordnung der Schweigepflicht, es sei denn, diese Pflicht wird durch eine Rechtsvorschrift (und nicht etwa durch eine Übereinkunft der zuständigen Referenten o. ä.) ausdrücklich modifziert oder gar aufgehoben. Diese Grundsätze gelten auch im Besteuerungsverfahren.

Ich vertrete die Auffassung, daß einem Steuerpflichtigen, der nicht nur ein Auskunftsverweigerungsrecht besitzt, sondern einer beruflichen Auskunftsverweigerungspflicht unterliegt, aus dieser Pflicht heraus keine Nachteile entstehen dürfen. Daher darf ein Arzt, der wegen der von ihm zu beachtenden ärztlichen Schweigepflicht nicht bereit ist, den Patientennamen in das Fahrtenbuch einzutragen, nicht einer für ihn nachteiligen Pauschalbesteuerung unterworfen werden. Dies würde nämlich zu einer Ungleichbehandlung gegenüber solchen Steuerpflichtigen führen, die einer solchen Auskunftsverweigerungspflicht nicht unterliegen.

Weiterhin würde der Arzt ggf. mit der Preisgabe des Patientennamens ein fremdes Geheimnis i. S. d. § 203 StGB offenbaren, zumal dadurch bekannt würde, wer sich in ärztlicher Behandlung befindet bzw. befand. Insbesondere läßt der Kontakt zu einem Facharzt (z. B. Kardiologe, Nervenarzt, Frauenarzt, Urologe, usw.) Rückschlüsse auf die Art der Erkrankung zu. § 102 AO enthält ebensowenig wie § 53 StPO einen Rechtfertigungsgrund für den Bruch der Schweigepflicht nach § 203 StGB, so daß sich ein Arzt, der im Besteuerungsverfahren den Patientennamen angibt, der Gefahr eines strafrechtlichen Ermittlungsverfahrens aussetzt.

Die Finanzbehörden dürfen folglich m. E. auch in Zukunft von den Ärzten nicht die Angabe des Patientennamens im Fahrtenbuch für steuerliche Zwecke verlangen. Das Interesse des durch die ärztliche Schweigepflicht geschützten Personenkreises überwiegt dabei dem Interesse der Finanzbehörden an einer lückenlosen Ermittlung des steuerrelevanten Sachverhalts. Wäre etwas anderes gewollt, hätte der Gesetzgeber Regelungen schaffen müssen, welche Berufsgeheimnisträger im Besteuerungsverfahren von von einer gesetzlichen Schweigepflicht entbinden.

Auf eine Zustimmung des Patienten kann der Arzt nicht verwiesen werden, da bereits bei der Verweigerung dieser - natürlich freiwilligen - Zustimmung durch einen oder wenige Patienten das Fahrtenbuch genaugenommen insgesamt unrichtig würde.

Der Grundsatz der Verhältnismäßigkeit läßt im übrigen einen Selbstbeleg des Arztes als ausreichend zu. Mir ist kein Fall bekannt, daß etwa die Steuerbehörde stichprobenweise Patienten befragt hätte. Ferner hat die Finanzverwaltung bislang nicht vorgetragen, daß die Ärzteschaft bei der Absetzung von Werbungskosten/Betriebsausgaben auf dem Gebiet der Pkw-Kosten erheblich manipulieren würde.

Richtet sich ein steuerstrafrechtliches Ermittlungsverfahren gegen den Arzt, können Patientenunterlagen eingesehen und dann (aber erst dann) können dort die nötigen Eintragungen über Besuchs-Fahrten verifiziert, mit den Abrechnungen verglichen und eventuell durch Zeugnis des Patienten hinterfragt werden. Im Normalfall muß die namenlose Angabe des Arztes genügen.

Das SMF teilte mir mit, daß die Finanzbehörden des Freistaates Sachsen schon bisher nicht auf die Angabe des Patientennamens in Fahrtenbüchern verzichten durften. Lediglich in einzelnen Ländern wurde in Mitteilungen der Finanzverwaltung die Auffassung vertreten, daß Ärzte, die ständig Hausbesuche machen, den Anforderungen an die ordnungsgemäße Führung des Fahrtenbuchs genügen, wenn für die Angabe des aufgesuchten Geschäftspartners lediglich „Patientenbesuch“ eingetragen wird. Im Rahmen einer bundesweiten Abstimmung wurde für diese Länder zugelassen, diese Praxis noch bis zum 31.12.1997 zu tolerieren. Im Freistaat Sachsen hatte es eine vergleichbare Mitteilung der Finanzverwaltung nicht gegeben. Das SMF besteht weiterhin auf Angabe des Patientennamens in den Fahrtenbüchern der Ärzte.

Das ist wegen fehlender klarer Rechtsgrundlage rechtswidrig; die abgestimmte Meinung der zuständigen Referenten, Erlasse oder Verwaltungsvorschriften ersetzen nicht die verfassungsrechtlich gebotene Rechtsnorm.
Das SMF, das dem Rechtsstaat verpflichtet ist und mit uns ernsthaft nach einer Lösung sucht, fühlt sich jedoch an die gemeinsame Haltung des Bundes und der Länder gebunden.

Die Problematik bedarf weiterhin bundesweiter Erörterung.

## 6.6 Datenverarbeitungsverfahren zur Durchführung der Prüfung von Steuerberatern

Das SMF hat die nach dem StBerG und der DVStB durchzuführende Prüfung und Zulassung von Steuerberatern mit einem DV-Verfahren wesentlich vereinfacht.

Gegen die Antragsformulare für die Feststellung der Zulassungsvoraussetzungen (*Zulassung zur Eignungsprüfung, Bestellung/Wiederbestellung als Steuerberater, verbindliche Auskunft nach § 7 DVStB und Befreiung von der Steuerberaterprüfung*) habe ich keine Einwände erhoben. Die Sicherheitsvorkehrungen (verschlüsselt per Mail) für das DV-Verfahren einschließlich Datenaustausch zwischen dem SMF und der OFD Chemnitz sind ausreichend.
Ich habe angeregt, die nach § 31 DVStB festgelegten Aufbewahrungsfristen der Aufsichtsarbeiten für bestandene (zwei Jahre) und nicht bestandene Prüfungen (zehn Jahre) sowie das Verfahren über den Datenaustausch zwischen der bestellenden Behörde und der Berufskammer (als registerführende Stelle) und die erforderlichen Eintragungen in das Berufsregister (§§ 39 und 46 DVStB) im gemäß § 10 SächsDSG zu führenden Dateien- und Geräteverzeichnis zu berücksichtigen.
Das DV-Verfahren wird bereits angewendet.

# 7 Kultus

## 7.1 Schülerbefragung an einem sächsischen Gymnasium

Im Frühjahr 1997 berichteten mehrere Zeitungen über einen geplanten „Lehrer-TÜV“ an einem Gymnasium. Die Schüler sollten auf Initiative des Elternrats ihre Schüler-Lehrer-Beziehung sowie die allgemeine Situation an der Schule bewerten. Ich habe den Fragebogen angefordert und mich erkundigt, wie die Befragung durchgeführt werden soll. Solche Befragungen sind datenschutzrechtlich problematisch, weil sie im Schulgesetz nicht vorgesehen sind und deshalb nur auf freiwilliger Basis von Schülern *und* Lehrern durchgeführt werden dürfen.

Für die Befragung waren zwei Fragebogen vorgesehen, der erste zur „Evaluation der Schule“, der zweite zur „Evaluation der Schüler-Lehrer-Beziehung“, wobei jeder Schüler jeden ihn unterrichtenden Lehrer einzeln bewerten sollte. Gegen Form und Inhalt beider Fragebogen bestanden keine datenschutzrechtlichen Bedenken, weder gegen die Fragen im einzelnen noch gegen die Art ihrer Beantwortung, die anhand einer Bewertungsskala erfolgen sollte.

Das Verfahren zur *Evaluation der Schule* war datenschutzrechtlich unbedenklich. Die Fragebogen sollten im Eingangsbereich der Schule ausgelegt werden, damit jeder Schüler, der sich beteiligen will, einen Fragebogen mit nach Hause nehmen und dort ausfüllen kann. Für die Rückgabe war ein zentraler Kasten vorgesehen. Damit war die Anonymität gewährleistet. Da bei einer anonymen Befragung zur Beurteilung einer öffentlichen Einrichtung keine personenbezogenen Daten verarbeitet werden, fällt sie auch nicht in den Anwendungsbereich des Sächsischen Datenschutzgesetzes. Insoweit erübrigt sich auch eine datenschutzrechtliche Bewertung der Freiwilligkeit.

Das Verfahren zur *Evaluation der Schüler-Lehrer-Beziehung* dagegen läßt sich in Bezug auf die Lehrer weder anonym noch freiwillig durchführen, denn die Tatsache, ob sich ein Lehrer bewerten läßt oder nicht, ist bereits ein personenbezogenes Datum, dessen Bekanntwerden sich in einer Schule nicht vermeiden läßt. Das macht zugleich die Freiwilligkeit fragwürdig, denn ein Lehrer, der sich einer solchen Befragung entzieht, ist einem negatives Werturteil ausgesetzt und sieht sich so einem faktischen Teilnahmezwang gegenüber. Auch den Wert und damit die Erforderlichkeit der Befragung habe ich in Frage gestellt, weil sie durch gruppendynamische Prozesse beeinträchtigt wird, die - gerade bei Schülern - zu wissenschaftlich unsicheren Evaluationen führen. Und insbesondere: Welche konkreten Maßnahmen will man mit derart unsicherem Datenmaterial begründen? Von diesem Teil der Befragung ist dann abgesehen worden.

## 7.2 Datenschutz bei einem Schulprojekt zur präventiven und integrativen Erziehungshilfe

Die Beratungsstelle einer Schule für Erziehungshilfe hatte in Zusammenarbeit mit dem Schulträger, den Schulaufsichtsbehörden, dem Jugendamt, einer Universität und einer Grundschule ein Projekt zur präventiven und integrativen Erziehungshilfe mit folgenden Zielen konzipiert:

- individuelle Förderung von Schülern im schulischen und außerschulischen Bereich durch Unterstützung und Beratung der Schüler sowie der Sorgeberechtigten,

- Leistung von Erziehungshilfe bei der Integration von Schülern mit einem förmlich festgestellten sonderpädagogischen Förderbedarf (integrative Erziehungshilfe),

- Leistung von Erziehungshilfe für verhaltensauffällige Schüler ohne förmlich festgestellten Förderungsbedarf, um den Verhaltensstörungen entgegenzuwirken und zu verhindern, daß sie an einer Schule für Erziehungshilfe unterrichtet werden müssen (präventive Erziehungshilfe),

- Entwicklung theoretischer Grundlagen für die praktische Arbeit in Grund- und Förderschulen für Erziehungshilfe und deren Beratungsstellen.

Das Projekt wurde „Sonderaufgabe“ einer Beratungsstelle an einer Förderschule für Erziehungshilfe und sollte von einem Team aus Grund- und Förderschullehrern, einem Sozialarbeiter des Jugendamtes und einem Universitätsmitarbeiter durchgeführt werden.

Ich bin um eine datenschutzrechtliche Bewertung des Projekts gebeten worden.

Diese erwies sich insofern als schwierig, weil hier an der „Schnittstelle Kind“ zwei völlig verschiedene gesetzliche Aufgaben ineinandergreifen. Soweit die Projektarbeit den Schulbereich betrifft, handelt es sich um eine Aufgabe nach dem Sächsischen Schulgesetz, soweit sie darüber hinausgeht, handelt es sich um eine Aufgabe der Kinder- und Jugendhilfe (§ 2 Abs. 2 Nr. 1, 2 und 4 SGB VIII). Bei dieser Konstellation ist es nicht möglich, die im Rahmen des Projekts anfallenden und zu verarbeiteten Daten ausschließlich dem Geltungsbereich des Schulgesetzes oder des Sozialgesetzbuchs zuzuordnen. Von einer solchen Zuordnung hängt jedoch ab, ob es sich um Sozialdaten oder sonstige personenbezogene Daten handelt und damit, welche Datenverarbeitungsvorschriften Anwendung finden (SGB VIII/ SGB X oder das SächsDSG).

Da die Mitarbeiter öffentlicher Stellen keine andere als ihre gesetzliche Aufgabe wahrnehmen dürfen (die Mitarbeiter des Jugendamtes z. B. keine schulischen Aufgaben, die Lehrer keine Aufgaben aus der Kinder- und Jugendhilfe), folgt daraus für die Projektarbeit, daß ein und dasselbe Datum in der Hand von Sozialarbeitern als Sozialdatum, in der Hand von Lehrern oder Universitätsmitarbeitern als sonstiges personenbezogenes Datum verarbeitet wird. Damit hat jeder Projektmitarbeiter die Datenschutzbestimmungen zu beachten, die für seine Aufgabe gelten. Die daraus resultierenden Schwierigkeiten sind theoretischer Natur und können in der Praxis vernachlässigt werden, wenn eine umfassende Aufklärung der Betroffenen erfolgt und eine umfassende, informierte und wirklich freiwillige Einwilligung vorliegt.

Zu klären war auch, ob die Projektmitarbeiter der gesetzlichen Schweigepflicht nach § 203 Abs. 1 Nr. 4 StGB unterliegen (Erziehungs- und Jugendberater in einer Beratungsstelle, die von einer Körperschaft des öffentlichen Rechts anerkannt ist). Das

SMK hat das bejaht. Diese Auffassung ist nicht zweifelsfrei, weil dem Gesetzeswortlaut nach die bei den Förderschulen eingerichteten Beratungsstellen keine von einer Körperschaft des öffentlichen Rechts *anerkannten* Beratungsstellen sind. Da sie aber Teil einer Körperschaft des öffentlichen Rechts sind, sprechen gute Argumente dafür, sie wie *anerkannte* Beratungsstellen zu behandeln.

Als Konsequenz aus dieser Schweigepflicht ergibt sich für die Projektmitarbeiter, daß sie ohne Offenbarungsbefugnis die ihnen anvertrauten Daten nicht weitergeben dürfen - auch nicht untereinander. Bei der praktischen Projektarbeit vertrauen die Betroffenen nicht allen Mitarbeitern ihre sensiblen, sozialen und gesundheitlichen Daten an; solche Informationen müssen aber im Rahmen der Teamarbeit erörtert werden können. Folglich haben die Sorgeberechtigten die Mitarbeiter des Teams für ihre gemeinsame Arbeit von der Schweigepflicht zu entbinden. Für den Sozialarbeiter kommt als besondere Schwierigkeit hinzu, daß er möglicherweise aus seiner Hauptaufgabe Vorkenntnisse über einen Schüler und sein persönliches Umfeld hat oder im Rahmen einer parallelen bzw. begleitenden Hilfe in der Familie weitergehende Kenntnisse erlangt. Diese unterliegen ebenfalls der Schweigepflicht, sind aber nicht unbedingt von der Schweigepflichtentbindung der Sorgeberechtigten umfaßt, z. B. dann, wenn andere Familienmitglieder dem Sozialarbeiter Persönliches anvertraut haben. Insoweit liegt es in der schwierigen Verantwortung des Sozialarbeiters, hier sauber zu trennen. Ggf. hat er sich von weiteren Personen von der Schweigepflicht entbinden zu lassen.

In der Verfahrenskonzeption war vorgesehen, daß verhaltensauffällige Schüler den Projektmitarbeitern von der Grundschule gemeldet werden. Dies ist ohne Einwilligung der Betroffenen unzulässig, weil ihnen die Teilnahme am Projekt freisteht und nicht abzusehen ist, ob sie sich beteiligen werden. Deshalb verbietet sich eine Meldung hinter ihrem Rücken.

Ausgehend von vorstehenden Überlegungen habe ich folgende Anforderungen an das Projekt formuliert und Vorschläge für die dabei zu verwendenden Formblätter erarbeitet:

1. Ohne Einwilligung der Sorgeberechtigten dürfen von der Schule keine Schüler für das Projekt gemeldet werden. Die Sorgeberechtigten sind vorab über die beabsichtigte Meldung, den Zweck des Projekts sowie die Freiwilligkeit der Teilnahme schriftlich zu informieren und um Einwilligung zu bitten. Als Alternative kommt die Meldung durch die Sorgeberechtigten in Betracht.

2. Aufgrund der Meldung informiert der verantwortliche Projektmitarbeiter die Sorgeberechtigten ausführlich über das Projekt, holt deren Einwilligung für die Teilnahme des Schülers in der in den §§ 4 und 11 SächsDSG vorgeschriebenen Form sowie eine schriftliche Entbindung der Projektmitarbeiter von ihrer Schweigepflicht für Zwecke der Teamarbeit und der notwendigen Zusammenarbeit mit der Schule ein.

3. Sobald es erforderlich ist, weitere Personen oder Stellen hinzuzuziehen (z. B. Einholung fachärztlicher Gutachten), werden die Sorgeberechtigten darüber informiert und erneut um Einwilligung und Schweigepflichtentbindung gebeten. Ist die hinzuzuziehende Person (z. B. Berufspsychologe, Facharzt) ihrerseits schweigepflichtig, so muß auch sie von der Schweigepflicht entbunden werden, damit sie dem Projektteam persönliche oder sachliche Verhältnisse von Betroffenen offenbaren darf. Diese Schweigepflichtentbindung darf von dem verantwortlichen Mitarbeiter aus dem Projektteam eingeholt und der schweigepflichtigen Person vorgelegt werden.

4. Alle Projektmitarbeiter sind über die Bedeutung der Schweigepflicht zu belehren.

Wie mir das SMK mitgeteilt hat, sind meine Vorschläge umgesetzt worden.

## 7.3 Formblätter für das Aufnahmeverfahren an Förderschulen

In 5/7.1 hatte ich darüber berichtet, daß mich das SMK an der Erarbeitung eines Vordrucksatzes beteiligt hat, der im Rahmen des Aufnahmeverfahrens zum Besuch von Förderschulen verwendet werden soll. Die Aufgabe ist abgeschlossen. Die Formblätter sind mit der „Verwaltungsvorschrift des Sächsischen Staatsministeriums für Kultus über die im Rahmen des Aufnahmeverfahrens an Förderschulen gemäß § 12 Abs. 8 Verordnung des Sächsischen Staatsministeriums für Kultus über Förderschulen im Freistaat Sachsen zu verwendenden Formblätter“ vom 26. August 1997 (Amtsblatt des SMK Nr. 12/1997) verbindlich geworden. Ein Großteil meiner Vorschläge ist berücksichtigt worden. Nunmehr ersetzen sechs Vordrucke die bis dahin verwendete 18seitige „Pädagogisch-psychologische-medizinische Dokumentation“.

## 7.4 Heimatkunde- und Sachunterricht in der Grundschule

In einer Grundschulklasse stellte die Klassenlehrerin Hausaufgaben, in deren Rahmen die Kinder Angaben u. a. über das Einkommen der Eltern, Art und Grundriß der Wohnung und den Besitzstand der Eltern machen sollten.

Der Lehrplan für die Grundschule sieht in der Heimatkunde und im Sachunterricht vor, den Kindern Hilfe bei der Erschließung ihrer Lebenumwelt zu geben. Aus diesem Grunde soll in der Klasse 1, Lernbereich 1, das Leben in der Familie vorgestellt werden. In der Klasse 2 sind Arbeit und Beruf der Eltern Gegenstand des Unterrichts, in der Klasse 3 u. a. Möglichkeiten der Hilfe in nicht intakten Familien.

Bereits in der Vergangenheit hatte ich im Zusammenhang mit der Erstellung von Familienstammbäumen anerkannt, daß die Vorgaben des Lehrplans ein wesentlicher Bestandteil des wichtigen Unterrichtsziels sind, das Kind mit seiner Umwelt vertraut zu machen (3/7.1.4). Zugleich habe ich darauf hingewiesen, daß ein Spannungsverhältnis zu den ebenfalls berechtigten Anliegen des Rechts auf informationelle Selbstbestimmung und der Privatsphäre von Eltern und Kindern besteht. Das SMK hatte daraufhin in einer Verfügung die Oberschulämter und staatlichen Schulämter auf

datenschutzrechtliche Probleme aufmerksam gemacht, die über die Erstellung von Familienstammbäumen hinaus auch in anderen Bereichen der Heimatkunde und des Sachkundeunterrichts bestehen.

Die Forderung an die Kinder, wie im hier vorliegenden Fall, die Privatsphäre der Familie in weiten Bereichen offenzulegen, stellt keine angemessene Lösung dieses Spannungsverhältnisses dar. Auch aus pädagogischer Sicht ist zu fragen, ob ein am sozialen Status orientiertes Konkurrenzdenken gefördert wird, was nicht Zweck des Unterrichts sein kann.

Die Belange der Privatsphäre müssen in den Lehrplänen ausreichend Berücksichtigung finden. Das SMK teilte mir mit, daß die Evaluation der Lehrpläne im Grundschulbereich noch nicht abgeschlossen sei. Mit einer kurzfristigen Überarbeitung einzelner Lehrpläne sei nicht zu rechnen. Das Staatsministerium beabsichtigt jedoch, die Schulleiter der Grundschulen in einem Brief erneut auf die besonderen datenschutzrechtlichen Belange bei der Behandlung von Themen im Heimatkundeunterricht und Sachkundeunterricht hinzuweisen und in einigen Punkten eine Änderung der Lehrpläne zu verfügen.

Eine Orientierung zur Erreichung dieses Ziels könnten z. B. die Rahmenrichtlinien für die Grundschule in Niedersachsen bieten, in denen festgehalten ist, daß beim Thema „Das Kind in der Familie“ zusätzliche Gespräche mit den Eltern nötig sind, um Konflikte zu vermeiden. Aus Gründen des pädagogischen Taktes soll von einer erdachten Familie, nicht von den häuslichen Verhältnissen der Schüler ausgegangen, also eine ähnliche Lösung erreicht werden, wie ich sie für den Familienstammbaum vorgeschlagen habe. Weiterhin wird darauf hingewiesen, daß Schüler sich nicht genötigt fühlen dürfen, gegen ihren Willen oder gegen den Willen der Eltern personenbezogene Informationen aus der Familie preisgeben zu müssen.

Dies alles gebietet nicht nur ein vernünftiger Datenschutz, sondern der normale menschliche Takt.

## 7.5 Aushang von Schulanfänger-Listen in einem Lebensmittelgeschäft

Von einer Familie habe ich erfahren, daß vor Beginn des neuen Schuljahres in einem Lebensmittelgeschäft des Ortes eine Liste mit den Namen und Anschriften der Erstkläßler ausgehängt worden war. Die Vermutung lag nahe, daß die Daten von der Grundschule weitergegeben worden waren. Dies hat sich nicht bestätigt, die Daten stammten aus der Gemeindeverwaltung.

Wie mir der Bürgermeister dazu mitteilte, sei es ortsüblich, Erstkläßlern den Schulanfang durch kleine Geschenke „schmackhaft“ zu machen - auch im wörtlichen Sinne. Um diese Tradition lebendig zu erhalten, seien die Namen der Schulanfänger wie in jedem Jahr in den Ortsteilen der Gemeinde öffentlich bekanntgemacht worden, so daß davon ausgegangen werden könne, daß die Namen aus dieser Quelle stammten.

Schade wäre es, wenn aus Gründen des Datenschutzes eine nette Tradition abgeschafft werden müßte und so den Kindern die Freude über kleine Geschenke genommen würde. Deshalb habe ich mit dem Bürgermeister nach einer datenschutzgerechten Lösung gesucht. Diese soll nun darin bestehen, im Amtsblatt der Gemeinde darauf hinzuweisen, daß sich diejenigen Eltern melden können, die eine Veröffentlichung der Daten wünschen.

Eine solche Verfahrensweise entspricht § 4 des Sächsischen Datenschutzgesetzes, wonach die Übermittlung personenbezogener Daten mit Einwilligung der Betroffenen zulässig ist. Abs. 3 dieser Vorschrift sieht zwar die Schriftform für eine Einwilligung vor, auf sie kann jedoch verzichtet werden, wenn sie unangemessen ist. Im vorliegenden Fall würde ich sie für unangemessen halten, weil die meisten Betroffenen vermutlich anrufen werden und eine Tradition nicht bürokratisiert werden sollte.

Dies habe ich der Familie mitgeteilt.

# 8 Justiz

## 8.1 Datenschutz bei der Sächsischen Rechtsanwaltskammer

Die Defizite bei der Datenverarbeitung im Zulassungsverfahren zur Fachanwaltschaft (vgl. 4/8.5; 5/8.10) habe ich zum Anlaß genommen, einen unangemeldeten Informations- und Kontrollbesuch bei der Sächsischen Rechtsanwaltskammer durchzuführen:

- Hierbei mußte ich zunächst feststellen, daß die der Kammer im Fachanwaltszulassungsverfahren von den Antragstellern vorgelegten Unterlagen in der - mehr als 100 Kilometer vom Sitz der Rechtsanwaltskammer entfernten - Privatkanzlei des für die Vorbereitung der Prüfung zuständigen Vorstandsmitgliedes aufbewahrt werden. Dies betraf nicht nur die in der Bearbeitung befindlichen, sondern auch die Unterlagen aus abgeschlossenen Verfahren. Als Begründung für diese dem Grundsatz der Datensicherheit zuwiderlaufende Praxis gab die Kammer „Platzgründe“ an.

  Das rechtsaufsichtsführende SMJus hat mir inzwischen zugesichert, daß sämtliche Aktenbestände aus entschiedenen Zulassungsverfahren künftig in der Geschäftsstelle der Rechtsanwaltskammer aufbewahrt werden.

- Meine Kontrolle zeigte darüber hinaus, daß die Bediensteten der Geschäftsstelle der Kammer nicht einer Überprüfung auf Stasi-Mitarbeit unterzogen worden sind, obwohl ihre Tätigkeit dem öffentlichen Dienst zugehört. Weil nach Art. 119 SächsVerf die Eignung einer Person für den öffentlichen Dienst fehlt, wenn sie für das MfS tätig war und zudem die Vorschrift des § 9 SächsDSG öffentliche Dienstherren verpflichtet, auch personelle Maßnahmen zu treffen, die eine gesetzmäßige Datenverarbeitung gewährleisten, ist es auch aus Gründen der abstrakten Datensicherheit unerläßlich, im öffentlichen Dienst Überprüfungen nach dem

Stasi-Unterlagengesetz vorzunehmen. Ich habe deshalb das SMJus von diesem Überprüfungsdefizit bei der Sächsischen Rechtsanwaltskammer unterrichtet.

- Die Problematik der Überprüfung auf MfS-Mitarbeit habe ich mit dem SMJus auch hinsichtlich der Vorstandsmitglieder der Kammer eingehend erörtert. Zwar sind die Mitglieder des Vorstands nicht bei der Kammer „beschäftigt" im Sinne des § 119 SächsVerf; sie sind jedoch Amtsträger, soweit sie hoheitliche Aufgaben nach § 73 BRAO wahrnehmen, so z. B. im Falle der Entscheidung über die Verleihung der Befugnis, die Bezeichnung „Fachanwalt" zu führen. Dieser hoheitliche Charakter der Tätigkeit gebietet es, daß die Funktionsträger der Rechtsanwaltskammer besondere personelle Anforderungen erfüllen müssen, um die Gewähr dafür zu bieten, in rechtmäßiger und verantwortungsbewußter Weise mit sensiblen Daten (z. B. Mandanten- und Gutachtendaten) umzugehen. Wegen ihrer Bedeutung habe ich die Thematik auf dem Jour fixe mit der Amtsleitung des SMJus besprochen. Mir wurde dort zugesagt zu prüfen, ob gemäß § 4 des Gesetzes zur Prüfung von Rechtsanwaltzulassungen vom 24. Juli 1992 (BGBl. I S. 1386) die Vorstandsmitglieder der Sächsischen Rechtsanwaltskammer einer erneuten Überprüfung nach dem StUG zu unterziehen sind.

Ich werde die Angelegenheit weiter im Auge behalten.

## 8.2 Nutzung von personenbezogenen Daten über eingestellte strafrechtliche Ermittlungsverfahren

Aus Anlaß einer Eingabe bin ich der Frage nachgegangen, ob und in welchem Umfang Informationen über frühere, eingestellte strafrechtliche Ermittlungsverfahren genutzt werden dürfen. Angesichts des inzwischen in Probebetrieb geführten landesweiten zentralen staatsanwaltschaftlichen Register STARIS (vgl. 4/8.3.2), das als Teilstufe des künftigen bundesweiten staatswaltschaftlichen Verfahrensregisters gemäß § 474 StPO automatisiert betrieben wird, gewinnt dieses Problem wegen der kurzfristigen Verfügbarkeit der gespeicherten Informationen erhöhte Relevanz.

Zum rechtlichen Hintergrund: Welche personenbezogenen Daten in dem Register gespeichert und aus diesem abgerufen werden dürfen, ergibt sich aus § 474 Abs. 2 und 3 Satz 2 StPO. Hiernach sind die Staatsanwaltschaften unter anderem auch befugt, auf Einstellungsverfügungen und die zugrunde liegenden Akten für Zwecke eines neuen Strafverfahrens zuzugreifen (besser müßte es heißen: „... zur Durchführung eines Strafverfahrens"). Dies bedeutet aber nicht, daß die Staatsanwaltschaft allein die Tatsache, daß gegen den Beschuldigten in der Vergangenheit ermittelt worden ist, zu seinen Lasten verwerten darf (etwa nach dem Motto: „Irgend etwas wird schon dran gewesen sein").

Wie ich bei einem Beratungsbesuch feststellen konnte, wendet die Staatsanwaltschaft Dresden folgendes - mit mir abgestimmtes - datenschutzgerechte Verfahren an: Anhand des STARIS-Auszugs (Verfahrensliste) erfährt die Staatsanwaltschaft von ggf. eingestellten Ermittlungsverfahren gegen den Beschuldigten. Beabsichtigt

sie, diese Verfahren im laufenden Verfahren zu berücksichtigen, muß sie die Einstellungsverfügungen (möglicherweise nach Übersendung durch andere Staatsanwaltschaften) *inhaltlich* auswerten. Bestand kein Anfangsverdacht (hätte also die Staatsanwaltschaft gemäß § 152 Abs. 2 StPO von der Strafverfolgung von vornherein absehen müssen) oder steht die Unschuld des Betroffenen fest, dürfen aus der Einstellung keine negativen Rückschlüsse auf das laufende Verfahren gezogen werden. Ansonsten (z. B. der Verdacht besteht, er ist jedoch nicht „hinreichend" zur Erhebung der öffentlichen Klage gewesen) darf die ermittelnde Staatsanwaltschaft die Daten aus den Einstellungsverfügungen unter Beachtung des Grundsatzes der Verhältnismäßigkeit offen verwerten.

## 8.3 Informationen an gemeinnützige Empfänger von Bußgeldern

Bereits in 1/8.2 hatte ich kritisiert, daß es bei einer Einstellung von Strafverfahren nach § 153 a StPO mit der damit verbundenen Auflage gegenüber dem Beschuldigten, einen bestimmten Geldbetrag an eine gemeinnützige Einrichtung zu bezahlen, datenschutzrechtlich unzulässig ist, wenn die Einrichtung zur Überwachung des Zahlungseingangs Kenntnis von Namen und Anschrift des Beschuldigten erhält. Denn die Datenübermittlung an die Einrichtung kann weder auf eine hinreichende gesetzliche Grundlage noch auf eine wirksame Einwilligung gestützt werden.

Nach meinen langjährigen Verhandlungen mit dem SMJus hat die sächsische Justiz jetzt folgendes Verfahren eingeführt: Danach soll dem Beschuldigten ein Wahlrecht eingeräumt werden zwischen einer Zahlung an die Staatskasse zu deren Gunsten oder seiner Einwilligung zur Übermittlung personenbezogener Daten an eine gemeinnützige Einrichtung.

Wann eine endgültige und wirklich zufriedenstellende gesetzliche Regelung durch den Bundesgesetzgeber im Rahmen des Strafverfahrensänderungsgesetzes 96 geschaffen wird, ist derzeit noch nicht abzusehen.

# 9 Wirtschaft und Arbeit

## 9.1 Straßenverkehrswesen

### 9.1.1 Übermittlung von nicht aufgeklärten schwerwiegenden Verkehrsverstößen durch die Bußgeldstelle an die Zulassungsstelle zur Erteilung einer Fahrtenbuchauflage gemäß § 31a StVZO

Nicht selten ordnen die Zulassungsstellen bei nicht aufgeklärten schwerwiegenden Verkehrsverstößen gegenüber dem Fahrzeughalter die Führung eines Fahrtenbuchs an, wenn die Feststellung des Fahrzeugführers nicht möglich war. Rechtsgrundalge hierfür ist § 31a StVZO.

Um nach § 31a StVZO vorgehen zu können, sind die Zulassungsstellen auf die regelmäßige Übermittlung solcher Verkehrsverstöße durch die Bußgeldstellen angewiesen. Eine bundesweite Umfrage des BfD ergab, daß die erforderliche regelmäßige Datenübermittlung durch § 46 Abs. 1 OWiG i. V. m. § 13 Abs. 1 Nr. 1 EGGVG i. d. F. des JuMiG vom 18. Juni 1997 (BGBl. I S. 1430) gedeckt sei.

### 9.1.2 Radarmessung durch Private

Der Boulevardpresse war zu entnehmen, daß ein sächsischer Landkreis eine private Firma mit der Durchführung von Radarmessungen zur Geschwindigkeitsüberwachung beauftragt haben soll. Die Geräte seien nicht geeicht, der Vertrag mit der Firma sei leistungsbezogen (Stichwort: „Kopfgeld“).

Obwohl ich im allgemeinen nichts von reißerischen Presseberichten halte, habe ich das Landratsamt zur Stellungnahme aufgefordert. Es stellte sich heraus, daß die Geschwindigkeitsmessungen ausschließlich durch Bedienstete des Landratsamts durchgeführt wurden. Lediglich die zur Geschwindigkeitsmessung erforderlichen Geräte wurden angemietet, wobei der Vermieter beim Einsatz des Lichtschrankenmeßgeräts ein technisches Mitspracherecht hatte. Die Verfahrensweise entsprach den Vorgaben der Rechtsprechung zur Geschwindigkeitsmessung durch Private (siehe auch 5/9.1.5). Die mir vom Landratsamt zur Verfügung gestellten Unterlagen belegten darüber hinaus, daß die eingesetzte Lichtschrankenanlage geeicht war. Es lag kein Verstoß gegen datenschutzrechtliche Bestimmungen vor.

## 9.2 Gewerberecht

### Mitteilung über die Erteilung von Reisegewerbekarten an die IHK’n

Die IHK zu Leipzig bat das SMWA, die Gewerbeämter zu veranlassen, ihr regelmäßig die Daten von Reisegewerbekarteninhabern zu übermitteln. Diese Daten würden zur Feststellung der IHK-Mitgliedschaft (§ 2 IHK-G) der Reisegewerbetreibenden benötigt.

Mit dem SMWA bin ich einig, daß regelmäßig Datenübermittlungen an die IHK’n nach § 14 Abs. 5 Nr. 1 GewO ausschließlich bei *stehendem* Gewerbe zulässig sind.

Gemäß § 2 IHK-G gehören zur Industrie- und Handelskammer u. a. natürliche Personen, sofern sie zur Gewerbesteuer veranlagt sind *und* im Bezirk der Industrie- und Handelskammer entweder eine gewerbliche Niederlassung oder eine Betriebsstätte oder eine Verkaufsstelle unterhalten.

Insbesondere im Reisegewerbe kann nicht davon ausgegangen werden, daß diese beiden Voraussetzungen erfüllt sind, so daß Datenübermittlungen über diesen Personenkreis an die IHK’n unzulässig sind. Die regelmäßige Übermittlung der Daten der nicht kammerpflichtigen Reisegewerbekarteninhaber würde zudem zu einem

(großen) Datenbestand führen, der für die Aufgabenerfüllung der IHK nicht erforderlich ist.

Sollte ein gewerbesteuerpflichtiger Reisegewerbekarteninhaber allerdings gleichzeitig eine gewerbliche Niederlassung, eine Betriebsstätte oder eine Verkaufsstelle unterhalten, würden die IHK'n die Daten bereits nach § 14 Abs. 5 Nr. 1 GewO erhalten.

## 9.3 Industrie- und Handelskammern; Handwerkskammern

### Übermittlung von Besteuerungsgrundlagen durch die Finanzämter an die Industrie- und Handelskammern und Handwerkskammern zur Festsetzung der Kammerbeiträge

In vielen Anfragen zweifelten Mitglieder der IHK und der HWK die Zulässigkeit der Mitteilung ihrer Besteuerungsgrundlagen durch die Finanzämter an die Kammern als Grundlage für die Festsetzung der Kammerbeiträge an. Sie sahen darin einen Verstoß gegen „den Datenschutz".

Dabei wurde übersehen, daß sich die Zulässigkeit solcher Mitteilungen für die Bemessung der Kammerbeiträge nach § 113 Abs. 2 HandwO, § 9 Abs. 2 IHK-G i. V. m. § 31 Abs. 1 AO bemißt. Danach sind die Finanzbehörden berechtigt, Besteuerungsgrundlagen, Steuermeßbeträge und Steuerbeträge an Körperschaften des öffentlichen Rechts (hier die Kammern) zur Festsetzung von solchen Abgaben mitzuteilen, die an diese Besteuerungsgrundlagen, Steuermeßbeträge oder Steuerbeträge anknüpfen. Dies ist bei den Kammerbeiträgen der Fall.

## 9.4 Offene Vermögensfragen

In diesem Jahr nicht belegt.

## 9.5 Sonstiges

### Berufliche Fortbildung - Lebenslauferstellung bei der Zulassung zu Prüfungen

Immer wieder stelle ich in Prüfungsordnungen der Regierungspräsidien Bestimmungen fest, wonach dem Antrag auf Prüfungszulassung u. a. ein (tabellarischer) Lebenslauf beizufügen ist. Nach § 11 Abs. 1 SächsDSG ist aber das Erheben personenbezogener Daten nur zulässig, soweit ihre Kenntnis zur Aufgabenerfüllung der erhebenden Stelle erforderlich ist.

Nachdem ich mit dem SMWA schon früher (vgl. 4/9.3.2) Konsens erzielen konnte, daß Lebensläufe als Prüfungsvoraussetzung nicht erforderlich sind, habe ich die Regierungspräsidien aufgefordert, in allen Prüfungsordnungen ihres Zuständigkeits-

bereichs auf tabellarische Lebensläufe für die Zulassung zu einzelnen Prüfungen zu verzichten, weil diese das Persönlichkeitsrecht der Betroffenen regelmäßig tief berühren.

Ein Regierungspräsidium erklärte daraufhin, die Vorlage eines Lebenslaufs sei in Einzelfällen dann „dienlich", wenn der Bewerber fehlende Qualifikationsnachweise durch Eigenauskünfte ersetzen müsse. Insbesondere Teilnehmern, die nicht die übliche Ausbildung durchlaufen hätten, werde so die Möglichkeit eröffnet, auf „andere Weise" ihre Eignung auf Zulassung zur Prüfung glaubhaft zu machen.

Dem Regierungspräsidium habe ich entgegengehalten, daß es selbst die Erstellung von Lebensläufen als Zulassungsvoraussetzung zu Prüfungen lediglich für „dienlich" und „zweckmäßig" erachtet. Der datenschutzrechtliche Grundsatz der Erforderlichkeit bedeutet aber, 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. Ebensowenig reicht es aus, wenn die Daten zur Aufgabenerfüllung der erhebenden Stelle nur „dienlich" oder z. B. als Hintergrundinformation oder zur „Abrundung des Bildes" nützlich sind. Vielmehr muß es der öffentlichen Stelle unmöglich sein, ihre Aufgabe ohne Kenntnis der Daten ordnungsgemäß zu erfüllen (vgl. im übrigen Simitis/Dammann/Geiger/Mallmann/Walz, § 13 Rdnr. 23). Ein *unnötiges* Ausforschen des Persönlichkeitsbereichs gilt es jedenfalls zu verhindern.

Falls ein Bewerber sich tatsächlich nicht in einem besonderen Lehrgang auf die fragliche Prüfung vorbereitet hat - und nur dann -, kann er seine Befähigung auch auf andere Art und Weise, beispielsweise über Zeugnisse, Bescheinigungen oder eine von ihm angefertigte Aufstellung seines beruflichen Werdegangs belegen. Selbst hier sind alle anderen, üblicherweise in einem Lebenslauf enthaltenen persönlichen Angaben überflüssig. Daß es Befreiungstatbestände für die einzelnen Prüfungen gibt, kann jeder Prüfling unschwer den jeweils einschlägigen Vorschriften entnehmen.

Die Regierungspräsidien sind meiner Aufforderung zur Überprüfung der Prüfungsordnungen und zum Verzicht auf Lebensläufe inzwischen nachgekommen.

# 10 Soziales und Gesundheit

## 10.1 Gesundheitswesen

### 10.1.1 Wartung und Fernwartung von Datenverarbeitungsanlagen in Krankenhäusern, Verpflichtung nach dem Verpflichtungsgesetz

Die Wartung und Fernwartung von Datenverarbeitungsanlagen im Krankenhausbereich wird regelmäßig von Privatfirmen durchgeführt, weil die heutigen EDV-Systeme eine Wartung durch die Systembetreuer der Krankenhäuser nur noch einge-

schränkt zulassen, insbesondere das Erkennen und Beheben von Fehlern in der Soft- und Hardware im Echtbetrieb. Zu diesem Zweck müssen die Mitarbeiter der Wartungsfirmen ggf. Patientendaten notwendigerweise einsehen. Problematisch ist, ob insoweit eine Befugnis zur Offenbarung des nach § 203 Abs. 1 StGB geschützten Patientengeheimnisses besteht; denn es wird bezweifelt, daß ein solcher Mitarbeiter zu den berufsmäßig tätigen Gehilfen des Arztes i. S. d. § 203 Abs. 3 StGB gehört. Zu dieser Problematik haben mich die Krankenhäuser um Beantwortung folgender Fragen gebeten:

1. Ist eine Wartung eine Datenverarbeitung im Auftrag?
2. Welche Befugnis besteht zur Offenbarung des von § 203 Strafgesetzbuch geschützten Patientengeheimnisses?
3. Durch welche Maßnahme kann gemäß § 33 Abs. 10 SächsKHG sichergestellt werden, daß bei einer Datenverarbeitung im Auftrag der Auftragnehmer die § 203 StGB entsprechende Schweigepflicht einhält?

Dazu habe ich folgendes vertreten:

1. *Datenverarbeitung im Auftrag*
   Nach wie vor gehen die Meinungen darüber auseinander, ob eine (Fern-)Wartung eine Datenverarbeitung im Auftrag darstellt. Für mich ist sie es aus folgenden Gründen:

   Werden zur Fehlersuche und Fehlerbeseitigung Patientendaten eingesehen, Datenbestände kopiert, gesichert, eingespielt, Datenbanken „repariert", Datensätze korrigiert oder Vergleichsläufe zwischen echten Datenbeständen durchgeführt, so handelt es sich bei jedem dieser Vorgänge um einen Datenverarbeitungsvorgang, nämlich um ein Nutzen. § 3 Abs. 2 Nr. 6 SächsDSG definiert als Nutzen „jede sonstige Verwendung personenbezogener Daten". Auch aus § 12 Abs. 3 SächsDSG ergibt sich, daß die Wartung eine Datennutzung ist, denn in dieser Vorschrift stellt der Gesetzgeber ausdrücklich klar: Bei einer Wartung liegt keine zweckändernde *Nutzung* vor.

   Das SMI ist zwar anderer Auffassung. An der Anwendbarkeit von § 33 Abs. 10 SächsKHG ändert das aber nichts; denn in dieser Vorschrift heißt es:

   *Das Krankenhaus kann sich zur Verarbeitung von Patientendaten anderer Personen oder Stellen bedienen, wenn sichergestellt ist, daß diese die Datenschutzbestimmungen dieses Gesetzes und die § 203 Strafgesetzbuch entsprechende Schweigepflicht einhalten. Das Krankenhaus ist verpflichtet, erforderlichenfalls den Auftragnehmer anzuweisen, Technik und Organisation der Datensicherung zu ergänzen. Die Auftragserteilung bedarf der vorherigen Zustimmung durch die zuständige Behörde.* (Anm.: Zuständig sind die Regierungspräsidien)

   Es ist also unerheblich, ob die Daten in einem personellen oder automatisierten Verfahren, als Haupt- oder Nebenzweck aus einem Vertragsverhältnis, für einen Einzelfall oder eine Vielzahl von Fällen verarbeitet werden. Entscheidend ist, daß

eine andere Stelle als das Krankenhaus die Patientendaten verarbeitet. Ist dies der Fall, muß den Anforderungen des § 33 Abs. 10 SächsKHG Rechnung getragen werden. Dazu gehört u. a., daß das Regierungspräsidium der Auftragserteilung vorab zustimmt.

Mit dieser Regelung wollte der Gesetzgeber Patientendaten bei der Verarbeitung durch Stellen außerhalb des Krankenhauses demselben Schutzniveau unterwerfen wie bei einer Verarbeitung innerhalb des Krankenhauses. Dabei hat er es für notwendig gehalten, in einem behördlichen Zustimmungsverfahren überprüfen zu lassen, daß dies gewährleistet ist. So ist es nach meiner Auffassung auch kein Widerspruch, wenn der Vertrag zwischen einem Krankenhaus und einer externen Wartungsfirma einerseits von der Zustimmung des Regierungspräsidiums abhängig ist, sich aber andererseits für das externe Unternehmen keine Verpflichtung ergibt, eine Wartung als „geschäftsmäßige Datenverarbeitung im Auftrag“ gemäß § 32 BDSG zu melden. In dieser Frage besteht Übereinstimmung mit dem SMI und den Regierungspräsidien.

2. *Offenbarungsbefugnis*
   Ohne ausdrückliche Schweigepflichtentbindung durch einen Patienten kann sich eine Offenbarungsbefugnis z. B. aus gesetzlichen Vorschriften ergeben. § 33 Abs. 10 SächsKHG ist eine solche gesetzliche Offenbarungsbefugnis. Hier läßt der Gesetzgeber mit Blick auf § 203 StGB für Patientendaten die Datenverarbeitung im Auftrag ausdrücklich zu, knüpft sie aber an bestimmte Bedingungen. So muß u. a. sichergestellt sein, daß beim Auftragnehmer eine § 203 StGB entsprechende Schweigepflicht eingehalten wird.

   § 33 Abs. 10 SächsKHG wäre überflüssig, wenn nicht eine vom Patientenwillen unabhängige Offenbarungsbefugnis bestünde. Eine Datenverarbeitung im Auftrag ist nur dann praktikabel, wenn nicht einzelne Fälle ausgenommen werden müssen. Jede andere Gesetzesauslegung hätte zur Folge, daß jeder Patient um Erteilung einer Schweigepflichtentbindung zu bitten wäre. Für die wenigen Patienten, die sie nicht erteilen, müßten Sonderlösungen gefunden werden.

   Auch wenn für Wartungszwecke eine grundsätzliche Befugnis zur Offenbarung des Patientengeheimnisses besteht, dürfen Patientendaten nur im Ausnahmefall bekanntgegeben werden. Die Wartung hat möglichst ohne Zugriff auf Patientendaten auszukommen (z. B. Verwendung von Testdaten). Eine weitere Möglichkeit besteht in der „Verfremdung“ von Namen und Anschrift.

3. *Sicherstellung der Schweigepflicht*
   In dieser Frage befinden wir uns noch in der Diskussion mit SMS, SMI, den Ärzte- und Zahnärztekammern und der Sächsischen Krankenhausgesellschaft.

### 10.1.2 Kontrolle eines sächsischen Landeskrankenhauses

In einem sächsischen Landeskrankenhaus habe ich eine Querschnittskontrolle durchgeführt, die sich auf Stichproben beschränkte und mir einen Überblick über die

Einhaltung des Datenschutzes vermitteln sollte. Von meinen Feststellungen möchte ich folgende hervorheben:

1. *Krankenhausinterner Datenschutzbeauftragter*
   Gemäß § 33 Abs. 8 Satz 2 SächsKHG hat der Krankenhausträger einen Beauftragten für den Datenschutz zu bestellen. Die Bestellung erfolgte dreieinhalb Jahre nach Inkrafttreten des Sächsischen Krankenhausgesetzes. Das halte ich für zu spät.

   Zum internen Datenschutzbeauftragten dürfen nur Personen bestellt werden, die dadurch keinem Interessenkonflikt mit sonstigen dienstlichen Aufgaben ausgesetzt sind (§ 33 Abs. 8 Satz 3 SächsKHG). Der jetzige Datenschutzbeauftragte ist Leiter des Finanz- und Rechnungswesens, so daß solche Interessenkonflikte vermutlich nicht auftreten werden. Bei dem vorangegangenen Datenschutzbeauftragten, dem Leiter der EDV-Abteilung, war das nicht der Fall; denn zu seinen Aufgaben gehörte die Kontrolle der eigenen Tätigkeit, was mit einer qualifizierten internen Kontrolle nicht zu vereinbaren ist.

2. *Allgemeiner Datenschutz*
   Da Patientendaten ein besonders hohes Schutzniveau zukommt, sind umfangreiche Datensicherheitsmaßnahmen notwendig. Diese waren erst ansatzweise realisiert. Schriftlich geregelt war bis auf die Behandlung der Posteingänge (s. Nr. 6) kein datenschutzrechtlich relevanter Bereich.

3. *Verpflichtung auf das Datengeheimnis*
   Mit Ausnahme der Mitarbeiter in der Wäscherei und der angestellten Handwerker wurde das Personal gemäß § 6 SächsDSG auf das Datengeheimnis verpflichtet und über die Bedeutung der ärztlichen Schweigepflicht (§ 203 Strafgesetzbuch) sowie die Amtsverschwiegenheit (§ 9 BAT-O) belehrt. Da die von der Verpflichtung ausgenommenen Mitarbeiter bei Ausübung ihrer Tätigkeit wohl nicht mit personenbezogenen Daten in Berührung kommen, ist dies nicht zu beanstanden.

4. *Automatisierte Verarbeitung von Beschäftigtendaten*
   Das Krankenhaus betreibt eine digitale Telekommunikationsanlage. Daten von Gesprächen, die Beschäftigte von dienstlichen Apparaten aus führen, werden erfaßt und monatlich ausgewertet.

   Nach § 31 Abs. 7 SächsDSG darf eine automatisierte Verarbeitung von Beschäftigtendaten nur im Benehmen mit dem Sächsischen Datenschutzbeauftragten eingeführt, angewendet, geändert oder erweitert werden. Das Benehmen war nicht hergestellt worden. Ich habe gebeten, die Meldungen für alle in Betracht kommenden Verfahren nachzureichen.

5. *Datensicherheit im Rahmen der automatisierten Datenverarbeitung*
   Der Serverraum im Erdgeschoß ist kein ständig besetzter Arbeitsplatz; er wird nur sporadisch und dann zu kurzfristigem Arbeiten betreten. Die ungesicherten Fenster bieten wenig Schutz, so daß durch Anschläge und Vandalismus aufgrund

der Konzentration von IT-Geräten ein deutlich höherer Schaden eintreten kann als in Räumen, in denen „nur“ PCs installiert sind. Mindestens ebenso gravierend können die Auswirkungen auf die zentral im Server gespeicherten Datenbestände sein, weil vom Server aus mehr Manipulations- oder Sabotagemöglichkeiten bestehen als von einem PC.

Deshalb habe ich gefordert, die Fenster im Serverraum zu sichern und ihn durch Sicherheitstüren (z. B. Stahlblechtüren) gegen den Zutritt unbefugter Personen zu schützen. Eine solche Maßnahme würde gleichzeitig dem Brandschutz dienen, der aus datenschutzrechtlicher Sicht der Vernichtung von Datenmaterial vorbeugt. Zusätzlich habe ich den Einbau von Gefahrenmeldeanlagen (Einbruch, Diebstahl, Brand) empfohlen, so daß frühzeitig auf Gefahren hingewiesen wird und sofort Gegenmaßnahmen eingeleitet werden können. Darüber hinaus sollten die Namen der zutrittsberechtigten Personen schriftlich festgelegt, ihre Zahl auf ein Mindestmaß reduziert und erfolgte Zutritte dokumentiert werden.

6. *Posteingänge*
   Die Verfahrensweise, wonach alle mit persönlicher Anschrift versehenen Postsendungen ungeöffnet an den Empfänger weitergeleitet werden, war nicht zu beanstanden. Als persönlich adressiert gelten Sendungen, bei denen der Name des Adressaten vor der Anschrift des Krankenhauses genannt wird oder die an anderer Stelle einen Zusatz wie „persönlich“ oder „vertraulich“ enthalten bzw. durch andere Merkmale erkennbar einen persönlichen Charakter haben.

7. *Patientenaufnahme*
   Bei der stationären Aufnahme eines Patienten werden seine Daten im automatisierten System ITOS erhoben und gespeichert. Die Angaben zur *Nationalität* und zum *Familienstand* haben sich als nicht erforderlich herausgestellt und dürfen deshalb künftig nicht mehr erhoben werden. Soweit sie bereits gespeichert sind, hat eine Löschung zu erfolgen (§ 19 Abs. 1 SächsDSG). Ist diese nicht oder nur mit unverhältnismäßig hohem Aufwand möglich, sind die Daten zu sperren (§§ 19 Abs. 4 Nr. 2, 20 Abs. 1 SächsDSG).

   Die *Konfessionszugehörigkeit* wird zur Weitergabe an die Krankenhausseelsorge erfragt. Der Patient wird weder auf die Freiwilligkeit der Angabe hingewiesen noch über den Verwendungszweck informiert. Dem Patienten ist mitzuteilen, welchen Zwecken die Angabe der Konfessionszugehörigkeit dient und daß die Angabe freiwillig ist.

   Der *Arbeitgeber* wird zur Weitergabe an die Krankenkassen erfragt. Die Erforderlichkeit ist noch ungeklärt.

   Es besteht keine Möglichkeit, die Namen derjenigen Personen einzugeben, denen Auskunft über den Aufenthalt des Patienten erteilt werden darf. Lediglich eine *Auskunftssperre* ist vorgesehen, so daß sich der Patient zwischen den Alternativen „alle“ oder „keiner“ entscheiden muß. Eine Erweiterung der Eingabemöglichkeiten sollte angestrebt werden.

8. *Archivierung von Patientenakten*
   Im krankenhauseigenen Archiv sind die Akten der seit 1950 entlassenen, verlegten oder verstorbenen Patienten vorhanden. Die bis Ende 1950 abgeschlossenen Patientenakten wurden an das Sächsische Staatsarchiv abgegeben. Auch die vorhandenen Akten sollen dem Staatsarchiv übergeben werden.

   Die archivrechtliche Behandlung von Patientenakten ist noch nicht abschließend geklärt. So ist insbesondere die Anbietepflicht nach § 5 Abs. 1 und 2 SächsArchG im Verhältnis zu der Regelung in § 33 Abs. 6 SächsKHG und der für Altdaten (Unterlagen, die vor dem 3. Oktober 1990 entstanden sind) geltenden Sonderregelung problematisch. Dieser Problemkreis wird derzeit mit dem SMI erörtert.

   Innerhalb eines Krankenhauses unterliegen Patientendaten der Zweckbindung nach § 33 Abs. 2 Nr. 1 bis 3 SächsKHG. Derzeit erhält jeder Mitarbeiter des Krankenhauses die Akten ehemaliger Patienten ohne besondere Prüfung. Dies gefährdet die datenschutzgerechte Verwendung von Patientendaten. Hier fehlt eine organisatorische Regelung, z. B. durch eine Archivordnung, die so aussehen könnte, daß archivierte Patientenakten nur bestimmten, namentlich festgelegten Personen ausgehändigt werden.

### 10.1.3 Datenschutz im Maßregelvollzug

In 5/10.1.11 habe ich über die Absicht des SMS berichtet, für den Datenschutz im Maßregelvollzug eine Dienstanweisung zu erarbeiten. Inzwischen liegt ein Entwurf vor. Ich habe dazu ausführlich Stellung genommen. Es zeichnet sich ab, daß noch eine Reihe von Einzelfragen aus der komplexen und schwierigen Materie „Datenschutz im Maßregelvollzug“ diskutiert werden muß, um Lösungen zu finden, die der Praxis und dem Datenschutz gerecht werden.

### 10.1.4 Befragung ambulanter Suchtberatungsstellen durch ein sächsisches Landeskrankenhaus

Um bei einem Patienten das Rückfallrisiko nach einer stationären Suchtbehandlung zu mindern, gehört es zur Therapie im Krankenhaus, ihn zur Nachbetreuung in einer Suchtberatungsstelle zu motivieren. Bei ca. zwei Dritteln der Patienten gelingt dies.

Ein sächsisches Landeskrankenhaus wollte bei den Beratungsstellen in seinem Einzugsgebiet zur Qualitätskontrolle der eigenen Therapiemaßnahmen eine patientenbezogene Befragung durchführen. Festgestellt werden sollte, welcher „Patiententyp“ keine Beratungsstellen aufsucht und welche Zusammenhänge zwischen Anzahl und Zeitdauer stationärer Aufenthalte bestehen. Auch Aufschlüsse über Häufigkeit und Schwere von Rückfällen waren von Interesse. Zu diesem Zweck wurde mit Einverständnis des Patienten der Beratungsstelle seines Vertrauens ein Fragebogen und ein Entlassungsbericht übersandt. Der Fragebogen sollte nach Ablauf des Beobachtungszeitraums ausgefüllt an das Krankenhaus zurückgegeben werden.

Ein Träger von Suchtberatungsstellen trug mir seine datenschutzrechtlichen Bedenken vor, wobei er den Wert solcher Untersuchungen nicht in Frage gestellt hat. Bedenklich erschien ihm aber, daß die Anonymität der Patienten nicht gewährleistet war, was letztlich auch zu einer Kontrolle der Beratungsstellen verwendet werden könnte. Bedenken bestanden zudem gegen Form und Inhalt der Einverständniserklärung. Für wünschenswert hielt der Träger eine Datenerhebung beim Betroffenen durch das Krankenhaus, also seine direkte Befragung ohne Einschaltung der Suchtberatungsstelle.

Nach Auffassung des Krankenhauses scheidet eine unmittelbare Nacherhebung beim Patienten durch Übersendung des Fragebogens aus, weil die Objektivität der Angaben nicht gesichert wäre.

Ich bin gebeten worden, mich für ein datenschutzgerechtes Verfahren einzusetzen. Das habe ich getan und konnte folgendes erreichen:

*Verfahren zur Gewährleistung der Freiwilligkeit*
Die Befragung einer Suchtberatungsstelle über einen Patienten ist gemäß § 4 Abs. 1 Nr. 2 SächsDSG nur mit seiner Einwilligung zulässig. Diese ist an bestimmte Voraussetzungen, insbesondere die Schriftform, gebunden, wobei der Patient den in § 203 Strafgesetzbuch bezeichneten Personenkreis des Krankenhauses und der Suchtberatungsstelle zusätzlich von der gesetzlichen Schweigepflicht entbinden muß.

Das Krankenhaus verfährt folgendermaßen: Dem Patienten wird in einem Therapiegespräch vor seiner Entlassung die Bedeutung der Datenerhebung erläutert und der Fragebogen inhaltlich vorgestellt. Er wird darüber informiert, daß die Beratungsstelle einen Bericht über seine Suchtbehandlung erhält, daß seine Einwilligung Voraussetzung für die Befragung ist und daß ihm bei Verweigerung der Einwilligung keine Nachteile entstehen werden. Er gibt eine entsprechende schriftliche Erklärung und Schweigepflichtentbindung ab (s. u.). Dafür sind *drei* Formblätter vorzusehen. Zwei Exemplare unterzeichnet der Patient im Original - eins für die Beratungsstelle, eins für das Krankenhaus -, ein Formblatt erhält er ausgehändigt.

*Anonymität der Befragung*
Auch bei Datenerhebungen auf freiwilliger Basis hat die Anonymität des Betroffenen Vorrang. Nur wenn mit einer anonymen Erhebung das angestrebte Ziel nicht erreicht werden kann, darf sie personenbezogenen durchgeführt werden.

Wie sich zeigte, beeinträchtigt eine anonyme Befragung das Ergebnis nicht. Deshalb wurde der Aufbau des Fragebogens so verändert, daß die für die Suchtberatungsstelle bestimmten Patientendaten vor Rücksendung abgetrennt werden können. Daten, die über Bemerkungszeilen erhoben werden sollten, sind durch anzukreuzende Datenkataloge ersetzt worden, statt genauer Datumsangaben sind jetzt nur noch Jahresangaben vorgesehen.
Diese Anonymität erschwert es gleichzeitig, die Suchtberatungsstelle zu identifizieren.

*Einwilligungserklärung, Schweigepflichtentbindung*
Die bisher verwendete Einverständniserklärung, die offensichtlich für die Nachbehandlung durch einen niedergelassen Arzt vorgesehen war, entsprach nicht den datenschutzrechtlichen Erfordernissen. Künftig wird das folgende, von mir vorgeschlagene Formblatt verwendet:

**Einwilligungserklärung, Schweigepflichtentbindung**

Ich bin damit einverstanden, daß das Krankenhaus einen Entlassungsbericht über meine Suchtbehandlung mit den für die Suchtberatungsstelle

_____

Name der Einrichtung

_____

Anschrift der Einrichtung

erforderlichen Angaben erstellt und an diese weitergibt. Außerdem bin ich damit einverstanden, daß die Suchtberatungsstelle dem Krankenhaus über den weiteren Verlauf meiner Krankheit berichtet. Dies wird in Form eines Fragebogens geschehen, der mir bekannt ist. Damit soll dem Krankenhaus eine verbesserte Qualitätskontrolle ermöglicht werden. Die nach § 203 Strafgesetzbuch zur Verschwiegenheit verpflichteten Personen des Krankenhauses und der Suchtberatungsstelle entbinde ich *insoweit* von ihrer gesetzlichen Schweigepflicht.

Ich bin darauf hingewiesen worden, daß mir durch eine Verweigerung dieser Einwilligung keine Nachteile entstehen werden und daß ich berechtigt bin, sie jederzeit ohne Angabe von Gründen zu widerrufen.

_____

Name, Vorname, Anschrift, Geburtsdatum der Patientin / des Patienten

_____ _____

Ort, Datum Unterschrift der Patientin / des Patienten

### 10.1.5 Besetzung des Botendienstes innerhalb eines Krankenhauses mit Zivildienstleistenden

Ein Kreiskrankenhaus fragte, ob es zulässig sei, den Botendienst mit Zivildienstleistenden zu besetzen und was ggf. beachtet werden müsse. Dazu habe ich folgendes gesagt:

Die Besetzung des Botendienstes mit Zivildienstleistenden ist unter bestimmten Voraussetzungen zulässig. Da Boten nicht an den in § 3 Abs. 2 SächsDSG genannten Datenverarbeitungsvorgängen beteiligt sind, ihre Tätigkeit sie aber mit personenbezogenen Daten, hier insbesondere Patientendaten, in Verbindung bringt, hängt ihr Einsatz davon ab, daß sie die Datensicherheit nicht gefährden (§ 33 Abs. 8 i. V. m. § 33 Abs. 1 SächsKHG und § 9 Abs. 2 SächsDSG). Einen möglichen Datenmißbrauch hat der Krankenhausträger durch technische und organisatorische Maßnahmen zu verhindern, wobei die getroffenen Maßnahmen erforderlich und angemessen sein müssen. Aus meiner Sicht ist folgendes notwendig:

- *Sorgfältige Personalauswahl im Hinblick auf die Zuverlässigkeit*
  Wie mir das Krankenhaus mitgeteilt hat, würden die Zivildienstleistenden nicht ohne vorherige Rücksprache „zugeteilt". Vielmehr könne das Krankenhaus Vorstellungen zur Eignung eines Zivildienstleistenden äußern und auf diese Weise die Auswahl beeinflussen.

- *Einweisung in die Aufgabe*
  Die Zivildienstleistenden sind bei Einweisung in ihre Aufgabe ausdrücklich auf die Belange des Datenschutzes und ihre Sorgfaltspflicht hinzuweisen.

- *Verpflichtung auf das Datengeheimnis gemäß § 6 SächsDSG*
  Ich habe dem Krankenhaus empfohlen, das von mir speziell für den Krankenhausbereich entworfene Muster für eine „Schweigepflichterklärung" auch bei Zivildienstleistenden zu verwenden und ihnen das zugehörige Merkblatt auszuhändigen. Beides ist in 5/10.1.4 abgedruckt.

- *Transportsicherung der Unterlagen*
  Es muß gewährleistet sein, daß die Datenträger, also Akten, einzelne Schriftstücke, elektronische Speichermedien, Röntgenaufnahmen etc., nicht unbefugt gelesen, kopiert, verändert, gelöscht oder entfernt werden (§ 9 Abs. 2 Nr. 9 SächsDSG). Dies sollte vorrangig durch technische Maßnahmen sichergestellt werden (z. B. verschließbare Transportbehälter, Sicherung des Transportwagens gegen das Herausrutschen von Gegenständen). Auf keinen Fall darf der Bote den Transportwagen unbeaufsichtigt lassen.

### 10.1.6 Aushänge in einem Krankenhaus über Personen, denen Hausverbot erteilt wurde

Von dem Besucher eines Kreiskrankenhauses war mir mitgeteilt worden, es gäbe in den Eingangsbereichen der einzelnen Gebäude Aushänge mit den Namen und Anschriften von Personen, denen Hausverbot erteilt wurde.

Ich habe das Krankenhaus darüber unterrichtet, daß eine solche Praxis mit geltendem Datenschutzrecht nicht zu vereinbaren ist. Auch die Wirksamkeit solcher Aushänge habe ich angezweifelt, weil nicht kontrolliert wird, ob die genannten Personen das Krankenhaus betreten. Besonders problematisch sind Aushänge über Personen, die Angehörige oder Bezugspersonen von Patienten sind, weil hier Patientendaten veröffentlicht werden. § 33 Abs. 1 Satz 3 SächsKHG stellt ausdrücklich klar, daß die Daten dieser Personen dazu gehören. Unter welchen Voraussetzungen Patientendaten an Dritte weitergegeben werden dürfen, regelt § 33 Abs. 3 SächsKHG. Nach dieser Vorschrift bestand keine Befugnis zur Datenübermittlung. Die Aushänge waren also unzulässig; das Krankenhaus hat sie entfernt.

## 10.2 Sozialwesen

### 10.2.1 Aktenführung im Allgemeinen Sozialen Dienst des Jugendamts

Ein örtlicher Träger der öffentlichen Jugendhilfe beabsichtigt, eine Dienstanweisung über die Aktenführung im Allgemeinen Sozialen Dienst (ASD) des Jugendamts zu erlassen. Er hat mir einen Entwurf mit der Bitte um Stellungnahme vorgelegt.

Ausgangspunkt der Überlegungen sind die gesetzlichen Regelungen des SGB VIII und, soweit dieses keine Aussagen enthält, des SGB X.

§ 63 Abs. 2 SGB VIII legt den Grundsatz fest, daß für unterschiedliche Aufgaben der Jugendhilfe unterschiedliche Akten geführt werden müssen. Nach Abs. 2 Satz 1 dürfen Daten, die zur Erfüllung unterschiedlicher Aufgaben der Jugendhilfe erhoben wurden, nur zusammengeführt werden, wenn und auch nur solange dies wegen eines unmittelbaren Sachzusammenhangs erforderlich ist. Dieser unmittelbare Sachzusammenhang ist z. B. gegeben, wenn für dieselbe Person oder für dieselbe Familie unterschiedliche Leistungen erbracht werden. Das Gesetz ordnet also an, daß auch in diesen Fällen grundsätzlich verschiedene Akten zu führen sind und daß Daten nur solange zusammengeführt werden, wie dies wegen des unmittelbaren Sachzusammenhangs erforderlich ist.

Noch strenger ist die Regelung des § 63 Abs. 2 Satz 2. Daten, die zu Leistungszwecken im Sinne des § 2 Abs. 2 SGB VIII, und Daten, die für andere Aufgaben des Jugendamts nach § 2 Abs. 3 SGB VIII erhoben wurden, dürfen nur zusammengeführt werden, soweit dies zur Erfüllung der jeweiligen Aufgabe erforderlich ist.

Der Entwurf der Dienstanweisung sah getrennte Akten vor, und zwar die objektive Leistungsakte und die subjektive Leistungsakte, daneben „lose Vorgänge“. Die objektive Leistungsakte dient als zentrale Dokumentation. Sie soll alle Unterlagen enthalten, die für die Jugendhilfeleistung, also auch das Verwaltungsverfahren, erforderlich sind, wie den Antrag, Hilfepläne, Stellungnahmen von Heimen, ärztliche Befunde, Schriftverkehr mit der wirtschaftlichen Jugendhilfe und den Bewilligungsbescheid.

Der Inhalt der subjektiven Leistungsakte wird in dem Entwurf nicht im einzelnen genannt, sondern es wird nur ausgeführt, daß alle nicht für die objektive Leistungsakte bestimmten Unterlagen in die subjektive Leistungsakte gehören. Sie soll insbesondere den internen Beratungsprozeß dokumentieren. Daher enthält sie z. B. Vermerke über Gespräche mit Betroffenen und Unterlagen, die nicht anderen Stellen zugänglich gemacht werden sollen. Sie ist also das interne Arbeitsmittel des Sozialarbeiters. Hingegen soll die objektive Leistungsakte das Verwaltungsverfahren auch nach außen dokumentieren, indem etwa die Akte oder einzelne Teile an andere Stellen wie Gerichte abgegeben werden.

Dieser Ansatz des Entwurfs entsprach den Empfehlungen des Deutschen Vereins für öffentliche und private Fürsorge „Aktenführung in der kommunalen Sozialverwaltung“ und dem Modell in der Arbeitsanweisung „Aktenführung in den sozialen Diensten der Stadt Essen“; ähnliche Vorschläge finden sich in der Literatur. Hintergrund ist der Gedanke, daß in der Arbeit des ASD der Schutz des Vertrauensverhältnisses zwischen Sozialarbeiter und Klient eine solche Aktenführung erforderlich macht. Allerdings berücksichtigte der Entwurf noch nicht ausreichend die in § 63 Abs. 2 Satz 2 SGB VIII geforderte getrennte Aktenführung für Leistungen und andere Aufgaben.

In der Muster-Arbeitsanweisung der Stadt Essen wird, insoweit abweichend von dem mir vorgelegten Entwurf, eine Aufteilung der Verfahrensakten für das Verwaltungsverfahren und für das gerichtliche Verfahren vorgeschlagen. Eine Trennung ist ebenfalls erforderlich, wenn nur ein Verwaltungsverfahren vorliegt, aber z. B. eine Inobhutnahme verknüpft wird mit einer Leistung nach den § 27 ff. SGB VIII (wenn nicht die Zusammenführung zur Erfüllung der jeweiligen Aufgabe erforderlich ist).

Besonders schwierig ist es, in der Aktenführung den besonderen Vertrauensschutz des § 65 SGB VIII, § 203 Abs. 1 StGB zu verwirklichen, der auch innerhalb des Jugendamts zu beachten ist. Zunächst ist allerdings zu prüfen, ob diese besondere Schweigepflicht besteht und ob der Betroffene nicht z. B. in die Weitergabe des von ihm Offenbarten eingewilligt hat oder aufgrund einer Rechtsgüterabwägung eine Offenbarung erlaubt ist. Wenn die Schweigepflicht besteht, ist allerdings fraglich, ob solche Informationen in die subjektive Akte gehören. Ihre Aufgabe ist es, wie ausgeführt, den Beratungsprozeß zu dokumentieren. Daher ist es unter Umständen erforderlich, sie z. B. bei dienstrechtlichen Auseinandersetzungen dem Fachvorgesetzten vorzulegen. Aus diesem Grunde ist zu überlegen, ob man, den Empfehlungen des Deutschen Vereins folgend, als dritte Kategorie den „Aufschrieb“ einführt. Er enthält nach diesen Vorstellungen solche der besonderen Schweigepflicht unterliegenden Informationen, aber auch nur dem persönlichen Gebrauch des Sozialarbeiters dienenden Notizen über Eindrücke, Vermutungen, Überlegungen, weiterhin vorläufige Entwürfe, nicht ausgewertete Informationen und andere Aufzeichnungen, die nicht in der subjektiven Leistungsakte aufbewahrt werden sollen.

Akten oder Aktenteile müssen unter Umständen innerhalb des Jugendamts oder an Stellen außerhalb des Jugendamtes, wie Gerichte, weitergegeben werden. Eine Weitergabe der Unterlagen *außerhalb* des Jugendamtes ist eine Übermittlung, die nur

zulässig ist, wenn die Voraussetzungen der §§ 64, 65 SGB VIII, §§ 67 d bis 78 SGB X vorliegen. Besonders problematisch ist in diesem Zusammenhang die Regelung des § 76 SGB X.

Bei einer Weitergabe *innerhalb* des Jugendamtes ist fraglich, ob es sich ebenfalls um eine Übermittlung von Daten, oder, weil man das Jugendamt als eine einzige Stelle betrachtet, um eine Nutzung von Daten handelt. Auch wenn man eine Nutzung annimmt, dürfen die Unterlagen nicht beliebig weitergeben werden. Nach § 35 Abs. 1 Satz 2 SGB I umfaßt die Wahrung des Sozialgeheimisses die Verpflichtung, auch innerhalb des Leistungsträgers sicherzustellen, daß Sozialdaten nur Befugten zugänglich sind oder nur an diese weitergegeben werden. Daher müssen die Voraussetzungen einer Nutzung gemäß § 64 Abs. 1 SGB VIII, § 67 c SGB X erfüllt sein. Von besonderer Bedeutung sind die bereits oben erwähnten besonderen Schweigepflichten des § 65 SGB VIII, § 203 Abs. 1 StGB.

Eine Herausgabe kompletter Akten an andere Behörden ist in der Regel nicht erforderlich und damit unzulässig. Bereits beim Aufbau der objektiven Leistungsakte sollte daher berücksichtigt werden, wie möglichst problemlos eine gute Aufteilung erreicht werden kann.

Die Akte ist nicht nur Arbeitsmittel der Behörde. Sie ist auch Grundlage, elementaren Rechten des Betroffenen Geltung zu verschaffen, nämlich dem Recht auf Akteneinsicht nach § 25 SGB X und dem Auskunftsrecht des § 67 SGB VIII. Die Aktenführung ist so zu organisieren, daß der Betroffene diese Rechte wahrnehmen kann und zudem die Akteneinsicht für die Behörde mit einem möglichst geringen organisatorischen Aufwand verbunden ist.

Gemäß § 84 Abs. 2 Satz 2 SGB X sind Sozialdaten zu löschen, wenn ihre Kenntnis für die speichernde Stelle für die Erfüllung ihrer Aufgaben nicht mehr erforderlich ist und kein Grund zu der Annahme besteht, daß durch die Löschung schutzwürdige Interessen des Betroffenen beeinträchtigt werden. Unter den Voraussetzungen des Abs. 3 tritt an die Stelle einer Löschung eine Sperrung der Daten. Unklar ist zur Zeit noch, ob das Jugendamt vor einer Löschung die Unterlagen dem städtischen Archiv anzubieten hat. Diese Frage werde ich mit dem für das Archivwesen zuständigen Sächsischen Staatsministerium des Innern klären.

Zu beachten ist schließlich § 78 a Satz 1 SGB X. Diese Vorschrift ordnet an, daß das Jugendamt die technischen und organisatorischen Maßnahmen einschließlich des Erlasses einer Dienstanweisung zu treffen hat, die erforderlich sind, um die Anforderung des Sozialgesetzbuches zu erfüllen. Nach Satz 2 sind Maßnahmen nicht erforderlich, wenn ihr Aufwand in keinem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht. In der Anlage zu dieser Vorschrift werden Maßnahmen genannt, die zur Erreichung dieses Ziels zu treffen sind. Sie beziehen sich zwar nur auf die automatisierte Datenverarbeitung. Die Forderung nach technischen und organisatorischen Maßnahmen zu Gewährleistung des Sozialdatenschutzes gilt allerdings auch für die Führung von Akten. Die Anlage enthält daher auch Anhaltspunkte für eine Sicherung von Akten.

Das Jugendamt wird den Entwurf gemeinsam mit mir überarbeiten. Wie die genannten gesetzlichen Anforderungen umzusetzen sind, kann nur in der Praxis entschieden werden. Bei vielen Mitarbeitern wird die Befürchtung entstehen, daß eine gesetzeskonforme Aktenführung nicht mit den Anforderungen der Praxis zu vereinbaren ist. In der Tat wird die Anwendung des Gesetzes in einigen Bereichen zu einer Komplizierung des Verfahrens führen, etwa bei der Aktentrennung. Andererseits können gerade die gesetzlichen Regelungen zu einer übersichtlichen, straffen Aktenführung und damit zur Arbeitserleichterung beitragen.

### 10.2.2 Datenschutz in örtlichen Betreuungsbehörden

Ist eine volljährige Person nicht (mehr) in der Lage, ihre persönlichen Angelegenheiten zu erledigen, weil sie psychisch krank oder körperlich, seelisch oder geistig behindert ist, bestellt das Vormundschaftsgericht für sie einen Betreuer und bestimmt den Aufgabenkreis, in welchem der Betreuer für die betreute Person handelt (§§ 1897 ff. BGB). Örtliche Betreuungsbehörden unterstützen sowohl das Gericht bei der Feststellung des Sachverhalts und bei der Gewinnung geeigneter Betreuer (§ 8 BtBG) als auch die Betreuer bei der Durchführung ihrer Aufgabe. Für diese Zwecke führen sie Akten über Betreuer und Betreute. Zum Umgang mit diesen Akten sind mir eine Reihe von Fragen gestellt worden, die anhand des Sächsischen Datenschutzgesetzes zu beantworten waren, weil in keiner bereichsspezifischen Rechtsvorschrift (z. B. Betreuungsbehördengesetz, Bürgerliches Gesetzbuch) der datenschutzgerechte Umgang mit personenbezogenen Daten von Betreuern und Betreuten geregelt ist.

Folgendes war zu klären:

1. *Aufbewahrungsfrist für Betreutenakten und Aktenvernichtung*
   Da es keine gesetzliche Aufbewahrungsfrist für Betreutenakten gibt, konnte ich lediglich empfehlen, die Frist anhand der praktischen Bedürfnisse festzulegen und dabei zu beachten, daß gemäß § 19 Abs. 2 SächsDSG die gesamte Akte zu löschen (vernichten) ist, wenn sie zur Aufgabenerfüllung nicht mehr erforderlich ist. Danach darf die Aufbewahrungsfrist nur den Zeitraum umfassen, in dem erfahrungsgemäß noch auf abgeschlossene Betreuungsfälle zurückgegriffen werden muß.

   Nach Ablauf der Aufbewahrungsfrist dürfen die Akten grundsätzlich gelöscht werden. Zuvor ist zweierlei zu beachten:

- Die Löschung muß unterbleiben, wenn Grund zu der Annahme besteht, daß dadurch schutzwürdige Interessen des Betroffenen beeinträchtigt würden (§ 19 Abs. 4 Nr. 1 SächsDSG). Diese können in möglichen Haftungsansprüchen gegen Betreuer liegen (Einzelbetreuer § 1833 BGB; Betreuungsvereine §§ 30, 31 BGB; Betreuungsbehörden §§ 31, 89, 839 BGB), die unter Umständen erst nach 30 Jahren verjähren (§ 852 BGB). Möglicherweise kommt allein aus diesem Grund eine generelle Aufbewahrungsfrist von 30 Jahren in Betracht.

Sind schutzwürdige Interessen im Einzelfall zu beachten, muß die betreffende Akte bis zum Wegfall der Gründe vorgehalten werden. Für diese Zeit sind die Daten gemäß § 20 SächsDSG zu sperren.

- Die zur Löschung vorgesehenen Akten sind von den kommunalen Betreuungsbehörden dem nach der Archivsatzung zuständigen Archiv zur Übernahme anzubieten. Soweit Landesbehörden als Betreuungsbehörden tätig sind, haben sie die Akten dem zuständigen staatlichen Archiv anzubieten (§ 19 Abs. 1 Nr. 2 und Abs. 3 SächsDSG i. V. m. dem Sächsischen Archivgesetz). Erst wenn die Übernahme abgelehnt oder die Äußerungsfrist des Archivs verstrichen ist, dürfen die Akten vernichtet werden.

  Ist eine Akte zu löschen und hat der *Betreute* sein Interesse an der Aushändigung bekundet, so bestehen keine Bedenken, ihm die Akte in dem Umfang auszuhändigen, in dem er nach § 17 SächsDSG ein Einsichtsrecht hätte. Ebenso bestehen keine Bedenken, anderen Personen Unterlagen aus der Akte zur Verfügung zu stellen, soweit sie nach § 17 SächsDSG einen Auskunftsanspruch hätten. Es sind also insbesondere die Einschränkungen des Absatzes 5 zu beachten. Ein Rechtsanspruch auf Aushändigung besteht in keinem Fall, da die Verfügungsberechtigung bei der Behörde als Eigentümerin liegt.

2. *Einsicht in Betreutenakten*

2.1 Nach § 17 Abs. 3 SächsDSG hat der Betreute das Recht, die über ihn geführte Akte einzusehen. Dieses Recht darf nur aus den in § 17 Abs. 5 SächsDSG genannten Gründen eingeschränkt werden. Einzelheiten dazu finden sich in meiner Bekanntmachung vom 1. Juli 1994 (SächsABl. S. 982). Zu ergänzen bleibt, daß nach herrschender Meinung einem Betroffenen im Rahmen der Akteneinsicht auf Wunsch Kopien von Unterlagen zu überlassen sind.

Grundsätzlich kann der Betreute Dritte bevollmächtigen, die Akteneinsicht an seiner Stelle wahrzunehmen. Kann der Betreute z. B. wegen einer geistigen Schwäche keine Vollmacht erteilen, bestehen aus meiner Sicht keine Bedenken, dem Betreuer Akteneinsicht zu gewähren, wenn dies von seinem Aufgabenkreis umfaßt ist. Andernfalls wäre zu prüfen, ob eine Aufgabenerweiterung in Betracht kommt.

2.2 Enthält die Betreutenakte Daten über Dritte (z. B. Angehörige, Freunde), ist diesen Personen auf Antrag gemäß § 17 Abs. 1 *Auskunft* über die zu ihrer Person gespeicherten Daten zu erteilen. Bei der Auskunftserteilung sind die Einschränkungen des § 17 Abs. 5 SächsDSG zu beachten.

2.3 Wünscht eine Person oder eine öffentliche oder nicht-öffentliche Stelle Auskunft über den Betreuten, so ist die Zulässigkeit der Datenübermittlung zu prüfen (§§ 13, 14, 15 SächsDSG). Ggf. ist die Einwilligung des Betreuten bzw. Betreuers in der von § 4 Abs. 2 und 3 SächsDSG vorgeschriebenen Form einzuholen.

3. *Öffnung der vom Vormundschaftsgericht zurückgesandten Betreutenakten*
   Ist die Betreuungsbehörde Teil einer Organisationseinheit mit einer zentralen Poststelle, so ist sicherzustellen, daß bei Rückgabe der Betreutenakten die Sendung verschlossen in die Hände des zuständigen Bearbeiters gelangt. Dies kann dadurch erreicht werden, daß in der Anschrift der Name des zuständigen Bearbeiters, ggf. mit dem Zusatz „o. V. i. A." (Abkürzung für „oder Vertreter im Amt"), *vor* den Behördennamen gesetzt wird. Die genannte Person bzw. ihr Vertreter ist in diesem Fall der Adressat und hat das Recht, die Sendung ungeöffnet zu erhalten. Eine andere Möglichkeit besteht darin, den Namen mit dem Zusatz „persönlich" oder „vertraulich" zu versehen. Auch in diesem Fall darf die Sendung nicht in der zentralen Poststelle geöffnet werden, selbst wenn der Behördenname an erster Stelle steht. Der Zusatz „z. Hd." ist dagegen lediglich ein Zuordnungs- bzw. Verteilerhinweis des Absenders; eine so adressierte Sendung wird regelmäßig in der zentralen Poststelle einer Behörde geöffnet. Falls einem Vormundschaftsgericht diese Behördenpraxis unbekannt sein sollte, wäre es darauf hinzuweisen.

   Fragen der Adressierung von Behördenbriefen und der Postverteilung in Behörden habe ich in 3/14.8 behandelt (s. auch 5.5.9).

### 10.2.3 Befreiung von der Rundfunkgebührenpflicht

Bereits in 4/10.2.12 habe ich ausführlich begründet, daß das gegenwärtige Verfahren der Rundfunkgebührenbefreiung eine Reihe datenschutzrechtlicher Fragen aufwirft. Dazu gehört insbesondere, daß zwei Stellen, nämlich das Sozialamt und der Mitteldeutsche Rundfunk (MDR) zum Teil sensible Daten wie Angaben zu Behinderungen und zu Einkommensverhältnissen verarbeiten, obwohl die Beteiligung zweier Stellen nicht erforderlich ist. Daher haben die Landesbeauftragten für den Datenschutz von Sachsen-Anhalt, Thüringen und Sachsen eine Änderung des Verfahrens dahingehend gefordert, daß die Sozialämter die Entscheidung über die Rundfunkgebührenbefreiung treffen.

Eine solche Änderung setzt eine Novellierung der für die Bundesländer geltenden jeweiligen Rundfunkgebührenbefreiungsverordnungen voraus. In einigen Bundesländern, etwa in Nordrhein-Westfalen, entscheiden bereits jetzt die Sozialämter über den Antrag. Der Entwurf einer neuen Rundfunkgebührenbefreiungsverordnung, der von der „AG Rundfunkgebührenrecht ARD/ZDF" am 17.5.1996 beschlossen worden war, behielt jedoch das bisherige Verfahren im wesentlichen bei. Auch die Rundfunkreferenten der „MDR-Länder" haben sich bisher dem Vorschlag der drei Landesdatenschutzbeauftragten nicht angeschlossen.

Dennoch werden die Landesdatenschutzbeauftragten weiterhin auf eine grundlegende Veränderung des Verfahrens drängen. Falls sie nicht bald zu erreichen ist, werden sie zumindest die in 4/10.2.12 genannten Detailprobleme aufgreifen und eine Lösung suchen. Zu diesen Detailproblemen gehört die Frage, ob das Sozialamt Daten im Auftrag des MDR verarbeitet. Die weitreichenden Prüfungsbefugnisse des Sozialamts sprechen dafür, daß es sich nicht um eine Auftragsdatenverarbeitung, sondern

eine Funktionsübertragung handelt. Zu klären ist ebenfalls nach wie vor, welche Nachweise der MDR für die Befreiung verlangen kann und wie die GEZ beteiligt ist; weiterhin das Problem der Datenerhebung bei Dritten.

### 10.2.4 Mitteilungen an Finanzämter durch Sozialversicherungsträger

Seit 1996 diskutieren die Sozialversicherungsträger, das Bundesministerium der Finanzen (BMF) sowie der Bundesbeauftragte und die Landesbeauftragten für den Datenschutz, ob Zahlungen von Sozialversicherungsträgern an Leistungserbringer und ehrenamtlich Tätige dem Sozialgeheimnis unterliegen. In diesem Fall wären die Zahlungen den Finanzämtern nicht mitzuteilen. Die Meinungen gehen nach wie vor auseinander. Im Zuge der Diskussion ist bisher nicht untersucht worden, ob die Mitteilungen möglicherweise nach anderen Vorschriften der Mitteilungsverordnung unabhängig von einer Beurteilung der Zahlungen als Sozialdaten unterbleiben können.

Ich bin dieser Frage nachgegangen und zu folgendem Ergebnis gekommen:

1. *Zahlungen an Leistungserbringer*
   Aus Sicht der Finanzverwaltung stellen Banküberweisungen auf ein Geschäftskonto sicher, daß die eingegangenen Zahlungen von den Steuerpflichtigen als Betriebseinnahmen angegeben werden. Die Überweisungen erscheinen auf den Kontoauszügen und ermöglichen den Finanzämtern bei Prüfungen eine zuverlässige Kontrolle. Aus diesem Grunde besteht gemäß § 2 Satz 1 MV *keine Anzeigepflicht, wenn die Zahlungen für Lieferungen und Leistungen durch Banküberweisung auf ein Geschäftskonto vorgenommen* werden. Erfolgen die Zahlungen dagegen auf ein anderes als das Geschäftskonto oder auf einem der in § 2 Satz 1 Nr. 1 MV genannten „unüblichen“ Zahlungswege (bar, postbar, Scheck, Zahlungsanweisung zur Verrechnung, Aufrechnung), hat die Finanzverwaltung diese Kontrollmöglichkeit nicht mehr; deshalb sind solche Zahlungen mitteilungspflichtig.

   Ärzte, Apotheker, Krankenhäuser usw. erbringen Lieferungen oder Leistungen im Sinne von § 2 MV und unterhalten Geschäftskonten. Sie stellen den überwiegenden Teil der Zahlungsempfänger. Wie ich erfahren konnte, sind Zahlungen auf den oben genannten unüblichen Zahlungswegen große Ausnahmen. Der übliche Zahlungsweg ist die Banküberweisung in einem automatisierten Abrechnungsverfahren auf das vom Leistungserbringer für diese Zwecke angegebene Konto. Daß dies sein Privatkonto oder das Konto eines Dritten ist, wird von kompetenter Stelle für praxisfremd gehalten.

   Wie ich aus der Finanzverwaltung erfahren habe, verwechseln etliche Behörden die „Zahlungsanweisung zur Verrechnung“ mit der „Banküberweisung“, so daß immer wieder Banküberweisungen auf ein Geschäftskonto mitgeteilt werden. Bei Zahlungsanweisungen zur Verrechnung handelt es sich jedoch um ein mit erheblichen Gebühren (10 DM pro Fall) belastetes Verfahren, das die Post AG anbietet. Im Kundenauftrag übersendet sie dem Zahlungsempfänger ein scheckähnliches

Dokument, das dieser in bar einlösen oder einem beliebigen Konto gutschreiben lassen kann. Nach Einlösung wird das Konto des Auftraggebers in entsprechender Höhe belastet.
Dieses unübliche Verfahren unterliegt allerdings der Mitteilungspflicht.

2. *Zahlungen an ehrenamtlich Tätige*
Bei ehrenamtlich Tätigen befreit im Gegensatz zu den Leistungserbringern allein die Zahlung durch Banküberweisung nicht von der Mitteilungspflicht.

Gemäß § 41 SGB V erhalten ehrenamtlich Tätige Entschädigungen. Zu der Frage, ob es sich bei diesen Entschädigungen um Zahlungen für *Leistungen* im Sinne von § 2 MV handelt, vertreten die Spitzenverbände der Krankenkassen und das BMF unterschiedliche Auffassungen. Ich neige der Auffassung des BMF zu, wonach *jedes* Tun, Dulden oder Unterlassen eine Leistung darstellt. Eine solche Auslegung wäre systematisch richtig, weil die Mitteilungsverordnung eine steuerrechtliche Vorschrift ist und das Steuerrecht bei den verschiedenen Steuerarten an diesen Leistungsbegriff anknüpft.

Weil die ehrenamtliche Tätigkeit eine Leistung gemäß § 2 MV darstellt, ergibt sich im Regelfall eine Mitteilungspflicht nach Satz 2 dieser Vorschrift: Zum einen werden nur in wenigen Fällen ehrenamtlicher Tätigkeit die Zahlungen auf ein Geschäftskonto erfolgen - entweder, weil ein solches nicht vorhanden ist (wohl in der Mehrzahl) oder weil Buchführungsvorschriften (z. B. Kontenklarheit bei Gewerbetreibenden) die Vereinnahmung betriebsfremder Zahlungen auf einem Geschäftskonto nicht zulassen. Zum anderen können die in Betracht kommenden ehrenamtlichen Tätigkeiten schon ihrer Art nach nicht im Rahmen einer gewerblichen, land- und forstwirtschaftlichen oder freiberuflichen Tätigkeit erbracht werden (s. §§ 13, 15, 18 Einkommensteuergesetz). Selbst wenn dies denkbar sein sollte, wäre für den Sozialleistungsträger kaum erkennbar, ob es sich um die Haupttätigkeit des Zahlungsempfängers handelt. Aber auch dieses Problem relativiert sich mit Blick auf § 7 Abs. 2 MV, da Zahlungen von weniger als 3 000 DM pro Empfänger und Kalenderjahr nicht mitteilungspflichtig sind.

Dies habe ich den anderen Datenschutzbeauftragten mitgeteilt, um zu einer Entschärfung der weiteren Diskussion beizutragen.

### 10.2.5 Einheitliches Meldeverfahren zur Durchführung der Familienversicherung

Die Krankenkassen forderten ihre Mitglieder zu Angaben über die Krankenversicherung ihrer Angehörigen auf, und zwar rückwirkend zum 1. April 1994. Mehrere Betroffene baten mich um datenschutzrechtliche Prüfung.

Hintergrund dieser Prüfung war, daß sich die Versichertenverzeichnisse der Krankenkasse nicht auf aktuellem Stand befanden. Dies führte u. a. zu Fehlern bei der Berechnung des Risikostrukturausgleichs (durch den Risikostrukturausgleich werden gemäß § 266 Abs. 1 SGB V die finanziellen Auswirkungen von Unterschieden u. a. in

der Zahl der Familienversicherten zwischen den Krankenkassen ausgeglichen). Aufsichtsbehörden und Gerichte hatten deshalb eine Korrektur der Versichertenverzeichnisse gefordert.

Grundlage des Vorgehens der Krankenkassen war das von ihren Spitzenverbänden beschlossene „Einheitliche Meldeverfahren zur Durchführung der Familienversicherung“ vom 28. September 1993 in der Fassung vom 15. Januar 1997. Danach dient das Meldeverfahren u. a. dem Zweck, die Familienversicherten für den Risikostrukturausgleich vollständig zu erfassen und die Versichertenverzeichnisse der Krankenkassen zu aktualisieren.

Von Datenschutzbeauftragten wurde kritisiert, daß die Krankenkassen Daten für die Verzeichnisse auch dann erhoben, wenn ihnen vollständige Angaben vorlagen.

Unabhängig davon bestehen einige Einwände gegen die verwendeten Formulare. So muß nach dem Vordruck „Angaben zur Feststellung der Familienversicherung“ für Kinder ab dem 18. Lebensjahr eine Schulbescheinigung beigefügt werden. Kinder sind bis zur Vollendung des 23. Lebensjahres versichert, wenn sie nicht erwerbstätig sind, bis zur Vollendung des 25. Lebensjahres, wenn sie sich in Schul- oder Berufsausbildung befinden (§ 10 Abs. 2 Nr. 2 und 3 SGB V). Für den Zeitraum zwischen der Vollendung des 18. Lebensjahres (bis zu diesem Zeitpunkt ist das Kind ohnehin versichert) und der Vollendung des 23. Lebensjahres kommt es also nicht darauf an, ob es eine Schule oder Hochschule besucht, sondern nur darauf, ob es erwerbstätig ist. Streng genommen reicht es daher aus, wenn das Mitglied eine entsprechende Versicherung abgibt.

Hingegen fehlen im Vordruck Angaben, die der Krankenkasse die Feststellung ermöglichen, ob die weiteren Voraussetzungen vorliegen, die neben der Schul- und Berufsausbildung eine Familienversicherung des Kindes begründen, z. B. die Ableistung eines sozialen Jahres.

Die Angabe „Verwandschaftsverhältnis zum Mitglied: z. B. leibliches Kind, Stief- oder Pflegekind/Enkel“ läßt befürchten, daß sich manches Mitglied durch die Formulierung genötigt sehen wird, ein Adoptionsverhältnis offenzulegen. Das angenommene Kind ist weder ein leibliches noch ein Stief- oder Pflegekind oder ein Enkel. Durch das vorangestellte „z. B.“ wird suggeriert, daß von der Aufzählung nicht erfaßte Kindschaftsverhältnisse zu nennen sind, also in diesem Falle die Adoption.

Eine Ausforschung des Adoptionsverhältnisses verstößt gegen § 1758 BGB. Sie wird von den Krankenkassen sicherlich nicht beabsichtigt und sollte daher durch eine geänderte Formulierung vermieden werden, zumal das Kind in jedem Falle Kenntnis von der Angabe erhält, wenn es, wie vorgesehen, auf demselben Blatt unterschreibt. Abgesehen davon ist fraglich, ob eine Notwendigkeit besteht, nach der Art des Kindschaftsverhältnisses zu differenzieren, weil als Kinder auch Stiefkinder, Pflegekinder und Enkel gelten (§ 10 Abs. 4 Satz 1 SGB V). Eine Notwendigkeit zur Unterscheidung ergibt sich allenfalls bei Stiefkindern und Enkeln aus dem Tatbestandsmerkmal „die das Kind überwiegend unterhält“.

Gefragt wird bei Ehegatten und bei den Kindern nach der Art und der Gesamthöhe des Einkommens. Die Höhe des Einkommens ist jedoch nur von Bedeutung, wenn es die in § 10 Abs. 1 Nr. 5 SGB V genannten Grenzen überschreitet. Es ist also gleichgültig, ob das Kind z. B. im Jahr 1997 in den alten Bundesländern 615,- DM oder 6115,- DM verdient hat. In beiden Fällen hat es die Grenze überschritten. Demgemäß werden im Vordruck „Angaben zur Überprüfung der Familienversicherung" nur die Einkommensgrenzen genannt. Von Bedeutung ist allenfalls wegen § 10 Abs. 3 SGB V die genaue Höhe des Gesamteinkommens des Ehegatten. Hier handelt es sich jedoch um einen besonderen Fall, der entsprechend behandelt werden sollte.

Nicht erkennbar ist z. B. auch, weshalb das Gesamteinkommen eines hauptberuflich selbständig erwerbstätigen Kindes angegeben werden soll, obwohl bereits wegen der hauptberuflichen selbständigen Erwerbstätigkeit eine Familienversicherung nicht in Betracht kommt (§ 10 Abs. 1 Nr. 4 SGB V).

Die Spitzenverbände müssen also die Notwendigkeit der Angaben zu Art und Höhe des Einkommens im einzelnen begründen.

Einzuwenden ist weiterhin, daß der Datenschutzhinweis nicht die Anforderungen des § 67 a Abs. 3 SGB X erfüllt, weil der Betroffene nicht auf die Rechtsfolgen einer Verweigerung von Angaben hingewiesen wird. Nach Nr. 8 des einheitlichen Meldeverfahrens zieht die Krankenkasse die Krankenversichertenkarte ein.

Das zur Vorlage einer Schulbescheinigung und zum Datenschutzhinweis Gesagte gilt ebenfalls für den Vordruck „Angaben zur Überprüfung der Familienversicherung".

Weil die Spitzenverbände in einer Protokollnotiz zum Einheitlichen Meldeverfahren vereinbart haben, die Erfahrungen mit diesem Verfahren auszuwerten, habe ich den Bundesbeauftragten für den Datenschutz gebeten, meine Einwände den Spitzenverbänden mitzuteilen. Zu einem entsprechenden Schreiben des Bundesbeauftragten für den Datenschutz haben sie sich bisher nicht geäußert.

### 10.2.6 Anforderung von Mitgliederverzeichnissen

Ein als freier Träger der Jugendhilfe anerkannter Verein beklagte sich, das Sächsische Landesjugendamt fordere im Zusammenhang mit einem Förderantrag mittels eines Formblatts u. a. ein „aktuelles Mitgliederverzeichnis" an. In ähnlicher Weise habe das SMK telefonisch die Übersendung eines solchen Verzeichnisses verlangt.
Ich habe beide Stellen um Mitteilung gebeten, ob und aus welchen Gründen das Mitgliederverzeichnis zu den Fördervoraussetzungen gehört bzw. für die Antragsbearbeitung benötigt wird.
Das SMK teilte mir mit, in Anwendung der „Förderrichtlinie zur Gewährung von Zuwendungen im Bereich Jugendarbeit/Jugendverbandsarbeit gemäß §§ 11,12 SGB VIII" sei ein Überblick über die Mitgliedschaft von Verbänden und Vereinen bei landesweiten Zusammenschlüssen der Jugendarbeit notwendig, um die Fördervoraussetzungen zu prüfen. Die Erhebung personenbezogener Daten sei zu keiner Zeit beabsichtigt gewesen. Im Ergebnis eines klarstellenden Telefongesprächs mit

dem betroffenen Verein seien daher nur die Anzahl der natürlichen Personen, die Mitglied sind, und die Anschriften sonstiger - nicht natürlicher - Mitglieder dem SMK mitgeteilt worden. Eine in einem Einzelfall erfolgte Mitteilung personenbezogener Daten im Zusammenhang mit diesen Prüfungen sei, wie mir das SMK versicherte, gemäß § 19 Abs. 1 Nr. 1 SächsDSG gelöscht worden.
Im Zusammenhang mit dem verwendeten Formblatt habe ich zugunsten des Landesjugendamts unterstellt, daß es sich hierbei „nur“ um eine mißglückte Formulierung handelt. Gemeint war wohl nicht, wie die Begriffswahl nahelegt, ein Verzeichnis der natürlichen Personen, die Mitglieder des Vereins sind, sondern der Mitgliedsverbände oder -vereine.
Auf meinen Wunsch hat das SMK das Landesjugendamt aufgefordert, die bisherige Formulierung entsprechend zu präzisieren. Ferner habe das Landesjugendamt zu prüfen, ob aufgrund einer Fehlinterpretation möglicherweise doch personenbezogene Daten von Mitgliedern einzelner freier Träger der Jugendhilfe vorhanden sind, die gemäß §§ 19,20 SächsDSG zu löschen bzw. zu sperren sind. Das Landesjugendamt hat mir bestätigt, daß es seitdem die präzisierte Formulierung verwende.

## 10.3 Lebensmittelüberwachung und Veterinärwesen

In diesem Jahr nicht belegt.

## 10.4 Rehabilitierungsgesetze

### Zugang der Rehabilitierungsbehörde zu Stasi-Unterlagen

Unter 3/10.4 habe ich mich bereits zu allgemeineren datenschutzrechtlichen Fragen geäußert, die sich im Hinblick auf die Ausschlußtatbestände für Leistungen nach den Rehabilitierungsgesetzen (1. und 2. SED-Unrechtsbereinigungsgesetz) stellen. Unter 4/10.4.2 habe ich konkreter die Frage erörtert, unter welchen allgemeinen Voraussetzungen die Rehabilitierungsbehörde befugt ist, Daten zu Ausschlußgründen zu *erheben*. Ein Petent hatte von seiner Stasi-(Opfer-)Akte, die mehr als 300 Seiten umfaßte und einen Zeitraum von fast 25 Jahren betraf, nur wenige Blätter zugänglich gemacht, und auch nur ausgewählte Teile der zu seinen Gunsten ergangenen strafrechtlichen Rehabilitierungsentscheidung.
Der aus diesen Bruchstücken sowie zusätzlichen Angaben des Antragstellers erkennbare Lebenslauf, insbesondere auch die persönlichen Vermögensverhältnisse, wiesen in der Tat Eigentümlichkeiten auf, von denen die Tatsache, daß der Petent im Jahre 1960 aus Westdeutschland zugezogen war, noch eine der unauffälligsten war.
Die Behörde hatte daher, entsprechend den im 4. Tätigkeitsbericht a. a. O. genannten Fallgruppenbildungen mit Recht Anlaß gesehen, pflichtgemäß von Amts wegen zu ermitteln, ob einer der Ausschlußgründe erfüllt sein könnte.

Zu diesem Zweck hatte die Behörde die Bearbeitung des Antrages davon abhängig gemacht, daß der Antragsteller darin einwilligte, daß die Rehabilitierungsbehörde in die vollständige Stasi-Opfer-Akte Einsicht nahm. Dagegen wandte sich die Eingabe - im Ergebnis ohne Erfolg. Die Behörde war auf die Einwilligung des Petenten nämlich nicht angewiesen. Sie hatte Zugang zu den beim BStU verwahrten, den Antragsteller als Observierungs-Objekt betreffenden Unterlagen. Ermöglicht wird dieser Datenzugang durch Regelungen des StUG; im einzelnen:

Das StUG gibt in § 21 Abs. 1 Nr. 1 - in dem für die Aufgabenerfüllung erforderlichen Umfang - Behörden, die für die Durchführung von Rehabilitierungsverfahren zuständig sind, Zugang zu den beim BStU vorhandenen Opferakten der Antragsteller von Rehabilitierungsverfahren.

Die im strafrechtlichen Rehabilitierungsverfahren beigezogene, vom Antragsteller in Bruchstücken vorgelegte, durch die vom BStU vorgenommene Paginierung als Einheit erkennbare, von der Stasi zur Person des Antragstellers geführte Akte ist offensichtlich eine Opferakte in dem Sinne, daß der Antragsteller, wenn nicht Betroffener, dann doch zumindest Dritter im Sinne von § 21 Abs. 1 i. V. m. § 6 Abs. 3, Abs. 7 StUG ist.

§ 21 Abs. 1 StUG erlaubt sowohl die Übermittlung durch den BStU an eine Rehabilitierungsbehörde als auch die damit verbundene Erhebung der betreffenden personenbezogenen Daten durch diese Behörde und genauso auch die Nutzung dieser Daten im Rehabilitierungsverfahren, wie sich anhand der Legaldefinition in § 6 Abs. 9 StUG ergibt.

Die Nutzung war im vorliegenden Fall auch nicht durch das Verwertungsverbot des § 5 Abs. 1, §§ 21 Abs. 2 StUG eingeschränkt. Denn die Voraussetzungen der Ausnahmeregelung des § 5 Abs. 1 Satz 2 StUG waren m. E. erfüllt: Der Antragsteller hat unvollständige und deshalb unzutreffende Angaben gemacht. Denn es ist das vollständige Verhältnis, in dem der Antragsteller im Laufe der Jahre zum MfS gestanden hat, für die Beurteilung des Vorliegens eines Ausschlußgrundes von Belang.
Mit anderen Worten: Unter dem Gesichtspunkt, daß Wahrheit immer die Vollständigkeit einschließt, habe ich keine Bedenken, das Tatbestandsmerkmal „unzutreffende Angaben“ in § 5 Abs.1 Satz 2 StUG so auszulegen, daß auch die bewußt unvollständige Angabe darunter fällt.

Daß in der Regel den für das Verwaltungsverfahren nach dem zwar 2. SED-Unrechtsgesetz zuständigen Behörden gemäß § 21 Abs. 1 Nr. 1 Zugang zu Opferakten der Antragsteller zu gewähren ist (vgl. ergänzend § 19 Abs. 1 und 2 StUG), entspricht auch der Rechtsauffassung des BStU.

Daneben gab es meiner Ansicht nach noch einen anderen Weg, zumindest den Inhalt der vollständigen Stasi-Opferakte zu bekommen: Im strafgerichtlichen Verfahren nach dem StrRehaG war eine vollständige Ablichtung der Stasi-Opfer-Akte als Entscheidungsgrundlage zu den Akten genommen worden. § 25 a StrRehaG erlaubt die *‘Verarbeitung’* und *‘Nutzung’* personenbezogener Daten aus strafrechtlichen Rehabilitierungsverfahren für andere Verfahren zur Rehabilitierung - soweit für die Verfahrensdurchführung erforderlich. Damit wird die für die Durchführung des anderen Rehabilitierungsverfahrens zuständige Stelle auch zur *Erhebung* dieser Daten ermächtigt. Die Vorschrift beschränkt sich also nicht darauf, nur die Übermittlung durch das Gericht (bzw. durch die für die Folgeentscheidungen nach §§ 16 ff. StrRehaG zuständige Behörde) und außerdem die Nutzung durch die andere Rehabilitierungsbehörde, nicht aber die bewußte Entgegennahme der Information durch diese

Behörde (denn das ist Erhebung!) zu erlauben: Dies wäre eine Lücke in der Datenverarbeitungserlaubnis, welche die gesamte Vorschrift sinnlos machte.

Das Landesamt für Familie und Soziales als Rehabilitierungsbehörde nach dem 2. SED-Unrechtsbereinigungsgesetz hat sich nunmehr meiner Rechtsauffassung angeschlossen.

# 11 Landwirtschaft, Ernährung und Forsten

## § 70 Abs. 3 LwAnpG: Das Staatsministerium lenkt ein

Auf meine Auffordung unter 5/11.1, die Ergebnisse der Prüfungen nach § 70 Abs. 3 LwAnpG allen ehemaligen LPG-Mitgliedern bekanntzumachen, da dies datenschutzrechtlich geboten sei, reagierte die Staatsregierung mit Unbehagen. In ihrer Stellungnahme zum Tätigkeitsbericht monierte sie die angebliche Unerfüllbarkeit dieser Forderung aufgrund der hohen Kosten, die eine Ermittlung der LPG-Mitglieder und deren Erben verursachen würde. Nur: das hatte ich nie verlangt.
Dieser verfehlten Auslegung meiner Forderung bin ich im Innenausschuß des Sächsischen Landtages entschieden entgegengetreten. Die Art und Weise der Bekanntgabe habe ich gerade offengelassen, da diese im Ermessen des SML liegt. Eine Bekanntgabe hätte auch erfolgen können, indem öffentlich auf die Existenz eines Prüfberichtes hingewiesen worden wäre.
Der Innenausschuß reichte die Sache an den Landwirtschaftsausschuß weiter. Dieser empfahl in meinem Sinne, die Staatsregierung zu ersuchen, im Zusammenwirken mit dem Sächsischen Datenschutzbeauftragten ein Verfahren zu finden, wie und in welcher Weise die Ergebnisse einer Überprüfung nach § 70 LwAnpG den Betroffenen bekanntgemacht werden können.

Da weiterer Aufklärungsbedarf bestand, welche Prüfberichte existieren, wem sie bekanntgegeben (besser: nicht bekanntgegeben) worden sind und aus welchen Gründen von einer Veröffentlichung abgesehen wurde, habe ich im SML eine Kontrolle durchgeführt.
Diese ergab, daß in der Mehrzahl der Fälle der Prüfbericht nicht bekanntgegeben, in einigen Fällen eine Einsichtnahme sogar ausdrücklich abgelehnt wurde unter dem rechtswidrigen Hinweis darauf, das Gutachten sei im öffentlichen Interesse erstellt worden und nicht zur Verfolgung privatrechtlicher Ansprüche.
Die im Zuge der Kontrolle geführten Gespräche konnten das Staatsministerium überzeugen. Es wurde folgende Einigung getroffen:

Es werden veröffentlicht:
- die Tatsache, daß ein Gutachten zu einer bestimmten namentlich genannten LPG erstattet wurde
- wer dieses Gutachten erstattet hat
- wann dieses Gutachten erstattet wurde
- daß dieses Gutachten durch die Betroffenen eingesehen und
- gegen Aufwendungserstattung auch schriftlich abgefordert werden kann

sowie
- daß es sich um ein Gutachten nach § 70 Abs. 3 Landwirtschaftsanpassungsgesetz handelt.

Die Veröffentlichung soll stattfinden:
- in einem Aushang im zuständigen Amt für Landwirtschaft
- in den zum Amtsbezirk des zuständigen Amtes für Landwirtschaft gehörenden Mitteilungsblättern der jeweiligen Gemeinden (es muß also zunächst festgestellt werden, welche Gemeinden die ehemalige LPG-Flächen bewirtschaften)
- in der örtlichen und regionalen Presse einschließlich der ortsüblichen Anzeigenblätter (hier ist der übliche Presseverteiler des Amtes für Landwirtschaft hilfreich).

Ich habe es dem SML überlassen zu entscheiden, ob darüber hinaus spezielle Behörden (z. B. Staatsanwaltschaft oder Landwirtschaftsgericht) von den zu veröffentlichenden Tatsachen informiert werden. Selbstverständlich muß es sich dabei um Behörden handeln, die von ihren Aufgaben und Befugnissen her mit den Gutachten in Verbindung kommen.

In der Gewißheit, daß das SML seine Versprechen eingehalten hat, sehe ich die Angelegenheit als erledigt an. Diese Erledigung werde ich dem Landwirtschaftsausschuß des Sächsischen Landtages sowie dem Innenausschuß des Sächsichen Landtages zur Kenntnis geben.

# 12 Umwelt und Landesentwicklung

## 12.1 Wassergesetz und Wasserbuchverordnung

Im Herbst 1996 hat das SMU mir den Entwurf einer Wasserbuchverordnung vorgelegt. Meine dagegen vorgebrachten grundlegenden Einwendungen waren auf die damals geltende Ermächtigungsgrundlage, § 105 Abs. 1 SächsWG, gestützt und betrafen die Verteilung der Zuständigkeit für die Führung des Wasserbuches auf verschiedene Behörden sowie den geplanten Inhalt des Registers.

Im zweiten Halbjahr 1997 habe ich gegen neue Entwürfe des Ministeriums erneut Einwände - u. a. gegen den Plan einer Führung zweier paralleler, gleichlautender Register - erhoben, und ich habe Vorschläge für eine Verbesserung der Ermächtigungsgrundlage im Wassergesetz gemacht.

Das SMU hat daraufhin eine Novellierung des Sächsischen Wassergesetzes vorbereitet. Was das Wasserbuch betrifft, habe ich keine Bedenken gegen die Neuregelung des § 106 Abs. 1 Satz 1 SächsWG geltend gemacht, der nunmehr ein Jedermann-Einsichtsrecht begründet. Das SMU hätte jedoch aus Gründen der rechtsstaatlich gebotenen Normenklarheit meinem Vorschlag folgen sollen, in der Vorschrift statt „Wasserbuch“ *Wasserbuchblatt* zu schreiben. Denn nur für diesen Teil des Wasser-

buchs gilt dieses Recht, wie der Eingeweihte Satz 2 der Vorschrift i. V. m. der Begründung des Regierungsentwurfes (LT-DS 2/7974) entnehmen kann. So aber verwendet Satz 3 der Vorschrift einen anderen, nämlich weiteren Wasserbuch-Begriff als Satz 1 - solche handwerklichen Ungenauigkeiten sollte man jedenfalls nicht bewußt begehen.
Sicherer wäre es auch gewesen, wenn man dabei geblieben wäre, meiner Anregung folgend in § 106 Abs. 1 Satz 4 Einsicht nur *nach* Zustimmung statt „mit Zustimmung" zu gewähren. Denn die nachträgliche Zustimmung (Genehmigung, vgl. § 184 Abs. 1 BGB) reicht als Grundlage rechtmäßigen Handelns der Behörde nicht aus; aus gutem Grund ist im Datenschutzrecht immer nur von der *Einwilligung*, also der vorherigen Zustimmung (vgl. § 183 Satz 1 BGB), die Rede.
Leider ist man auch meinem Wunsch nicht gefolgt, in der Überschrift des neuen § 10 klar und offen auszudrücken, worum es sich rechtlich, nämlich mit Wirkung für Grundrechte, handelt: Um eine *Landesdatenbank*.

## 12.2 Problem beim Outsourcing: Funktionsübernehmer jenseits der Landesgrenzen

Eine kleinere Gemeinde hatte von einem Unternehmen, welches seine Geschäftsräume außerhalb Sachsens hat, das Angebot bekommen, im Namen und für Rechnung der Gemeinde als der Trägerin der öffentlichen Trinkwasserversorgung die dabei anfallenden Gebühren einzuziehen.
Das Unternehmen, immerhin Tochterunternehmen eines bekannten Großkonzerns, hatte, wie der Vertragsentwurf zeigte, zutreffend erkannt, daß es nicht im Wege der Datenverarbeitung im Auftrag (§ 7 SächsDSG), sondern per Funktionsübertragung, also als beauftragter Unternehmer gemäß § 2 Abs. 2 Satz 1 SächsDSG, tätig sein würde: Es wollte sich die Daten der an die Trinkwasserversorgung Angeschlossenen gemäß § 13 SächsDSG von der Gemeinde übermitteln lassen und es wollte für die rein technische Durchführung sich eines Dritten als Auftragsdatenverarbeiters (gemäß § 7 SächsDSG) bedienen.

Da sich die Geschäftsräume des zu beauftragenden Unternehmers außerhalb Sachsen befinden würden, mußte eine unmittelbare Geltung der Vorschriften des Sächsischen Datenschutzgesetzes, insbesondere auch über die Kontrolle durch den Datenschutzbeauftragten gemäß § 24 SächsDSG, ausscheiden. Die im Gesetz gerade durch die Regelung des § 2 Abs. 2 SächsDSG gewollte uneingeschränkte Anwendung des Sächsischen Datenschutzgesetzes in solchen Fällen funktionsübertragender Privatisierung konnte daher nur mit Mitteln des Zivilrechts, d. h. vertraglich, gewährleistet werden. Wenn dies in einem solchen Vertrag mit der nötigen Eindeutigkeit geschieht und insbesondere der Unternehmer sich vertraglich, soweit es um die Ausführung des Vertrages geht, der Kontrolle durch den Sächsischen Datenschutzbeauftragten unterwirft, wird man solche Vereinbarungen nicht beanstanden können.

Andererseits fragt es sich, ob das Problem damit wirklich in praktisch befriedigender Weise gelöst wäre, daß der Sächsische Datenschutzbeauftragte z. B. in Brandenburg oder in Nordrhein-Westfalen auf privatrechtlicher Grundlage Kontrollen durchführte.

Auch die Einbeziehung des dortigen, auswärtigen Landesdatenschutzbeauftragten - die man auch schon im Vertrag zusätzlich vorsehen könnte - wäre wohl eine sehr umständliche Verfahrensweise: Dieser müßte dann gebeten werden, im Wege der Amtshilfe unter Anwendung des sächsischen Rechtes zu kontrollieren.

Hier ist meines Erachtens der Bundesgesetzgeber gefordert, sich etwas einfallen zu lassen.

# 13 Wissenschaft und Kunst

## 13.1 Einführung multifunktionaler Chipkarten für Studierende und Mitarbeiter an den Hochschulen im Freistaat Sachsen

Mehrere sächsische Hochschulen erproben derzeit den Einsatz von Chipkarten mit dem Ziel, den Universitätsbetrieb sowohl für die Studenten und das Hochschulpersonal als auch für die Hochschulverwaltung effektiv und serviceorientiert zu gestalten. Nach derzeitigem Diskussionsstand sollen die Chipkarten die folgenden hochschulinternen und hochschulexternen Funktionen ermöglichen, wobei eine beinahe beliebige Erweiterung der Anwendungsbereiche denkbar ist:

Funktionen innerhalb der Hochschule:
- *Ausweisfunktion* (hochschulinterne Identifikation),
- *Kontrollfunktion* (Prüfung von Zugangs- bzw. Nutzungsberechtigungen für Räume und Hochschuleinrichtungen),
- *Zahlungsfunktion* (Begleichung von Gebühren im Rahmen des Hochschulbetriebs mittels wiederaufladbarer Wertmarkenzähler, z. B. für Fotokopierbereich),
- *Studentenverwaltung* (Immatrikulation, Exmatrikulation, Ausdruck von Bescheinigungen, Rückmeldung, Studieninformationen etc. durch Interaktion des Karteninhabers),
- hochschuleigene Bibliotheksverwaltung,
- elektronische Unterschrift.

Funktionen außerhalb der Hochschule:
- *Ausweisfunktion* (hochschulexterne Identifikation),
- *Zahlungsfunktion* (z. B. bei Inanspruchnahme privater oder öffentlicher Einrichtungen wie Bäder, Kinos, Theater, öffentliche Verkehrsmittel, ggf. in Verbindung mit Vergünstigungen für Studenten),
- *Hochschulwechsel*,
- *Nutzung externer (Hochschul-) Bibliotheken*,
- *Inanspruchnahme von Leistungen des Studentenwerks* (z. B. Mensa-Nutzung)
- *elektronische Unterschrift*.

Das SMWK hat mich gebeten zu prüfen, ob und inwieweit der Einsatz hochschuleigener Chipkarten mit geltendem Datenschutzrecht vereinbar ist. Ich bin zu folgendem Ergebnis gekommen.

1 *Allgemeines zur Rechtslage*

1.1 Der Verwendung der Chipkarte im Sinne des Verarbeitungsmediums „Chipkarte“ stehen weder das Sächsische Hochschulgesetz noch das Sächsische Datenschutzgesetz entgegen. Die Frage, ob Artikel 20 und die Erwägungsgründe Nr. 53 und 54 der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24.10.95 (Amtsblatt der Europäischen Gemeinschaften Nr. L 282/45) für den Chipkarteneinsatz einschlägig sind und Eingang in diese Betrachtungen finden müssen, bedarf derzeit keiner Antwort, weil die Richtlinie noch in nationales und regionales (sächsisches) Recht umzusetzen ist.

1.2 Ob die Hochschulen aufgrund ihres Selbstverwaltungs- und Organisationsrechts Chipkarten als Pflichtkarten einführen dürfen, ist für die datenschutzrechtliche Beurteilung von besonderer Bedeutung. Eine Pflichtkarte bedarf einer normenklaren speziellen Rechtsgrundlage, die es bislang nicht gibt.

2 *Rechtslage beim hochschulinternen Einsatz von Chipkarten*

Bei der datenschutzrechtlichen Bewertung muß zwischen der Verarbeitung von Studierenden- und Mitarbeiterdaten differenziert werden, weil für jede Personengruppe andere Rechtsvorschriften gelten.

2.1 Verarbeitung von Studierendendaten

Grundlagen für die Datenverarbeitung sind § 135 Abs. 1 und 2 SHG und die Sächsische Studentendatenverordnung. Danach dürfen von der Hochschule auf der Chipkarte nur personenbezogene Daten gespeichert werden, die für die in § 135 Abs. 1 SHG genannten Zwecke *erforderlich* sind. Wegen der beispielhaften Aufzählung sind dies letztlich alle Daten, die von der Hochschule zu ihrer gesetzlichen Aufgabenerfüllung benötigt werden. Das bedeutet für jede einzelne Funktion, daß sie mit § 135 Abs. 1 SHG vereinbar sein muß. Diese Voraussetzung erfüllen die oben genannten Funktionen:

2.1.1 Die *Ausweisfunktion* der Chipkarte hat eine „doppelte Qualität“. Sie soll sowohl die visuelle als auch die automatisierte Identifikation des Karteninhabers ermöglichen. Selbst wenn die auf der Chipkarte sichtbaren Daten mit den für das Auge unsichtbaren Daten identisch sind, kommt der automatisierten Ausweisfunktion eine andere „Qualität“ zu als der visuellen, insbesondere dann, wenn sich unmittelbar an den Lesevorgang weitere automatisierte Datenverarbeitungsvorgänge anschließen. Die Studentendatenverordnung, die in § 7 abschließend aufzählt, welche Daten der Studentenausweis enthalten darf, berücksichtigt diese doppelte Qualität bisher nicht.

2.1.2 Gegen die Verwendung der Chipkarte im Rahmen der *hochschuleigenen Bibliotheksverwaltung* und einer damit ggf. verbundenen weitergehenden Verarbeitung für Zwecke der allgemeinen Studentenverwaltung (z. B. keine Exmatrikulation vor Rückgabe ausgeliehener Werke) bestehen keine

datenschutzrechtlichen Bedenken, weil dies der Zweckbestimmung von § 135 Abs. 1 SHG entspricht.

2.1.3 Soweit im Zusammenhang mit der *Zahlungsfunktion* keine personenbezogenen Daten verarbeitet werden, handelt es sich um einen datenschutzrechtlich nicht relevanten Vorgang. Verarbeitet die Hochschule aber Zahlungsdaten, die einen Personenbezug erlauben, ist dies nur im Rahmen von § 135 Abs. 1 und 2 SHG zulässig. Bei der Konzeption ist insbesondere die Zulässigkeit notwendiger Datenübermittlungen (z. B. an Kreditinstitute oder eine Clearingstelle) zu prüfen. Die gängigen Bargeld-Chipkarten hinterlassen detailierte Datenspuren. Dies müßte vermieden werden.

2.1.4 Alle *weitere Funktionen*, die oben aufgeführt sind, dürften zulässig sein.

2.1.5 Für *zukünftige Funktionen* gilt, daß sie nur dann zulässig sind und eingeführt werden dürfen, wenn sie sich in dem vom Hochschulgesetz vorgegebenen Rahmen bewegen (s. u.) Funktionen, die nicht der gesetzlichen Aufgabe entsprechen, sind auch auf freiwilliger Basis unzulässig, weil eine öffentliche Stelle ihre gesetzliche Aufgabe nicht mit Hilfe der Einwilligung erweitern darf (Vorbehalt des Gesetzes).

2.2 Verarbeitung von Mitarbeiterdaten

Eine spezialgesetzliche Vorschrift, welche die Verarbeitung personenbezogener *Mitarbeiterdaten* für Zwecke der hochschulinternen Organisation oder allgemeinen Personalverwaltung regelt, enthält das Sächsische Hochschulgesetz nicht, so daß insoweit das Sächsische Beamtengesetz, die Tarifverträge und subsidiär das Sächsische Datenschutzgesetz Anwendung finden. Demnach dürfen Chipkarten nur aufgrund einer entsprechenden Dienstvereinbarung verwendet werden.

3 *Rechtslage bei der Verwendung von Chipkarten außerhalb der Hochschule*

3.1 Soweit die Chipkarte eine visuelle Ausweisfunktion erfüllt, ergeben sich keine Unterschiede zum herkömmlichen Studentenausweis.

3.2 Die Verwendung der Chipkarte außerhalb des Organisationsbereichs einer Hochschule setzt voraus, daß die Hochschule der externen Stelle zumindest eine Leseberechtigung einräumt. Derzeit existiert kein Gesetz, das die Rechtevergabe einschränkt oder einer Zweckbestimmung unterwirft. Die Hochschule könnte damit grundsätzlich jeder externen Stelle den Zugriff auf die Chipkarte und damit auf die dort gespeicherten personenbezogenen Daten gestatten, sofern der Student das will.

3.3 Die Frage, in welchem Umfang eine Hochschule Schreib- oder Leserechte vergeben darf, berührt nicht die Frage, in welchen Umfang die lesende Stelle zur Datenerhebung berechtigt ist.

3.3.1 Handelt es sich um eine öffentliche Stelle des Freistaats Sachsen (z. B. eine andere Hochschule, Landes- und Universitätsbibliothek Dresden, Studentenwerk), hat sie die für sie geltenden Datenschutzbestimmungen zu beachten. Greift sie auf personenbezogene Daten zu, darf sie das nur, soweit die geltenden Datenschutzbestimmungen (bereichsspezifische Rechtsvorschriften bzw. Sächsisches Datenschutzgesetz) es erlauben. Die öffentliche Stelle darf also von der Chipkarte keine Daten erheben, die sie zur Durchführung ihrer gesetzlichen Aufgabe nicht benötigt, und keine Funktionen ausführen, die mit ihrer gesetzlichen Aufgabe nicht zu vereinbaren sind. Die kartenausgebende Hochschule hat gesetzlich weder das Recht noch die Pflicht, dies zu prüfen.

3.4 Der Zugriff auf Daten ohne Personenbezug (z. B. Gültigkeitsdatum) unterliegt keinen Beschränkungen.

3.5 Ist die lesende Stelle eine nicht-öffentliche Stelle (privater Dritter), hat sie die Vorschriften des Bundesdatenschutzgesetzes zu beachten.

4 *Datensicherheit*
Einzelheiten zu den Anforderungen an die Datensicherheit beim Einsatz von Chipkarten finden sich unter 5/14.7.

## 13.2 Allgemeine Rahmenbenutzungsordnung für die staatlichen Bibliotheken im Freistaat Sachsen (ARBOS)

Das SMWK hat mich gebeten, den Entwurf der Rahmenbenutzungsordnung zu prüfen. Dies habe ich getan. Meine ergänzenden Hinweise wurden weitgehend berücksichtigt.

So sind z. B. die Regelungen zum Datenschutz so weit konkretisiert worden, wie es für eine Benutzungsordnung sinnvoll ist, die den Rahmen für so unterschiedlich organisierte Bibliotheken vorgibt wie die *Sächsische Landesbibliothek - Staats- und Universitätsbibliothek Dresden*, die Bibliotheken der Hochschulen, der Berufsakademie Sachsen und der Museen im Geschäftsbereich des SMWK. Außerdem wurde hervorgehoben, daß Auskünfte über den Besteller oder Entleiher eines bestimmten Werks nicht ohne dessen schriftliche Einwilligung gegeben werden dürfen und nur im Ausnahmefall von der Schriftform abgesehen werden darf.

## 13.3 Beanstandung eines Kulturraums; zur Wirksamkeit von Einwilligungserklärungen

In 5/13 hatte ich über einen Kulturraum berichtet, der einen Ablehnungsbescheid über beantragte Fördermittel für eine Musikveranstaltung per „Verteiler“ drei nicht am Verwaltungsverfahren beteiligten Stellen übersandt hatte. Die Begründung im Ablehnungsbescheid enthielt Betrugsvorwürfe gegen den Antragsteller, einen eingetragenen Verein. Da eingetragene Vereine als juristische Personen des privaten Rechts nicht unter das Sächsische Datenschutzgesetz fallen, bestand das Kernproblem in der Frage, ob durch die Bescheidübersendung personenbezogene Datenübermittelt wur-

den und damit das durch Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG ge-schützte Persönlichkeitsrecht einer natürlichen Person verletzt worden ist. 0

Dies habe ich im vorliegenden Fall bejaht und eine *Beanstandung* ausgesprochen, und zwar aus folgenden Gründen:

Betrugs- bzw. Täuschungsvorwürfe können sich nicht gegen eine juristische Person richten, da juristische Personen keine Betrugs- und Täuschungshandlungen begehen können, sondern nur gegen die für sie handelnde(n) Person(en). Bei einem eingetragenen Verein ist dies gemäß § 26 Abs. 2 BGB der Vorstand, der den Verein gerichtlich und außergerichtlich vertritt und die Stellung eines gesetzlichen Vertreters hat. Über das Vereinsregister ist er namentlich bestimmbar.

Hier hatte der Vorstand im Vorfeld der geplanten Musikveranstaltung vorbereitende Gespräche und Vertragsverhandlungen mit zwei der Stellen geführt, denen später die Mehrfertigungen des Ablehnungsbescheids zugingen. Offenbar sollten sie eine Warnfunktion erfüllen (ebenso eine dritte an das Regierungspräsidium gesandte Mehrfertigung). Zumindest diese beiden Stellen konnten - und haben es vermutlich getan - die im Bescheid enthaltenen Anschuldigungen dem Betroffenen zuordnen, der ihnen gegenüber den Verein vertreten hat. Damit sind personenbezogene Daten übermittelt worden, die ihrem Inhalt nach geeignet sind, das Ansehen dieser Person herabzusetzen oder sogar zu beschädigen, schon weil sich in der Bescheidbegründung keine Auseinandersetzung mit einer Gegenäußerung (Anhörung) des Vereins findet. Diese hätte gemäß § 28 VwVfG bei der beabsichtigten Versagung der beantragten Vergünstigung erfolgen müssen (Obermeyer, Kommentar zum Verwaltungsverfahrensgesetz, 2. Aufl., § 28, Rdnr. 12).

Der Kulturraum hat die Übersendung von Mehrfertigungen des Ablehnungsbescheids damit gerechtfertigt, die Empfänger seien Verfahrensbeteiligte gemäß § 13 Abs. 2 VwVfG. Dies waren sie eindeutig nicht, weil die Entscheidung ihre rechtlichen Interessen nicht berührte.

Der Kulturraum legte mir eine Erklärung des Vereins vor, mit der sich dieser einverstanden erklärt hatte, „daß die sich aus den Antragsunterlagen ergebenden persönlichen und sachlichen Daten in elektronischen Dateien zu amtlichen Zwecken gespeichert und allen am Verfahren Beteiligten zur Kenntnis gegeben werden“. Zu einer solchen Erklärung ist folgendes zu sagen:

Soweit kein Gesetz oder eine sonstige Rechtsvorschrift die Übermittlung personenbezogener Daten erlaubt, ist sie gemäß § 4 Abs. 1 Nr. 2 SächsDSG mit Einwilligung des Betroffenen zulässig. Die hier abgegebene Erklärung umfaßt nicht die Übersendung von Bescheiden an Dritte, selbst wenn der in der Erklärung verwendete Begriff der „am Verfahren Beteiligten“ nicht im engen Sinn des Verwaltungsverfahrensgesetzes, sondern in einem weiten umgangssprachlichen Sinn verstanden wird. Denn eine öffentliche Stelle darf von einer Einwilligung nur innerhalb bestimmter Grenzen Gebrauch machen.

Eine Grenze ist der Wille des Betroffenen, der regelmäßig keinen Überblick über ein Verwaltungsverfahren hat, zumal dieses nicht in allen Einzelschritten vorhersehbar und der Verfahrensausgang offen ist. Deshalb darf eine zur Erleichterung oder Beschleunigung des Verwaltungsverfahrens erteilte, für die öffentliche Stelle also vorteilhafte Einwilligung, später von ihr nicht in einer für den Betroffenen nachteiligen Weise verwendet werden. Denn der Wille des Betroffenen umfaßt eine solche Verwendung nicht. Zwei weitere Aspekte kommen hinzu. Erstens liegt es nach dem Wortlaut des Einwilligungstextes nicht unbedingt auf der Hand, daß ein Bescheid zu den „sich aus den Antragsunterlagen ergebenden persönlichen und sachlichen Daten" gehört - im Gegenteil, jeder unbefangene Leser wird hier nicht an einen Bescheid denken. Zweitens entspricht eine solche Standarderklärung nicht den Erfordernissen des § 4 SächsDSG, vor allem nicht der darin vorgeschriebenen Hinweispflicht. Dies hat die Unwirksamkeit der Einwilligung zur Folge, weil unzureichend unterrichtete Betroffene nicht wirksam einwilligen können. Konsequenterweise muß bei einer unwirksamen Einwilligung auch die auf sie gestützte Datenverarbeitung unzulässig sein, weil ihr insoweit die rechtliche Legitimation fehlt (Simitis in Simitis/Dammann/Geiger/Mallmann/Walz, Kommentar zum Bundesdatenschutzgesetz, 4. Aufl., § 4, Rdnr. 60 ff.).

## 13.4 Forschungsvorhaben zur Lebenssituation von Frauen mit Behinderung

Das Bundesministerium für Familie, Senioren, Frauen und Jugend hatte ein Forschungsinstitut mit einer Studie über die Lebenssituation behinderter Frauen beauftragt. Das Institut wandte sich auch an das Sächsische Landesversorgungsamt.

Gegenüber dem Landesversorgungsamt habe ich geäußert, daß gegen die von dem Institut geplante Verfahrensweise der Datenerhebung datenschutzrechtliche Bedenken bestehen. Denn dem Forschungsinstitut sollten bundesweit Namen und Anschriften von etwa 5000 Frauen zur Verfügung gestellt werden. Die Befragung beschränkte sich auf 16- bis 60jährige körper- und sinnesbehinderte Frauen. Frauen mit geistiger Behinderung sollten nicht einbezogen werden.
Die datenschutzgerechteste Variante für die Einholung der Einwilligung der Frauen ist ein Adreßmittlungsverfahren, d. h. das Forschungsinstitut stellt die für das Forschungsvorhaben erforderlichen Unterlagen zusammen, die dann über das Landesversorgungsamt den nach einem Zufallsverfahren ermittelten behinderten Frauen zugeleitet werden.

Wie mir das Landesversorgungsamt mitteilte, werde dieses Adreßmitteilungsverfahren umgesetzt. Das Institut habe wegen datenschutzrechtlicher Bedenken des Landesversorgungsamts im Zusammenhang mit der Adressenübermittlung dieser Verfahrensabwandlung zugestimmt. Es übergebe dem Landesversorgungsamt daher ausreichend frankierte Umschläge mit einem Anschreiben, das mit dem Landesversorgungsamt abgestimmt sei und aus dem die Verfahrensweise des Versandes der Fragebögen und die Freiwilligkeit der Teilnahme hervorgingen. Das Landesversorgungsamt ermittle die Anschriften nach einem vorgegebenen Auswahlverfahren, adressiere und versende schließlich die Umschläge. Dieses Vorgehen habe ich begrüßt.

# 14 Technischer und organisatorischer Datenschutz

## 14.1 Auswirkungen telekommunikationsrechtlicher Vorschriften auf die öffentliche Verwaltung

In den letzten beiden Jahren sind eine Reihe von neuen rechtlichen Regelungen im Telekommunikations- und Multimediabereich (Telekommunikationsgesetz, Telekommunikationsdatenschutzverordnung, Informations- und Kommunikationsdienstegesetz, Mediendienstestaatsvertrag) verabschiedet worden, die auch Auswirkungen auf die Arbeit von öffentlichen Stellen haben. Sie regeln verschiedene Aspekte der Telekommunikation.

Grundlegend für das Telekommunikationsrecht ist das Telekommunikationsgesetz. Darin wird der „hardwarenahe" Bereich geregelt, während sich die anderen Neuregelungen mit der darüberliegenden Schicht der Dienste befassen. Es kann also durchaus der Fall eintreten, daß bei einem Telekommunikationsvorgang je nachdem, welchen Aspekt man betrachtet, gleichzeitig unterschiedliche Regelungen zu beachten sind. Benutzt z. B. ein Mitarbeiter einer öffentlichen Stelle den Zugang von T-Online, um dort einen Dienst abzurufen (z. B. das Angebot von SPIEGEL-Online), so wird eine Telefonverbindung zum T-Online-Server aufgebaut. Für sie ist wie für jede Telefonverbindung (zumindest auf der Strecke der Telekom, s. u.) das TKG mit seinen Regelungen einschlägig. Da der Mitarbeiter jedoch kein Telefongespräch führen will, sondern sich bei T-Online einwählt, ändert sich die Qualität der Kommunikation. Zusätzlich zur Telekommunikationsverbindung kommt noch die Nutzung eines Teledienstes von T-Online hinzu. Einschlägig ist das Teledienstegesetz, das Bestandteil des Informations- und Kommunikationsdienstegesetzes ist. Ruft der Mitarbeiter jetzt das Angebot des „Spiegel" ab, so gilt für dieses Verhältnis zwischen Mitarbeiter und „Spiegel" der Mediendienstestaatsvertrag, da der „Spiegel" „an die Allgemeinheit gerichtete Informations- und Kommunikationsdienste" anbietet (§ 2 Abs. 1 Mediendienstestaatsvertrag). An dem im Vergleich zur Realität noch einfachen Beispiel wird deutlich, daß die rechtliche Lage im Bereich der Telekommunikation mittlerweile recht kompliziert ist. Öffentliche Verwaltungen wollen aber für andere Dienstleistungen neben der Sprachtelefonie immer mehr auch die neuen Medien nutzen. Sie müssen sich deshalb mit der Rechtslage befassen und sie beachten.

*Telekommunikationsgesetz*

Betreiber von Telekommunikationsnetzen im Sinne des TKG sind auch öffentliche Stellen, sofern sie rechtliche und tatsächliche Kontrolle ausüben „über die Gesamtheit der Funktionen, die zur Erbringung von Telekommunikationsdienstleistungen oder nichtgewerblichen Telekommunikationszwecken über Telekommunikationsnetze unabdingbar zur Verfügung gestellt werden müssen; dies gilt auch dann, wenn im Rahmen des Telekommunikationsnetzes Übertragungswege zum Einsatz kommen, die im Eigentum Dritter stehen" (§ 3 Nr. 2). Dazu gehört zum Beispiel auch der TK-Anlagenverbund der Staatsregierung, selbst wenn dafür Leitungen der Telekom AG genutzt werden.

Allerdings ist für das interne Telefon- und Datennetz einer öffentlichen Stelle (ein sog. Corporate Network) das TKG zum großen Teil nicht einschlägig, da es sich vorrangig mit dem gewerblichen Angebot von Telekommunikation (also mit Gewinnerzielungsabsicht) beschäftigt. Der elfte Teil jedoch (Fernmeldegeheimnis, Datenschutz, Sicherung) gilt für das geschäftsmäßige Erbringen von Telekommunikationsdiensten, „das nachhaltige Angebot von Telekommunikation einschließlich des Angebots von Übertragungswegen für Dritte mit oder ohne Gewinnerzielungsabsicht“ (TKG § 3 Nr. 5). Nach der amtlichen Begründung zu § 85 Abs. 2 TKG ist dies schon dann der Fall, wenn öffentliche Stellen ihren Bediensteten das Telefonnetz zur privaten Nutzung überlassen: „Verpflichtet ist jeder, der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt. Hier wird bewußt vom ‚geschäftsmäßigen‘ (und nicht vom ‚gewerblichen‘) Erbringen von Telekommunikationsdiensten gesprochen, um deutlich zu machen, daß es hier nicht auf Gewinnerzielungsabsicht ankommt. ... auch ein ohne Gewinnerzielungsabsicht, auf Dauer angelegtes Angebot von Telekommunikationsdiensten verpflichtet zur Wahrung des Fernmeldegeheimnisses. Dem Fernmeldegeheimnis unterliegen damit z. B. Corporate Networks, Nebenstellenanlagen in Hotels und Krankenhäusern, Clubtelefone und Nebenstellenanlagen in Betrieben und Behörden, soweit sie den Beschäftigten zur privaten Nutzung zur Verfügung gestellt sind.“

In der Landesverwaltung ist für die Nutzung von TK-Anlagen die Dienstanschlußvorschrift (DAV), eine Verwaltungsvorschrift des SMF, maßgeblich. In meiner Stellungnahme zur Neufassung der DAV habe ich darauf hingewiesen, daß diese neuen gesetzlichen Regelungen auch bei der Überarbeitung zu beachten sind. So sollte die DAV, da sie zumindest in Teilbereichen das TKG zu berücksichtigen hat, sowohl bei den verwendeten Begriffen wie auch im gesamten Inhalt die Vorgaben des TKG beachten. Gleiches gilt für ähnliche Regelungen im kommunalen Bereich.

Für die DAV habe ich in Anlehnung an das TKG folgende Vorschläge gemacht:

- *Telekommunikation*

*„Telekommunikation“ ist der technische Vorgang des Aussendens, Übermittelns und Empfangens von Nachrichten jeglicher Art in der Form von Zeichen, Sprache, Bildern oder Tönen mittels Telekommunikationsanlagen,*

- *Telekommunikationseinrichtungen (TK-Einrichtungen)*

*„Telekommunikationseinrichtungen“ sind technische Einrichtungen oder Systeme, die als Nachrichten identifizierbare elektromagnetische oder optische Signale senden, übertragen, vermitteln, empfangen, steuern oder kontrollieren können, dazu gehören insbesondere Vermittlungseinrichtungen (TK-Anlagen) sowie Übertragungswege,*

- *Übertragungswege*

*„Übertragungswege“ sind Telekommunikationsanlagen in Form von Kabel- oder Funkverbindungen mit ihren übertragungstechnischen Einrichtungen als Punkt-zu-*

*Punkt- oder Punkt-zu-Mehrpunkt-Verbindungen mit einem bestimmten Informationsdurchsatzvermögen (Bandbreite oder Bitrate) einschließlich ihrer Abschlußeinrichtungen,*

- *Telekommunikationsnetze (TK-Netze)*

*„Telekommunikationsnetz" ist die Gesamtheit der technischen Einrichtungen (Übertragungswege, Vermittlungseinrichtungen und sonstige Einrichtungen, die zur Gewährleistung eines ordnungsgemäßen Betriebs des Telekommunikationsnetzes unerläßlich sind), die zur Erbringung von Telekommunikationszwecken im Sinne des TKG dient,*

- *Telekommunikationsgeräte (TK-Geräte)*

*Telekommunikationsgeräte sind Endeinrichtungen (leitungs- oder nichtleitungsgebundene Geräte), die unmittelbar an die Abschlußeinrichtung eines Telekommunikationsnetzes angeschlossen werden sollen oder die mit einem Telekommunikationsnetz zusammenarbeiten und dabei unmittelbar oder mittelbar an die Abschlußeinrichtung eines Telekommunikationsnetzes angeschlossen werden sollen.*

Der Begriff „Telekommunikation" ist aus § 3 TKG Nr. 16 übernommen. Die Definition der TK-Einrichtungen entspricht der der „Telekommunikationsanlagen" (§ 3 TKG Nr. 17): „Übertragungswege" ist aus Nr. 22, „Telekommunikationsnetze" aus Nr. 21 übernommen. Bei der Definition der „TK-Geräte" wurde Nr. 3 („Endeinrichtungen") mit dem Text des SMF-Entwurfes verbunden.

Insbesondere ist auf eine neue Entwicklung aufmerksam zu machen. Der Gesetzgeber unterscheidet im TKG nicht mehr zwischen Telekommunikation und Datenverarbeitung. Durch die technische Entwicklung sind beide Bereiche nicht mehr zu trennen. Sprachtelefonie findet mittlerweile digital statt (ISDN, Mobilfunk), DV-Anwendungen ermöglichen Sprachtelefonie (Internet-Telefon). Auch in der technischen Realisierung findet eine wechselseitige Durchdringung statt. Im TKG wird deshalb unter Telekommunikation der gesamte hardwarenahe Bereich der Verarbeitung und Übermittlung elektronischer Nachrichten verstanden - egal ob dies durch EDV-Anwendungen oder mittels klassischer Sprachtelefonie geschieht. An den Stellen, bei denen bisher Telekommunikation und Datenverarbeitung parallel gesehen wurde, muß die elektronische Datenverarbeitung neu als ein Bereich betrachtet werden, der auf der Telekommunikation aufsitzt. „Datennetze" als eigenständige Größe gibt es nicht mehr.

Da eine öffentliche Stelle auch Betreiber einer Telekommunikationsanlage im Sinne des TKG ist und geschäftsmäßig Telekommunikationsdienste anbietet (s. o.), hat sie auch auf die technische Realisierung der Vorschriften des elften Teiles des TKG zu achten.

§ 87 Abs. 1 TKG schreibt technische Schutzmaßnahmen vor. Dazu soll ein entsprechender Katalog durch die Regulierungsbehörde zusammen mit dem BSI erarbeitet werden. Er ist mittlerweile erschienen. Die Rechtsverordnung nach Abs. 3, die die Erfüllung der Verpflichtungen nach den Absätzen 1 und 2 näher regelt, existiert noch nicht.

In zwei weiteren Paragraphen werden die Zugriffsmöglichkeiten für Sicherheitsbehörden geregelt. § 88 TKG ermöglicht direkte Überwachungsmaßnahmen des Telekommunikationsverkehrs; § 90 TKG ermöglicht ein automatisiertes Verfahren, mit dem Sicherheitsbehörden Zugriff auf die Kundendaten der Betreiber erhalten. Zu § 88 TKG ist mir mittlerweile ein Entwurf einer Rechtsverordnung bekannt, der Einzelheiten regelt. Zu § 90 TKG liegt eine Schnittstellenbeschreibung für das automatisierte Verfahren nach Abs. 2 im BMPT vor.

§ 89 TKG schließlich beschäftigt sich mit der Beachtung des Datenschutzes bei der automatischen Erhebung, Verarbeitung und Nutzung von Telekommunikationsdaten. Näheres wird in einer Rechtsverordnung der Bundesregierung geregelt (§ 89 Abs. 1 TKG). Eine solche Rechtsverordnung existiert bereits, allerdings noch auf der Grundlage der vorherigen Phase der Postreform; dadurch erstreckt sich aber auch der Geltungsbereich dieser Verordnung entsprechend der damaligen Ermächtigung nicht auf den Bereich der Corporate Networks. Die neue Verordnung soll erst synchron mit der Umsetzung der ISDN-Richtlinie der EU erlassen werden (Termin Oktober 98). Allerdings ist durch die Auflösung des BMPT und durch die schleppende Novellierung des BDSG auch hier mit Verzögerungen zu rechnen.

*Tele- und Mediendienste*

Da Behörden mittlerweile nicht nur als Nutzer, sondern immer mehr auch als Anbieter von Tele- und Mediendiensten gegenüber externen Dritten auftreten, sind auch hier die gesetzlichen Regelungen bereits bei der Entwicklung der Angebote sowie bei ihrem Betrieb zu beachten. Beispielhaft seien hier neben der Nutzung der E-Mail für die Bürgerkommunikation die Internetpräsentationen öffentlicher Stellen, aber auch die Dienste des Statistischen Landesamtes genannt.
Grundsätzlich sollten folgende Gesichtspunkte bei der Planung eines Angebotes beachtet werden:

- Öffne ich mein Angebot externen Dritten bzw. ist dies vorgesehen?

Das ist bereits der Fall, wenn es den Bediensteten der Behörde zur *privaten* Nutzung offensteht. Wird diese Frage bejaht, so tritt die Behörde als Anbieter auf und hat damit auch ggf. die Regelungen des Telekommunikations- und Medienrechts zu beachten.

- Auf welcher gesetzlichen Grundlage bewegt sich das Angebot?

Falls eine spezialrechtliche Regelung (z. B. beim elektronischen Grundbuch) existiert, ist zu prüfen, inwieweit sie abschließend ist. Ansonsten gelten die Regelungen des Telekommunikations- und Medienrechts.
- Welchen Charakter hat mein Angebot?

Die Klärung dieser Frage ist wichtig für die Bestimmung der einschlägigen rechtlichen Regelungen. Bewegt sich das Angebot im Rahmen der Sprachtelefonie, so ist das TKG zu beachten; entsprechend bei Telediensten das IuKG, bei Mediendiensten der Mediendienstestaatsvertrag und (wohl weniger häufig) bei rundfunkähnlichen Mediendiensten der Rundfunkstaatsvertrag.

So ist z. B. im Bereich des Kommunikationsverbundes der Staatsregierung die Telefonauskunft unter der Nummer 1188, die den Bediensteten auch zur privaten Nutzung offensteht, ein solcher Fall. Sie bietet den gesamten Umfang der Telekom-Auskunft an. § 89 Abs. 90 TKG erlaubt Anbietern von Telekommunikation (in diesem Fall der Staatsregierung gegenüber ihren Bediensteten) die Auskunft über Nutzerdaten aus öffentlichen Verzeichnissen. Nach § 2 Abs. 2 Nr. 2 Teledienstegesetz (TDG) ist die Auskunft selbst ein Teledienst. Damit gelten für den Inhalt der Auskunft die datenschutzrechtlichen Vorschriften des TKG (§ 89 Abs. 9), die in Zukunft noch durch die TDSV (s. Anm. 4) spezifiziert werden, für den Vorgang der Auskunft jedoch neben den Bestimmungen des TKG für die normale Telefonverbindung noch die Vorschriften des Teledienstedatenschutzgesetzes (TDDSG).

Bereits in 5/14.4 habe ich bei der Internetbenutzung durch Behörden darauf verwiesen, daß bei der Benutzung eines Providers die Regelungen der Auftragsdatenverarbeitung zu beachten sind. Dies gilt natürlich auch generell für das Angebot von Tele- und Mediendiensten. Die anbietende Behörde bleibt stets verantwortlich für das gesamte Verfahren und muß damit auch sichern, daß sie diese Verantwortung wahrnehmen kann.

## 14.2 Datenschutz durch Verschlüsselung und digitale Signatur

Behörden und öffentliche Stellen übermitteln zunehmend auch personenbezogene Daten in Netzen oder auf maschinell lesbaren Datenträgern. Vor jeder Übermittlung muß geprüft werden, ob die gesetzliche Grundlage vorhanden und die personellen, technischen und organisatorischen Maßnahmen zur Gewährleistung des Datenschutzes ausreichend sind. Dabei ist selbstverständlich die Sensitivität (Eingriffstiefe in das Persönlichkeitsrecht) der Daten zu berücksichtigen.
Häufig ist jedoch festzustellen, daß der Datenschutz nicht gewährleistet werden kann, weil unbefugte Kenntnisnahme, Manipulation, Abhören der Leitungen oder Fehler während des Transportes nicht zu verhindern sind.
In diesen Fällen könnte der Datenschutz durch den Einsatz von kryptographischen Verfahren (Verschlüsselungsverfahren) ausreichend gesichert werden (s. a. 14.6).

*1. Verschlüsselungsverfahren*
Verschlüsselungsverfahren bestehen meist aus einem Ver- und einem Entschlüsselungsalgorithmus. Diese Verfahren wandeln einen unmittelbar lesbaren Klartext mit Hilfe kryptographischer Schlüssel in einen verschlüsselten (chiffrierten) Text um und umgekehrt. Ziel der Verschlüsselung ist es, Daten in mathematischer Weise so umzuformen, daß es einem Angreifer nicht mehr möglich ist, den Klartext aus einem verschlüsselten Text zurück zu gewinnen. Die Entschlüsselung darf nur

demjenigen möglich sein, der im Besitz des kryptographischen Schlüssels ist.
Die einfachste Methode, einen Klartext in einen verschlüsselten Text zu überführen, besteht darin, jedes Zeichen des Klartextes durch ein anderes, fest zugeordnetes Zeichen zu ersetzen. Neben dieser einfachen Substitutions-Methode gibt es noch weitere Verfahren, wie z. B. Block- und Stromchiffren. Bei einer Blockchiffrierung wird der Klartext in Blöcke, in der Regel mit einer Länge von 64 Bit, zerlegt und jeder Block wird mit einem festen Schlüssel chiffriert. Bei der Strom- oder Flußchiffrierung wird hingegen jedes einzelne Bit verschlüsselt. Auf die Vielzahl der mathematischen Verfahren zur Verschlüsselung kann hier nicht eingegangen werden. Am häufigsten werden für die Verschlüsselung von personenbezogenen Daten symmetrische und asymmetrische Verfahren eingesetzt.

*1.1 Symmetrische Verfahren*
Bei einem symmetrischen Verschlüsselungsverfahren wird nur ein Schlüssel zum Ver- und Entschlüsseln verwendet. Nachteilig ist, daß der Schlüssel sowohl beim Absender (Verschlüsselung) als auch auf beim Empfänger (Entschlüsselung) vorliegen und geheim gehalten werden muß. Problematisch ist dabei meist die sichere Schlüsselübermittlung.
Vor allem dann, wenn sehr viele Netzteilnehmer untereinander Daten übermitteln wollen und für jede Kommunikationsbeziehung unterschiedliche Schlüssel verwendet werden müssen, kann das Schlüsselmanagement sehr aufwendig werden.
Ein häufig eingesetztes symmetrisches Verschlüsselungsverfahren ist das DES-Verfahren (Data Encryption Standard). Es ist ein relativ schnelles kryptographisches Verfahren, mit dem in angemessener Zeit größere Datenmengen verschlüsselt werden können.

*1.2 Asymmetrische Verfahren*
Bei einem asymmetrischen Verschlüsselungsverfahren werden für die Ver- und Entschlüsselung jeweils unterschiedliche Schlüssel verwendet, zum einen der private Schlüssel, der beim Besitzer geheim zu halten ist, zum anderen der öffentliche Schlüssel, der in einem öffentlichen Verzeichnis oder Register hinterlegt und von dort abgerufen werden kann. Beide Schlüssel sind eindeutig einander zugeordnet, wobei es praktisch unmöglich ist, einen Schlüssel aus dem anderen oder aus dem verschlüsselten Text zu bestimmen.
Das Verfahren ermöglicht ein wesentlich vereinfachtes Schlüsselmanagement gegenüber dem symmetrischen Verfahren, denn jeder Absender von Daten (Nachrichten/ Informationen) benutzt zum Verschlüsseln den öffentlichen Schlüssel des Empfängers. Die verschlüsselte Nachricht kann jedoch mit dem öffentlichen Schlüssel nicht mehr entschlüsselt werden. Nur der rechtmäßige Empfänger mit seinem passenden geheimen Schlüssel ist in der Lage, den verschlüsselten Text wieder in Klartext umzuwandeln.
Ein häufig eingesetztes asymmetrisches Verfahren ist das RSA-Verfahren (Rivest-Shamir-Adleman). Nachteilig ist, daß das RSA-Verfahren sehr viel Rechenzeit benötigt. Daher wird dieses Verfahren meist nicht zum Verschlüsseln großer Datenmengen eingesetzt, sondern nur zum Erzeugen von elektronischen Unterschriften oder zum Verschlüsseln von Sitzungsschlüsseln. Ein Sitzungsschlüssel ist der geheim zu haltende Schlüssel für symmetrische Verfahren.

*2. Elektronische Unterschrift / digitale Signatur*
Eine Unterschrift soll ein Schriftstück eindeutig und nachweisbar einer bestimmten Person zuordnen. Auch elektronisch übermittelte Dokumente sollten glaubhaft durch eine Unterschrift gekennzeichnet werden können. Würde dazu jedoch die eigenhändige Unterschrift in digitalisierter Form vorliegen, könnte mit ihr jederzeit jedes beliebige Dokument unbemerkt „unterschrieben" werden. Außerdem könnte der Inhalt eines elektronisch übermittelten Dokumentes unbemerkt verändert oder verfälscht werden. Daher wurde nach einer Möglichkeit gesucht, nachweisbar und eindeutig eine digitale Unterschrift zu erzeugen und die Unverfälschtheit eines Dokumentes zu beweisen. Das Ergebnis ist die elektronische Unterschrift, die auch als digitale bzw. elektronische Signatur bezeichnet wird.

Der Begriff der digitalen Signatur ist im § 2 des Signaturgesetzes (SigG) so definiert: „Eine digitale Signatur im Sinne dieses Gesetzes ist ein mit einem privaten Signaturschlüssel erzeugtes Siegel zu digitalen Daten, das mit Hilfe eines zugehörigen öffentlichen Schlüssels, der mit einem Signaturschlüssel-Zertifikat einer Zertifizierungsstelle oder der Behörde nach § 3 versehen ist, den Inhaber des Signaturschlüssels und die Unverfälschtheit der Daten erkennen läßt."

Voraussetzung für die Erzeugung einer digitalen Signatur ist eine Schlüsselgenerierung für ein asymmetrisches Verfahren (öffentlicher und geheimer Schlüssel) in einer sicheren Umgebung und die beglaubigte Zuordnung der Schlüssel zu einer Person durch eine vertrauenswürdige Stelle (Zertifizierungsstelle). Der geheime Schlüssel wird meist im gesicherten Bereich auf einer PIN-geschützten SmartCard (Mikroprozessor-Chipkarte) von außen nicht ausles- und änderbar gespeichert.
Zur Erzeugung und Überprüfung einer digitalen Unterschrift müssen außerdem noch Signatursoftware und z. B. ein SmartCard-Leser vorhanden sein. Ein PC-Nutzer ist dann in der Lage, seine in Standardanwendungen (z. B. Word) geschriebene Dokumente zu signieren und zu übermitteln.

*2.1 Erzeugung und Prüfung digitaler Signaturen*
Ein elektronisch geschriebenes Dokument wird mit Hilfe der Signatursoftware komprimiert, indem ein „Hashwert" (ähnlich einer Prüf- oder Quersumme) erzeugt wird. Der Hashwert wird mit dem geheimen Schlüssel des Absenders verschlüsselt und an das Dokument angefügt. Dieser Vorgang wird als „Signieren" bezeichnet.
Der Empfänger entschlüsselt die Signatur mit dem öffentlichen Schlüssel des Absenders. Zugleich bildet der Empfänger aus dem übermittelten Dokument mit seiner Signatursoftware einen „selbst erzeugten" Hashwert. Sind beide Hashwerte (entschlüsselter und selbst erzeugter) identisch, ist sichergestellt, daß das Dokument während der Übermittlung nicht verändert wurde (Integrität) und daß das Dokument vom angegebenen Absender stammt (Authentizität).

Ohne Kenntnis des geheimen Schlüssels des Absenders ist keine Fälschung möglich. Jede noch so kleine Änderung der Signatur oder des Dokumentes würden eine Nichtübereinstimmung ergeben und das Dokument als gefälscht ablehnen.
Zur Erzeugung von Hashwerten gibt es verschiedene mathematische Algorithmen. Die heute am häufigsten implementierte Hashfunktion ist MD5 (128-Bit Hashwert;

die Kompression hat 4 Runden).

*2.2 Gesetzliche Grundlage für digitale Signaturen*

Inzwischen wurde die erforderliche gesetzliche Grundlage für digitale Signaturverfahren durch das Signaturgesetz (SigG) geschaffen. Es ist als 3. Artikel Bestandteil des am 1. August 1997 in Kraft getretenen Informations- und Kommunikationsdienstegesetzes (IuKDG) des Bundes.

Das Signaturgesetz und die Signaturverordnung (SigV) legen die technischen und organisatorischen Anforderungen für die Sicherungsinfrastruktur fest, unter denen digitale Signaturen als sicher gelten und Fälschungen zuverlässig festgestellt werden können. Sie bilden damit die Voraussetzung für einen elektronischen Rechts- und Geschäftsverkehr auch in offenen Netzen.

*3. „Standard"-Verschlüsselungsverfahren*

Eines der bekanntesten und im Internet frei erhältlichen Verschlüsselungsverfahren ist PGP (Pretty Good Privacy). PGP gilt als de-facto-Standard für private digitale Kommunikation.

Es verschlüsselt Dateien und E-Mails auch im Internet und kann Dokumente digital signieren.

Beachtet werden muß jedoch, daß PGP nur für den Privatgebrauch freigegeben ist, weil Lizenzbestimmungen des IDEA-Patents dagegen stehen. IDEA (International Data Encryption Algorithm) ist ein Verschlüsselungsalgorithmus, den PGP zum Verschlüsseln von Dateien benutzt.

*4. Zum sicheren Einsatz von Verschlüsselungsverfahren*

Beim Einsatz von Verschlüsselungsverfahren muß beachtet werden, daß die Sicherheit eines Verfahrens

- von der Güte des Algorithmus,
- der Schlüsselauswahl (Die Schlüssellänge ist vom eingesetzten Verfahren abhängig. Zur Schlüsselerzeugung sind geeignete Verfahren, z. B. Zufallszahlengeneratoren, einzusetzen.),
- und dem sicheren Umgang mit dem geheimen Schlüssel (z. B. sichere Aufbewahrung und Hinterlegung der Schlüssel, Übermittlung der Schlüssel zeitlich und räumlich getrennt von den Daten per Boten oder PIN-Brief zum Empfänger, Schlüsselwechsel in Abhängigkeit von der Bedrohung, von der Häufigkeit ihres Einsatzes oder sofort nach Bekanntwerden)

abhängig ist. Außerdem müssen die Verschlüsselungsfunktionen korrekt und nicht manipulierbar implementiert werden.

Zu beachten ist jedoch, daß auch anerkannte Verschlüsselungsverfahren vor allem bei zu geringer Schlüssellänge „geknackt" werden könnten.

Beispielsweise wurde der Schlüssel mit einer Länge von 40 Bit beim RSA-Verfahren innerhalb von dreieinhalb Stunden gebrochen. Dazu wurde allerdings die Rechnerkapazität auf 250 Rechner verteilt, um die 100 Milliarden Schlüsselmöglichkeiten zu testen. Auch beim DES-Verfahren wurde in den USA im Juni 1997 erstmals ein Schlüssel mit einer Länge von 56 Bit durch systematisches Durchprobieren mit verteilten Rechenkapazitäten des Internets gebrochen.

Dies zeigt, daß vor dem Einsatz von Verschlüsselungsverfahren unbedingt der Rat von Experten (z. B. Bundesamt für Sicherheit in der Informationstechnik - BSI) eingeholt werden sollte.
Zur Zeit gelten Schlüssellängen von 112 Bit für DES-Verfahren (Triple-DES) und von 512 Bit für RSA-Verfahren als sicher.

## 14.3 Teleheimarbeit

Im vergangenen Berichtszeitraum wurde ich mehrfach um Stellungnahmen zur Einrichtung von Teleheimarbeitsplätzen gebeten.

Bei der Teleheimarbeit sollen Bedienstete on-line oder off-line von einem PC oder Terminal aus in ihrem häuslichen Bereich Aufgaben des Dienstherrn erledigen. Die Einrichtung von Teleheimarbeitsplätzen durch eine Dienststelle kann zwar ökonomisch sinnvoll sein (z. B. Gewährleistung der ständigen Betriebsbereitschaft von Verfahren) oder eine verbesserte Vereinbarkeit von Beruf und Familie (z. B. während Erziehungs- und Pflegezeiten) ermöglichen, sie ist jedoch aus datenschutzrechtlicher Sicht problematisch:

- Beim Telearbeitsplatz fehlt die gesicherte Umgebung, die für einen Behördenarbeitsplatz notwendig ist. In der Regel haben Familienmitglieder und Gäste zum Telearbeitsplatz ungehinderten Zutritt.
- Für den Telearbeitsplatz muß der Zutritt zur Wohnung für Kontroll- und Prüfungszwecke durch die Behörde (Fachvorgesetzte) und den Datenschutzbeauftragten ermöglicht und vertraglich geregelt werden, weil sonst die Unverletzlichkeit der Wohnung (Art. 30 SächsVerf) dem entgegen steht.
- Ein Telearbeitsplatz darf nur eingerichtet werden, wenn durch personelle, technische und organisatorische Maßnahmen ein ausreichender Datenschutz gewährleistet werden kann.

Teleheimarbeit durch Behördenbedienstete erfolgt in Ausübung dienstlicher Tätigkeit. Deshalb ist in einem solchen Fall die betreffende Behörde selbst „speichernde“ bzw. „datenverarbeitende“ Stelle im Sinne des Sächsischen Datenschutzgesetzes, so daß die Datenverarbeitung den Bestimmungen dieses Gesetzes bzw. spezialrechtlichen Regelungen unterliegt. Es findet keine Auftragsdatenverarbeitung statt. Der Dienstherr bleibt weisungsbefugt. Er legt die Art und Weise fest, wie die Aufgaben zu erledigen sind.
Ich weise auch hin auf die Mitbestimmung der Personalvertretung gemäß § 80 Abs. 3 Nr. 15 SächsPersVG bei der Gestaltung von Arbeitsplätzen und bei der Auslagerung von Arbeitsplätzen aufgrund der Heimarbeit an technischen Geräten.

Damit die schutzwürdigen Belange und Rechte der Betroffenen bei der Verarbeitung personenbezogener Daten auch beim Heimarbeitsplatz erfüllt werden, muß die „datenverarbeitenden“ Stelle, also die Behörde, die konkreten personellen, technischen und organisatorischen Sicherungsmaßnahmen festlegen.
Für die Personalauswahl sind die Anforderungen an den Bediensteten bezüglich der Besonderheiten (Arbeitsaufgabe und das Sicherheitsbewußtsein) eines Heimarbeits-

platzes festzulegen. Der Bedienstete ist vertraglich an striktes Handeln nach Anweisungen zu binden, er hat besondere Sorgfaltspflichten zu erfüllen und ist zur Meldung besonderer Vorkommnisse zu verpflichten.
Aus datenschutzrechtlicher Sicht dürfen für Teleheimarbeit keine privaten PCs genutzt werden, weil dann weder eine Kontrolle durch die Behörde noch eine Trennung dienstlicher und privater Datenverarbeitung gewährleistet ist. Deshalb sind für die Teleheimarbeit grundsätzlich dienstliche Geräte und Systeme (z. B. PC, Modem) einzusetzen. Eine private Nutzung ist auszuschließen. Außerdem muß geregelt werden, daß die Behörde bzw. der Fachvorgesetzte und der Datenschutzbeauftragte Kontrollen am Telearbeitsplatz durchführen können. Deshalb empfiehlt sich die Teleheimarbeit zwischen der Dienststelle und den Mitarbeitern (z. B. in einer Dienstvereinbarung) vertraglich zu regeln und Rahmenbedingungen zu schaffen, die die ökonomische Notwendigkeit, die datenschutzrechtlichen und die personellen, technischen und organisatorischen Maßnahmen beachten. Vertraglich zu regeln wären beispielsweise:
- die Zulassung von außerbetrieblichen Arbeitsstätten,
- die Verteilung der Arbeitszeit auf Dienststelle und Wohnung,
- zur Verfügung gestellte Arbeitsmittel (z. B. PC, Modem),
- Ausschluß der privaten Nutzung der Arbeitsmittel,
- Festlegung zur Wartung der Arbeitsmittel,
- Aufwandserstattung (z. B. Gebühren für Telearbeit),
- Rückgabe der Arbeitsmittel nach Beendigung der Teleheimarbeit,
- Festlegung welche Arbeitsunterlagen außerbetrieblich verbracht werden dürfen,
- Kontrollmöglichkeiten durch die Dienststelle und den Datenschutzbeauftragten,
- Datenschutz- und Datensicherheitskonzept gemäß § 9 Abs. 2 SächsDSG für die Arbeitsstätte in der Wohnung des Mitarbeiters,
- Haftung und Versicherungsschutz des Mitarbeiters und seiner Familienangehörigen.

Ein Telearbeitsplatz kann nur dann eingerichtet werden, wenn die zu treffenden Sicherheitsmaßnahmen gemäß § 9 Abs. 2 SächsDSG unter Beachtung der Sensibilität der Daten ausreichend sind. Dazu sollen nachfolgend beispielhaft einzelne Maßnahmen aufgeführt werden:
- Die Inbetriebnahme des PC durch Unbefugte sollte durch Sicherheitssoft- und -hardware verhindert werden (z. B. BIOS-Paßwort, Geräteschlüssel, Bootschutz, Chipkarte und PIN-Code).
- Der sichere Zugang zum und Zugriff vom Telearbeitsplatz auf die jeweilige Anwendung des Rechners/Servers in der Behörde ist über öffentliche Netze zu gewährleisten. Dazu müssen Sicherheitsmaßnahmen auf dem Übertragungsweg und Abschottungsmaßnahmen beim Rechner der Behörde und beim PC in der Wohnung des Mitarbeiters realisiert werden. Dabei ist die Protokollierung sensibler Aktivitäten in der Anwendung oder im System und deren Kontrolle erforderlich.
- Vor Beginn einer Verbindung zum Rechner in der Behörde sollte Rufnummernübermittlung und Paßwortschutz oder Call-Back-Verfahren zur Authentifikation genutzt werden, um nur zugelassenen Anschluß- und Benutzerkennungen den Zugang zu ermöglichen.
- Das Paßwort sollte verschlüsselt übertragen werden. Ist dies nicht möglich, empfiehlt sich die Verwendung von Einmalpaßwörtern (müssen nach einmaligem

Gebrauch gewechselt werden).
- Die Zugangsrechte und Zugriffsrechte dürfen nur in dem Umfang eingeräumt werden, wie sie für die Wahrnehmung der Teleheimarbeit erforderlich sind.
- Die Modemverbindung ist zu trennen, wenn sich der Benutzer vom System abmeldet.
- Beim Verlassen des Heimarbeitsplatzes sind alle Informationen vor unbefugter Kenntnisnahme, Nutzung und Verarbeitung durch Unbefugte zu sichern.
- Arbeitsunterlagen, Datenträger usw. müssen verschlossen z. B. in einem Schrank oder Teil eines Schrankes aufbewahrt werden.
- Kryptographische Verfahren sollten eingesetzt werden, um Manipulationen, unbefugte Kenntnisnahme und Fehler während des Datentransportes zu verhindern.
- Falls ISDN zur Kommunikation genutzt wird, könnte ein spezielles Secure-CAPI (SCAPI) die notwendigen Sicherheitsfunktionen realisieren.
- Sicherheitsmodems können sowohl Benutzeridentifizierung wie kontrollierten Zugang gewährleisten und verschlüsselt kommunizieren.
- Für den Transport von Daten und Datenträgern sollte der Dienstherr zu verschließende Behältnisse bereitstellen.

Beachtet werden muß jedoch, daß aufgrund des höheren Risikos nicht alle Aufgaben einer Behörde in Heimarbeit erledigt werden können. Auf eine Verarbeitung von sensiblen Daten, wie z. B. Personal-, Sozial-, Steuer-, und Patientendaten, sollte in Teleheimarbeit verzichtet werden.

## 14.4 Haftraumkommunikationsanlage in einer JVA

Ein Insasse einer Justizvollzugsanstalt wandte sich mit einer Eingabe an mich. Die Privatsphäre der Häftlinge werde durch eine neue Haftraumkommunikationsanlage verletzt. Die Justizbediensteten hörten willkürlich und unter Verstoß gegen das SächsDSG unbemerkt die Gespräche der Insassen ab.

Ich habe dies zum Anlaß genommen, die JVA unangemeldet zu besuchen und die Einhaltung des Datenschutzes in der gesamten JVA und insbesondere die neue Haftraumkommunikationsanlage zu kontrollieren.

Im Vorgespräch mit dem Leiter der JVA wurde klar, daß er meine datenschutzrechtlichen Empfehlungen (4/8.2.1 und 5/8.5) nicht akzeptierte. Seiner Meinung nach müsse in der JVA jeder Vollzugsbeamte alles wissen. Insbesondere die Protokollierungen der Einsichtnahme in die Gefangenenpersonalakte brächte nichts, sie sei nur „Verwaltungsaufwand“ und im übrigen mit „Tricks“ leicht zu unterlaufen. Das Justizvollzugspersonal wäre auch überhaupt nicht persönlich an Gefangenendaten, auch wenn sie eventuelle Prominente beträfen, interessiert. Dokumentiert wird bisher nur die Mitnahme von Akten aus dem Aktenraum.

Im weiteren Verlauf des Gespräches stellte sich heraus, daß der Anstaltsleiter nicht wußte, wer zur Zeit das Amt des Datenschutzbeauftragten ausübe. Auch ob und von wem ein Datei- und Geräteverzeichnis geführt würde, war ihm nicht bekannt. Einzelheiten zur Haftraumkommunikationsanlage waren ihm ebenfalls nicht geläufig.

Diese Zustände sind meines Erachtens nicht hinnehmbar, da sie eine eindeutige Verletzung des § 9 SächsDSG darstellen. Ich wies den Anstaltsleiter darauf hin, daß eine konkrete (zweckgebundene) Dokumentation der Einsichtnahme in die Insassenakten zu erfolgen habe und daß die Mitarbeiter darüber zu belehren seien. Des weiteren sei ein Konzept der Maßnahmen nach § 9 SächsDSG zu erarbeiten.

Auf meine Nachfrage in Auswertung der Kontrolle erfuhr ich, daß ein neuer Datenschutzverantwortlicher ernannt worden war und daß das Dateien- und Geräteverzeichnis überarbeitet werden solle.

Die Haftraumkommunikationsanlage entsprach den Bestimmungen des SächsDSG. Das unerlaubte Mithören der Gespräche der Zelleninsassen durch Unbefugte ist technisch ausgeschlossen. Nur durch die Freischaltung der Anlage durch den Insassen oder einen anderen Zellenanwesenden kann eine Kommunikation erfolgen. Die Anlage ist mit neuen Softwaremodulen erweiterbar. So werden in der Untersuchungshaftanstalt in Chemnitz bereits der Name, Vorname und die Gefährdungsklassifizierung der Insassen auf dem Funktionsdisplay dargestellt. Dieses Modul soll sachsenweit eingeführt werden.

Erkundigungen bei dem Hersteller der Anlage ergaben, daß ein Softwaremodul geplant ist, welches das Abhören der Zelleninsassen ohne ihr Wissen technisch ermöglicht. Dabei muß die Anlage durch ein Chipkartenlesegerät erweitert und durch eine spezielle Chipkarte von Sondereinsatzkräften „scharfgeschaltet“ werden. Für zwei Haftanstalten in Nordrhein-Westfalen wären bereits Angebote seitens der Firma erfolgt.

Wie ich jedoch vom SMJus erfuhr, ist in Sachsen gleiches zur Zeit nicht zu erwarten. Die Privatsphäre der Insassen der JVA’s werde als hohes schützenswertes Rechtsgut betrachtet, das es zu bewahren gilt. Dieser Meinung schließe ich mich gern an.

## 14.5 „Hoax“ - Über den Umgang mit Viren-Fehlalarmen[1]

Virenwarnungen, die die gesamte DV-Branche in Aufruhr versetzen und sich danach in Wohlgefallen auflösen, sind bereits seit einigen Jahren bekannt. Durch die verstärkte Internet-Nutzung in Unternehmen und Behörden können sich diese Fehlwarnungen wesentlich schneller verbreiten und intern durch Netzüberlastungen und vergeudete Arbeitszeit im Einzelfall mehr Schaden anrichten als ein real existierender Virus. Im Fachjargon werden solche Fehlwarnungen mit dem Begriff „Hoax“ klassifiziert.

Die Wurzel des Hoax-Problems liegt darin, daß sich Warnmeldungen häufig schneller als Viren verbreiten. Ein Hoax besitzt keinen internen Verbreitungsmechanismus. Stattdessen werden menschliche Schwächen für die Verbreitung ausgenutzt. Ein Hoax warnt vor großen Schäden bis hin zur totalen Rechnerzerstörung und bittet darum, diese Warnung an alle Bekannten in der Welt weiterzugeben. Irgendein Nutzer beginnt, im Netz „Feuer“ zu rufen. Hinzu kommt, daß der Einsatz eines Hoax wesentlich effektiver ist als die Programmierung eines realen Virus. Außerdem wird

[1] Der Beitrag ist ein Nachdruck aus dem Datenschutzberater 1/98, S. 6 f. Ich danke Herrn Würmeling für die Genehmigung.

statt tiefergehender Systemkenntnisse nur ein quasi-technisches Wissen benötigt. Der Kreis der Personen, die einen Hoax erzeugen können, ist damit wesentlich größer als der Kreis potentieller Virenprogrammierer.

Mit der Verteilung der Warnung, also des eigentlichen Hoax, beginnt eine Kettenreaktion, die häufig durch zwei Entwicklungen gekennzeichnet ist. Gutmeinende Nutzer fügen eigene Warnungen hinzu, andere nicht so gutmeinende Nutzer erweitern die beschriebene Gefahr noch durch selbst erdachte Szenarien. Somit unterliegen die Benachrichtigungen, die einen Hoax charakterisieren, Änderungen. Daher kann ein Hoax in verschiedenen Variationen existieren und so mehr als einmal durch ein Netz rollen. So gab es zum Beispiel im Jahr 1996 die Warnung vor einem angeblichen „Penal"-Virus. Für einen aufmerksamen Beobachter der Szene war klar, daß diese Warnung identisch war mit einer früheren, die vor dem nicht existenten „Penpal"-Virus warnte. Nachdem also auf irgendeine Art und Weise das „p" entfernt wurde, suchte sich auch diese Hoax-Variation ihren Weg durch das Internet.

Wenn man die Hoax-Nachrichten der letzten Jahre betrachtet, lassen sich gemeinsame Faktoren erkennen. Normalerweise besteht ein Hoax aus einer Kombination der folgenden Faktoren:

- Gewarnt wird vor Viren oder Trojanischen Pferden, die mittels E-Mail über das Internet versandt wurden.
- Üblicherweise stammt die E-Mail von einer Person, manchmal von einem Unternehmen, niemals jedoch von einer Behörde.
- Die Nachricht warnt vor dem Lesen oder „Downloaden" des Virus und verspricht Rettung beim Löschen der den Virus enthaltenden Nachricht.
- Die beschriebene schadensstiftende Software soll unvergleichbar zerstörerische Wirkung, quasi „gottgleiche" Macht ausüben können. Ihr wird häufig die Fähigkeit zugeschrieben, sich über E-Mail selbständig weiterzuverbreiten. Die beschriebene schadensstiftende Wirkung ist in der Regel weit von dem entfernt, was technisch heute möglich ist.
- Im Verlauf der Nachricht wird der Leser mehrmals aufgefordert, jede Person im Bekanntenkreis via E-Mail zu warnen.
- Der Hoax gibt sich unter Bezugnahme auf irgendeine anerkannte öffentliche Institution den Anschein der Seriosität. Meistens wird die schadenstiftende Software von der Institution als „bad" oder „worried" bezeichnet.
- Die gesamte Nachricht ist in einem technisch anmutenden Sprachjargon verfaßt.

Wenn eine Nachricht als Hoax erkannt wird, sollten folgende Schritte unternommen werden:

- Leiten Sie die Nachricht nicht weiter, um zumindestens an dieser Stelle die Wanderschaft des Hoax zu unterbrechen.
- Unterrichten Sie den Sender der Nachricht über die wahre Natur der von ihm versandten E-Mail.
- Übermitteln Sie ihm Informationen über den Aufbau und die Wirkungsweise eines Hoax. Auf diese Art und Weise kann er in Zukunft ebenfalls einen zugesandten Hoax erkennen.
- Sollten Sie sich nicht sicher sein, ob eine Nachricht ein Hoax ist, dann überprüfen Sie auf seriösen Webseiten im Internet, Datenbanken von Anti-Virus-Software oder

über anerkannte Institutionen oder Fachliteratur, ob dieser Virus dort bekannt ist oder bereits als Hoax registriert wurde.

In Unternehmen und Behörden sollten alle am Internet angeschlossenen Mitarbeiter über den Umgang mit Hoax-Nachrichten informiert werden. Weitere Informationen über spezielle Hoax's, aktuelle Warnungen vor realen Viren und neuen Hoax's sowie eine Sammlung von sicherheitsbezogenen Links sind im Internet unter <http:// www.ers.Ibm.com/security-links"index.html> zu finden.

## 14.6 Datenschutzfreundliche Technologien [2]

1. Einleitung

Die Computertechnologie ist in alle Lebensbereiche eingedrungen und breitet sich mehr und mehr aus. Beim Einkaufen, Zahlen, Buchen und Reservieren mittels bequemer Chip- oder Magnetstreifenkarten, bei der Kommunikation mittels digitaler Netze, bei Arztbesuchen mit Krankenversichertenkarten oder evtl. zukünftig mit Patientenkarten, auch durch Teilnahme an Online-Diensten sowie an nationalen und internationalen Netzwerken fallen eine Fülle von Einzeldaten über den Nutzer an. Diese elektronischen Spuren sind geeignet, persönliche Profile über den Einzelnen hinsichtlich seines Verhaltens zu bilden.
Immer mehr Bürger benutzen diese Technologie. Doch nicht zuletzt aufgrund der Komplexität und der mangelnden Transparenz von Systemen der modernen Informations- und Kommunikationstechnik (IuK-Technik) für die Nutzer fehlen diesen in der Regel Kenntnis und Kontrolle über Art, Umfang, Speicherort, Speicherdauer und Verwendungszweck der über sie erhobenen und gespeicherten Daten.
Der Schutz der Privatheit des Einzelnen wird bei Nutzung dieser Systeme bisher vorwiegend dadurch angestrebt, daß der Zugang zu den erhobenen, gespeicherten und verarbeiteten personenbezogenen Daten mittels technischer und organisatorischer Maßnahmen beschränkt wird. Der Schutz der Privatheit des Einzelnen hängt somit lediglich von der Wirksamkeit der üblichen Sicherheitsmaßnahmen und der Gewissenhaftigkeit ab, mit der sie durchgeführt werden. Mit diesen Sicherheitsmaßnahmen werden nur die klassischen Schutzziele Integrität, Vertraulichkeit, Verfügbarkeit und Zurechenbarkeit der gespeicherten Daten verfolgt.
Es wächst die Erkenntnis, daß der zunehmenden Gefährdung der Privatheit des Einzelnen nur durch eine weitgehende Reduzierung der Menge der gespeicherten Daten wirksam begegnet werden kann. Die Nutzung von IuK-Technik durch natürliche Personen wird demzufolge auch zukünftig nur dann den Ansprüchen der Datenschutzfreundlichkeit gerecht, wenn sie nach dem Prinzip der Datensparsamkeit erfolgt, wobei *so wenig personenbezogene Daten wie möglich* erhoben, gespeichert und verarbeitet werden. Datenvermeidung ist die stets anzustrebende Form der Datensparsamkeit. In diesem Fall werden bei der Nutzung von IuK-Systemen *keine personenbezogenen Daten* erhoben, gespeichert und verarbeitet, die Nutzung der IuK-Systeme erfolgt also anonym. Inhaltlich sind diese Forderungen Bestandteil des in den Datenschutzgesetzen des Bundes und der Länder festgelegten Grundsatzes der

[2] Übernommen aus der Broschüre - Datenschutz-freundliche Technologien - des Arbeitskreises Technik der Datenschutzbeauftragten des Bundes und der Länder - Redaktionsschluß 22. Januar 1998.

Erforderlichkeit, der auch schon bisher bei der Ausgestaltung der IuK-Technik zu beachten war, allerdings mit der technischen Entwicklung zunehmende Bedeutung gewinnt.
Anhand von Betrachtungen konkreter Beispiele aus dem Medienbereich, dem elektronischen Zahlungsverkehr, dem Gesundheitsbereich, der Telekommunikation sowie aus den Bereichen Transport und Verkehr werden in der Anlage die in diesen Projekten gewählten Ansätze und Bemühungen zur Verwendung datenschutzfreundlicher Technologien aufgezeigt. Es werden Empfehlungen in allgemeiner Form und für den jeweiligen Bereich gegeben.

## 2. Notwendigkeit für Datenschutz durch Technik

### 2.1 Rechtliche Forderungen und Entwicklungen

Bereits 1983 hat das Bundesverfassungsgericht im Volkszählungsurteil - am Beispiel der Statistik - den Anspruch auf Anonymisierung anerkannt. Gemäß der bekannten Auffassung des Bundesverfassungsgerichts heißt es dort: „Für den Schutz des Rechts auf informationelle Selbstbestimmung ist - und zwar auch schon für das Erhebungsverfahren - ... die Einhaltung des Gebots einer möglichst frühzeitigen faktischen Anonymisierung unverzichtbar, verbunden mit Vorkehrungen gegen die Deanonymisierung“ (BVerfGE 65, 1 [49]). In der Rechtsprechung zum Medienrecht ist das Recht auf Anonymität ebenfalls seit längerem als besondere Ausprägung des Persönlichkeitsrechts anerkannt, beispielsweise vom Bundesgerichtshof: „Das Recht auf informationelle Selbstbestimmung schützt ... davor, aus dem Bereich der Anonymität in den einer persönlichen Bekanntheit gerückt zu werden“ (BGH AfP 1994, 306 [307]).
Auch der Rat für Forschung, Technologie und Innovation, der unter Federführung des Bundeskanzleramts und des Bundesministers für Bildung, Wissenschaft, Forschung und Technologie einen ausführlichen Bericht über Chancen, Innovationen und Herausforderungen der Informationsgesellschaft erstellt hat, hat das Thema Anonymisierung aufgegriffen. Der Rat führt in Kapitel 2.5 über Datenschutz folgendes aus: „Den Vorrang verdienen Verfahren, die den Betroffenen ein Höchstmaß an Anonymität gegenüber Netzbetreibern und Dienstleistungsanbietern sichern.“ Entsprechende Passagen finden sich auch in den Bundestags- und Bundesratsdrucksachen über „Deutschlands Weg in die Informationsgesellschaft“ wieder [BD776].
Der Grundsatz der Datenvermeidung ist auch im Informations- und Kommunikationsdienste-Gesetz (IuKDG), dort in Art. 2 Teledienstedatenschutzgesetz (TDDSG), und im Mediendienste-Staatsvertrag [MDStV] enthalten. Danach haben Anbieter von Tele- bzw. Mediendiensten den Nutzern die Inanspruchnahme und Bezahlung entweder vollständig anonym oder unter Verwendung eines Pseudonyms zu ermöglichen, soweit dies technisch möglich und zumutbar ist [IuKDG].
Die europäische Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten sowie zum freien Datenverkehr [95/46/EG] enthält den Grundsatz, daß eine Verarbeitung personenbezogener Daten nur stattfinden darf, soweit sie im Hinblick auf bestimmte und festgelegte Zwecke notwendig ist. Sie geht deshalb auch von dem Prinzip aus, daß das Recht auf Privatsphäre und Selbstbestimmung dadurch am wirksamsten geschützt wird, daß möglichst keine personenbezogenen Daten erhoben werden. Im Hinblick auf die Umsetzung dieses Grundsatzes

fördert die Europäische Kommission die Entwicklung und Anwendung datenschutzfreundlicher Technologien, insbesondere im Rahmen des elektronischen Handels, sowie beispielsweise die Möglichkeit anonymen Zugangs zu Netzen und anonyme Zahlungsweisen [KOM97].

## 2.2 Grundlegende Betrachtung von Informationssystemen

Betrachtet man traditionelle *informationsverarbeitende Systeme in ihrer komplexen Gesamtheit*, so sind einige klassische Einzelprozesse (Systemelemente) identifizierbar, in denen üblicherweise solche Daten, die zur Identifizierung des Benutzers geeignet sind, anfallen, bearbeitet und gespeichert werden:

- Autorisierung (Vergabe einer Berechtigung und eines Berechtigungsprofils zur Nutzung des Systems z. B. bei Vertragsabschluß, Personalisierung von Chipkarten usw.)
- Identifikation und Authentikation (Nachweisführung des Benutzers über seine grundsätzliche Berechtigung zur Nutzung des Systems)
- Zugriffskontrolle (Prüfung des Berechtigungsprofils relativ zu der gewünschten Aktion/Dienstleistung des Systems)
- Protokollierung (Festhalten von Aktionen gemeinsam mit Angaben zum Benutzer zum Zwecke der Nachweisführung)
- Abrechnung (Rechnungsstellung der erbrachten und in Anspruch genommenen Systemleistungen an den Benutzer)

Als Begründung für die jeweils erhobenen, anfallenden, gespeicherten und verarbeiteten personenbezogenen Daten werden überwiegend Abrechnungszwecke, verbesserte Kundenbetreuung, statistische sowie Kontrollzwecke angegeben.
Die tatsächliche Identität des Benutzers ist für die Funktionalität eines IuK-Systems grundsätzlich jedoch nicht erforderlich. Allenfalls in bestimmten Fällen zur Autorisierung, Abrechnung und Protokollierung könnte die tatsächliche Identität des Benutzers erforderlich sein und müßte dort offengelegt werden bzw. bekannt sein. In den übrigen Prozessen ist dies nicht notwendig (vgl. [RGB95]).
Wenn in einem System stattfindende Aktionen überwacht werden müssen und diese Überwachung nicht ausschließlich innerhalb des Systems möglich ist, so ist eine Protokollierung erforderlich. So ist z. B. die in den Datenschutzgesetzen des Bundes und der Länder vorgeschriebene Eingabekontrolle (z. B. Nr. 7 der Anlage zu § 9 BDSG) i. d. R. nur mit Hilfe der Protokollierung realisierbar, da die Zulässigkeit der Datenerhebung bzw. der Datenspeicherung nicht maschinell geprüft werden kann.
Bereits bei der Konzeption von IuK-Systemen sollte daher generell und für jeden einzelnen Prozeß untersucht werden, ob Daten zur wahren Identität des Einzelnen zur Verfügung stehen müssen oder ob eine anonyme oder pseudonyme Gestaltung in Frage kommt (siehe Abschnitte „Anonymisierung“ und „Pseudonymisierung“).

# 3. Anonymisierung

Anonymisierung ist eine Veränderung personenbezogener Daten derart, daß die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.
In den Datenschutzgesetzen von Bund und Ländern ist Anonymisierung unterschiedlich definiert. So ist in einigen Datenschutzgesetzen (z. B. § 3 Abs. 7 BDSG, Art. 4

Abs. 8 BayDSG, § 3 Abs. 7 LDSGRP, § 2 Abs. 7 DSG-LSA) für eine Anonymisierung bereits „das Verändern personenbezogener Daten derart, daß die Einzelangaben über persönliche oder sachliche Verhältnisse *nicht mehr oder nur mit einem unverhältnismäßig hohen Aufwand an Zeit, Kosten und Arbeitskraft* einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können“ ausreichend. Andere Datenschutzgesetze (z. B. § 3 Abs. 7 Nr. 5 DSGMV, § 3 Abs. 2 Nr. 4 SächsDSG, § 2 Abs. 2 Nr. 7 LDSGSH) stellen höhere Anforderungen. Hier wird unter Anonymisieren „das Verändern personenbezogener Daten derart, daß die Einzelangaben über persönliche oder sachliche Verhältnisse *nicht mehr* einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können“, verstanden.
Die Qualität der Anonymisierungsprozedur hängt von verschiedenen Einflußfaktoren ab. Entscheidend hierfür sind der Zeitpunkt der Anonymisierung, die Rücknahmefestigkeit der Anonymisierungsprozedur, die Mächtigkeit der Menge, in der sich der Betroffene verbirgt, und die Verkettungsmöglichkeit von einzelnen Transaktionen desselben Betroffenen.
Auch konkrete Einzelangaben in einem Datensatz/einer Transaktion (z. B. Beruf/Amt = Bundeskanzler, konkrete Einkommensangaben) sind für die Qualität der Anonymisierungsprozedur von Bedeutung und können die Mächtigkeit der Menge, in der sich der Betroffene verbirgt, verringern. Sind im Wertebereich Werte vorhanden, die die Anonymität gefährden, müssen sie mit anderen zusammengefaßt werden. Ist eine solche Veränderung aus technischen oder inhaltlichen Gründen nicht möglich, kann keine Anonymität erreicht werden.
Das Ziel datenschutzfreundlicher Technologien ist es unter anderem, Daten schon ohne Personenbezug zu erheben oder bereits personenbezogen erhobene Daten so bald wie möglich zu anonymisieren. Ein Höchstmaß an Anonymität wird erreicht, wenn personenbezogene Daten gar nicht erst entstehen. Gelungene Beispiele hierfür sind anonyme Telefonkarten und anonyme Zahlkarten im öffentlichen Personennahverkehr. Beispiele für die Anwendung der Anonymisierung sind im Bereich der Statistik und in der Forschung zu finden.

### 4. Pseudonymisierung

Pseudonymisierung 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.
Dazu werden beispielsweise die Identifikationsdaten durch eine Abbildungsvorschrift in ein willkürlich gewähltes Kennzeichen (das Pseudonym) überführt. Ziel eines solchen Verfahrens ist es, nur bei Bedarf und unter Einhaltung vorher definierter Rahmenbedingungen den Personenbezug wieder herstellen zu können. Die Reidentifizierung kann mitunter auch ausschließlich dem Betroffenen vorbehalten bleiben. Mit Referenz- und Einweg-Pseudonymen (siehe folgende Unterabschnitte) versehene Daten sind jedoch weiterhin personenbezogene Daten, da sie einer bestimmten oder bestimmbaren Person zugeordnet werden können.
Das Mittel der Pseudonymisierung sollte insbesondere dort eingesetzt werden, wo Anonymisierung nicht möglich ist.
Die Qualität der Pseudonymisierungsprozedur hängt von den gleichen Einflußfakto-

ren ab, wie die Stärke der Anonymisierungsprozedur, nämlich vom Zeitpunkt der Pseudonymisierung, von der Rücknahmefestigkeit der Pseudonymisierungsprozedur, von der Mächtigkeit der Menge, in der sich der Betroffene verbirgt, und von der Verkettungsmöglichkeit von einzelnen Transaktionen/Datensätzen desselben Betroffenen. Insbesondere können Transaktionen/Datensätze, die unter demselben Pseudonym getätigt/gespeichert wurden, miteinander verkettet werden.
Unter gleichen Bedingungen ist die Anonymisierung datenschutzfreundlicher als die Pseudonymisierung. Das Pseudonym kann dazu benutzt werden, den Personenbezug wiederherzustellen. Ansonsten kann ohne Berücksichtigung der genannten Faktoren nicht pauschal beurteilt werden, ob die Anonymisierung oder die Pseudonymisierung datensparsamer ist.
Je nach Verknüpfbarkeit und dem Geheimnisträger des Pseudonyms kann der Personenbezug

- nur vom Betroffenen (selbstgenerierte Pseudonyme),
- nur über eine Referenzliste (Referenz-Pseudonyme) oder
- nur unter Verwendung einer sog. Einweg-Funktion mit geheimen Parametern (Einweg-Pseudonyme)

wiederhergestellt werden.
Pseudonyme ermöglichen es, den Personenbezug herzustellen, so daß die Identität der Person nur in den vorab bestimmten Einzelfällen erkennbar wird.
Pseudonyme sollen zufällig und nicht vorhersagbar gewählt werden. Die Menge der möglichen Pseudonyme soll so mächtig sein, daß bei zufälliger Auswahl nicht zweimal das gleiche Pseudonym generiert wird. Ist eine hohe Sicherheit erforderlich, muß die Menge der Pseudonymkandidaten mindestens so mächtig sein wie der Wertebereich sicherer kryptographischer Hashfunktionen (siehe Abschnitt „Hashfunktionen“).
Pseudonyme sollten insbesondere nicht anwendungsübergreifend, sondern nur für jeweils ein Verfahren eingesetzt werden. Jede anwendungsübergreifende Benutzung eines einzigen Pseudonyms würde die Gefahr erhöhen, daß aus sämtlichen mit dem Pseudonym verbundenen Daten ein detailliertes Personenprofil erstellt werden kann, das wiederum den Rückschluß auf eine bestimmte Person erleichert. Aber auch innerhalb einer Anwendung ist die Verwendung nur eines einzigen Pseudonyms nicht unproblematisch.

## 4.1 Selbstgenerierte Pseudonyme

Selbstgenerierte Pseudonyme werden ausschließlich vom Betroffenen vergeben und nicht mit Identitätsdaten gleichzeitig verwendet oder gespeichert. Somit kann auch der Personenbezug nur vom Betroffenen selbst wiederhergestellt werden, i. d. R. nicht jedoch durch den Betreiber der IuK-Systeme.
Erfüllt die Menge der möglichen Pseudonyme die obigen Kriterien nicht, so ist ein Abgleich der selbstgewählten Pseudonyme mit den schon benutzten notwendig. Dies ist nur akzeptabel, wenn sich im „Trefferfall“ nicht ermitteln läßt, wer das Pseudonym ursprünglich gewählt hat. Kann das für eine Person in Frage kommende Pseudonym vorhergesagt werden, so kann zumindest ermittelt werden, ob Daten zu dieser Person bereits gespeichert sind. Diese Vorhersage dürfte z. B. bei selbstgewählten Vor- und Zunamen oder beim wählbaren Anteil von Autokennzeichen oft funktionieren.

Selbstgenerierte Pseudonyme sollten Verwendung finden bei wissenschaftlichen Studien, die einerseits aggregierte Auskünfte über bestimmte Personengruppen geben sollen, andererseits aber auch den Betroffenen die Möglichkeit einräumen möchten, sich über ihre persönlichen Einzelergebnisse unerkannt zu informieren. Da es für die auswertende Stelle nicht erforderlich ist, die erhobenen Daten personenbezogen auszuwerten, kann statt des Namens ein vom Betroffenen selbstgewähltes Pseudonym verwendet werden, mit dessen Hilfe der Betroffene - und nur er selbst - die Ergebnisse in Erfahrung bringen kann, die ausschließlich seinen Einzelfall betreffen.

## 4.2 Referenz-Pseudonyme

Bei Referenz-Pseudonymen kann der Personenbezug über entsprechende Referenzlisten wiederhergestellt werden. Ohne Hinzuziehung entsprechender Referenzlisten ist die Identität des Betroffenen i. d. R. jedoch nicht zu ermitteln.
Referenz-Pseudonyme eignen sich für Anwendungen, bei denen der Betroffene nur in bestimmten Ausnahmefällen ermittelt werden muß, beispielsweise bei fehlerhaften Zahlungsvorgängen. Um zu erreichen, daß die Pseudonyme nicht aufgelöst werden, ist es notwendig, die Referenzliste räumlich und organisatorisch getrennt von den pseudonymisierten Datensätzen z. B. in einer Vertrauensstelle (siehe Abschnitt „Vertrauensstellen“) zu speichern. Als besserer Schutz gegen die unbefugte Aufdekkung eines Pseudonyms können die Codes, die in den Referenzlisten zur Wiederherstellung des Personenbezugs gespeichert sind, auch auf mehrere Vertrauensstellen verteilt werden. Nur wenn sämtliche arbeitsteilig operierenden Akteure bereit sind, ihre jeweiligen Referenzlisten zur Verfügung zu stellen, kann das verwendete Pseudonym einer bestimmten Person zugeordnet werden.
Einweg-Pseudonyme
Einweg-Pseudonyme zeichnen sich dadurch aus, daß sie mittels Einweg-Funktion aus personenbezogenen Identitätsdaten - zumeist auf der Basis asymmetrischer Verschlüsselungsverfahren - gebildet werden. Dabei werden Einweg-Funktionen verwendet, die mit hoher Wahrscheinlichkeit ausschließen, daß die Identitätsdaten zweier Personen auf ein gemeinsames Pseudonym abgebildet werden.
Der Zusammenhang zwischen Identitätsdaten und Pseudonym wird folglich nicht mehr durch eine Tabelle (wie bei Referenzpseudonymen), sondern durch eine explizit formulierte (parametrisierbare) Vorschrift hergestellt. Die Sicherheit sollte nicht auf der Geheimhaltung dieser Vorschrift, sondern auf der Geheimhaltung der Parameter beruhen. Bei Referenzpseudonymen ist statt dessen die Tabelle geheimzuhalten.
Sowohl der Betroffene als auch der Betreiber des Verfahrens können nur dann depseudonymisieren, wenn sowohl die Parameter bekannt sind als auch die Abbildungsvorschrift bekannt ist/benutzt wird:

- Soll festgestellt werden, zu welcher Person ein bestimmtes Pseudonym zugeordnet ist, muß lediglich mittels der Abbildungsvorschrift aus den Identitätsdaten sämtlicher Personen, aus deren Reihen der Betroffene ermittelt werden soll, das jeweilige Pseudonym gebildet und mit dem zuzuordnenden Pseudonym verglichen werden.
- Andererseits läßt sich ermitteln, ob eine oder mehrere Personen mit einem Pseudonym in einem Datenbestand verzeichnet ist (sind), wenn Identitätsdaten und Abbildungsvorschrift (samt Parameter) bekannt sind. Falls dies zutrifft, sind auch die unter den entsprechenden Pseudonymen gespeicherten Daten zuordenbar.

Der Unterschied zu Referenzpseudonymen besteht darin, daß die Identitätsdaten der Betroffenen in den meisten Anwendungen nicht gespeichert werden müssen. Analog zu den Referenzpseudonymen ist aber auch hier eine Funktionentrennung notwendig: Instanzen, die die Pseudonyme verwalten bzw. die geheimen Parameter kennen und solche, die nur mit pseudonymisierten Daten umgehen, müssen voneinander getrennt werden. Bei Einhaltung dieser Funktionentrennung erscheinen die pseudonymisierten Identitätsdaten für diejenige Instanz, die nur mit den pseudonymisierten Daten umgehen kann, wie anonymisierte Daten.
Einweg-Pseudonyme eignen sich zum einen für Längsschnittuntersuchungen, bei denen nachträglich erhobene personenbezogene Daten mit Bestandsdaten zusammengeführt werden, ohne daß der Personenbezug für die statistische Auswertung der Daten erforderlich ist. Zum anderen können Einweg-Pseudonyme bei Auskunftssystemen eingesetzt werden, die Auskunft über die Zugehörigkeit bzw. Nicht-Zugehörigkeit einer Person zu einer bestimmten Gruppe geben, ohne daß dabei personenbezogene Identitätsdaten gespeichert werden müssen.

## 5. Realisierungshilfen

### 5.1 Hashfunktionen

Hashfunktionen werden in vielfältigem Zusammenhang in Sicherheitsverfahren verwendet, z. B. zur Unterstützung der Authentikation, der Erkennung der Datenunversehrtheit oder dem Urheber- und Empfängernachweis.
Bei einer Hashfunktion handelt es sich um einen Algorithmus, der eine Nachricht (Bitfolge) beliebiger Länge auf eine Nachricht (Bitfolge) fester, kurzer Länge - dem sogenannten Hashwert - abbildet. Eine Hashfunktion soll über folgende Eigenschaften verfügen:
- Einwegfunktions-Eigenschaft, d.h. zu einem vorgegebenen Wert soll es mit vertretbarem Aufwand unmöglich sein, eine Nachricht zu finden, die eben diesen Wert als Hashwert hat. Dieser „vertretbare Aufwand“ hängt vom Entwicklungsstand der einsetzbaren Technik und den Sicherheitsanforderungen des Anwenders ab.
- Kollisionsfreiheit, d.h. es soll mit vertretbarem Aufwand unmöglich sein, zwei Nachrichten mit demselben Hashwert zu finden.

Bei der Erzeugung von Pseudonymen ist besonders die Kollisionsfreiheit gefordert. Hashfunktionen sind im Gegensatz zu vielen Verschlüsselungsalgorithmen öffentlich bekannt und unterliegen damit intensiven Analysen von Experten, so daß ihre Stärken und Schwächen im allgemeinen bekannt sind. Zu den bekanntesten gehören MD4, MD5, SHA1, RIPEMD und RIPEMD160. Einige davon haben sich als unbrauchbar zur Erzeugung von Pseudonymen herausgestellt, da sie nicht kollisionsfrei sind. In Europa hat sich RIPEMD160 als Standard durchgesetzt. RIPEMD160 ist nach ISO/IEC 101183 genormt.
Zur Erzeugung von sicheren Pseudonymen empfiehlt es sich, eine Hashfunktion auszuwählen, die schon länger veröffentlicht und wissenschaftlich untersucht ist. Verschiedene Verfahren sind denkbar, vor Umsetzung ist allerdings unbedingt der Rat von Experten einzuholen.

### 5.2 Digitale Signaturen

Eine digitale Signatur ist ein mit einem privaten Signaturschlüssel erzeugtes Siegel zu

digitalen Daten, das mit Hilfe eines zugehörigen öffentlichen Schlüssels, der mit einem Signaturschlüssel-Zertifikat versehen ist, den Inhaber des Signaturschlüssels und die Unverfälschtheit der Daten erkennen läßt [SigG].
Verfahren zur digitalen Signatur sind aus elektronischen Kommunikationssystemen bekannt. Mit der digitalen Signatur kann der Nachweis der Urheberschaft eines Objektes (z. B. eines digitalen Schriftstücks wie einer E-Mail (elektronische Post)) erbracht werden. Ein direkter Rückschluß auf denjenigen, der das Objekt signierte, ist möglich - ja gewollt. Da die digitale Signatur (u. a. durch Anwendung von Hashfunktionen) jeweils speziell über dem zu signierenden Objekt gebildet wird, ist damit gleichzeitig die Integrität des signierten Objekts nachprüfbar.
Erzeugt der Betroffene selbst dezentral die Schlüssel, handelt es sich in gewisser Weise um ein spezielles selbstgeneriertes Pseudonym, weil der spezielle (private) Signaturschlüssel (zur Erzeugung der digitalen Signatur) nur dem rechtmäßigen Benutzer bekannt und zugänglich ist.

### 5.3 (Signaturschlüssel-)Zertifikat

Ein Zertifikat ist eine mit einer digitalen Signatur versehene digitale Bescheinigung über die Zuordnung eines öffentlichen Signaturschlüssels zu einer natürlichen Person [SigG]. Dabei handelt es sich um ein spezielles selbstgeneriertes Pseudonym der das Zertifikat ausstellenden Institution, mit dem die Zuordenbarkeit zweier, voneinander abhängiger Pseudonyme zu einer Person (öffentlicher Signaturschlüssel und zugehöriger privater Signaturschlüssel) sichergestellt wird.

### 5.4 Blinde digitale Signatur

Eine „blinde digitale Signatur“ stellt eine Variante der digitalen Signatur dar, mit der die Anonymität des Benutzers gewahrt wird. Der Unterschied zwischen beiden Signaturformen besteht darin, daß bei der blinden digitalen Signatur kein Rückschluß auf denjenigen möglich ist, der das signierte Objekt verwendet (Beispiel: eine Banknote entspricht einem blind digital signierten Objekt; der Benutzer der Banknote bleibt anonym). Die Echtheit des Objektes wird von einem außenstehenden Dritten durch seine digitale Signatur bestätigt (Zertifikat), der Benutzer tritt mit seiner eigenen Identität nicht in Erscheinung. Diese Form der digitalen Signatur wird z. B. für „Ecash“ (siehe Anlage, Abschnitt „Elektronische Zahlungssysteme“) verwendet.

### 5.5 Biometrische Verfahren

Bei der biometrischen Verschlüsselung werden körperliche Merkmale wie Augennetzhaut, Fingerabdruck usw. z.B. durch optische Geräte oder besondere Chipkarten derart digitalisiert und zu einer digitalen Zeichenfolge aufbereitet, daß diese als eindeutiges Merkmal für die betreffende Person verwendet werden können. Zur Feststellung von Identität und Authentizität der Person als Benutzer eines IuK-Systems ist das betreffende körperliche Merkmal erneut zu digitalisieren und mit dem gespeicherten Muster zu vergleichen. Der Berechnungsvorgang zur Erzeugung dieser identifizierenden Zeichenfolge ist nicht umkehrbar, er stellt eine Einwegfunktion dar. Insoweit ist ein derart erzeugtes biometrisches Merkmal einem Einweg-Pseudonym gleichzusetzen.

## 5.6 Vertrauensstellen

Vertrauensstellen sind für die Realisierung bestimmter Sicherheitsdienste und für die Akzeptanz ganzer IT-Infrastrukturen erforderlich. Die Funktion einer solchen Vertrauensstelle wird oft mit der eines Notars, also einer neutralen, unbeteiligten Instanz, verglichen. Dieser Instanz müssen in der Regel alle Beteiligten (das sind der Benutzer und ggf. seine Kommunikations- und Geschäftspartner sowie ggf. die Betreiber der verwendeten IuK-Systeme) im Hinblick darauf vertrauen, daß sie ihre Aufgaben korrekt erfüllt.
Der Benutzer vertraut beispielsweise darauf, daß die Geheimhaltung seiner wahren Identität bei Verwendung eines Pseudonyms gewährleistet wird bzw. daß - wenn rechtmäßig seine Identität aufgedeckt wird - er unverzüglich informiert wird, wann, gegenüber wem und warum die Aufdeckung erfolgte.
Das Vertrauen des Betreibers eines IuK-Systems erstreckt sich darauf, daß zur Wahrung seiner legitimen Interessen im definierten und vereinbarten Bedarfsfall (z. B. Aufdeckung von Leistungsmißbrauch) die tatsächliche Identität des Benutzers offengelegt wird.
Aufgaben von Vertrauensstellen können, neben den kommerziellen oder öffentlichen Trust Centern als sogenannte Trusted Third Parties (TTPs), auch unter der Kontrolle des Benutzers arbeitende Personal Trust Center (PTCs) übernehmen, z. B. „intelligente“ Sicherheitstoken wie SmartCards. Man unterscheidet vier Aufgabenbereiche, die von Vertrauensstellen erfüllt werden *können*:
*Schlüsselmanagement*
- Schlüsselgenerierung und -zurücknahme
- Speicherung von (öffentlichen) Schlüsseln
- Verteilung und Löschung/Sperrung von Schlüsseln

*Beglaubigungsleistungen*
- Ausstellung von Zertifikaten für öffentliche Schlüssel
- Personalisierung von Schlüsseln: Zuordnung zu einem Benutzer (Identität oder Pseudonym)
- Registrierung von Benutzern (Identitätsbeglaubigung und ggf. Zuordnung zu Pseudonymen)
- Personalisierung von PTCs
- Zertifizierung/Zulassung von TTPs

*Treuhänderfunktion*
treuhänderisches Hinterlegen beispielsweise von
- personenbezogenen Daten, z.B. Identifikationsdaten
- Schlüsseln zur Datensicherung

*Serverfunktionen*
- Online-Bereitstellung von Informationen für die Sicherheitsinfrastruktur, z.B.
- Verzeichnisse von (öffentlichen) Benutzerschlüsseln
- Authentisierungsinformationen (z.B. bei Kerberos)
- Zeitstempel
- Warnungen bei kritischen Sicherheitsereignissen

Um eine größtmögliche Vertrauenswürdigkeit der Vertrauensstellen zu erreichen, ist ein hohes Maß an Zuverlässigkeit und Fachkunde erforderlich. Die geforderte Neutra-

lität und Unabhängigkeit einer Vertrauensstelle darf nicht durch Interessenkollisionen eingeschränkt oder gefährdet werden; solche Probleme können durch ungeeignete Kombinationen mehrerer der oben genannten (Teil-)Aufgaben bzw. Rollen entstehen. Darüber hinaus sollten Aufgaben mit besonderen Sicherheitsanforderungen nicht von einer einzigen Vertrauensstelle erledigt, sondern auf mehrere Stellen verteilt werden. Außerdem sollten die Vertrauensstellen nach einer veröffentlichten Policy arbeiten, die eine klare Darstellung der Aufgaben und Sicherheitsanforderungen umfaßt und die möglichst benutzerüberprüfbar realisiert ist [FHK95].
Nicht alle der o. a. Aufgaben von Trust Centern sind zur Datenvermeidung und damit zur verstärkten Wahrung der Privatheit des Einzelnen geeignet, wie z. B. insbesondere die Generierung von Schlüsseln in Vertrauensstellen und das Bereithalten von öffentlichen Schlüsseln mit Identitäten.
Als Beispiele für Vertrauensstellen können hier die Funktionalität von First Virtual (siehe Anlage, Abschnitt „Elektronische Zahlungssysteme“) sowie die im Entwurf des Signaturgesetzes [SigG] beschriebenen Zertifizierungsstellen für die öffentlichen Schlüssel im Rahmen der digitalen Signatur genannt werden.
Im übrigen gibt es mittlerweile bereits eine Reihe von Unternehmen in der Bundesrepublik Deutschland, die einige oder alle der o.a. Dienstleistungen kommerziell anbieten.

## 5.7 Der Identity Protector

Wie oben dargestellt, lassen sich IuK-Systeme, für die eine anonyme Nutzungsform nicht vollständig möglich ist, derart in unterschiedliche Einzelprozesse zerlegen, daß unmittelbar personenbezogene Daten (Identitätsdaten) nur erhoben, gespeichert und verarbeitet werden, wo dies unabdingbar nötig ist.
Durch geeignete technische Maßnahmen muß dafür Sorge getragen werden, daß die Bereiche des IuK-Systems, die den vollen Personenbezug mit den Identitätsdaten benötigen, strikt von jenen getrennt werden, die nur mit einem Pseudonym auskommen. D. h., nur die tatsächlich und unmittelbar benötigten Daten stehen dem jeweiligen Prozeß zur Verfügung. Eine Zusammenführung von Identitätsdaten und Pseudonymdaten ist nur unter vorab und genau definierten Umständen möglich.
Diese Aufgaben kann ein „Identity Protector“ leisten. Er kann als Systemelement (Prozeß) betrachtet werden, das den Austausch von Identitätsdaten und Pseudonymdaten zwischen den übrigen Systemelementen steuert [BO96] [RGB95].
Für einen „Identity Protector“ sind verschiedene Ausprägungsformen möglich:

a) eigenständiges Element in einem IuK-System
b) eigenständiges IuK-System, das unter der Kontrolle des Benutzers steht
c) eigenständiges IuK-System, das unter der Kontrolle einer Vertrauensstelle steht (siehe Unterabschnitt „Vertrauensstellen“)

Im Falle a) sollte der Identity Protector ein - auch für den Betreiber des IuK-Systems - unveränderbarer Baustein sein. Die Realisierung ließe sich als Softwarebaustein im IuK-System selbst, im zugrundeliegenden Betriebssystem oder auch als Hardwarekomponente mit zugehöriger Software (z. B. als „Black-Box-Lösung“) bewerkstelligen.
Im Falle b) wäre eine Abbildung des Identity Protectors z. B. in Form einer Smartcard als intelligentes Sicherheitstoken und als PTC möglich.

Der Identity Protector kann folgende Funktionalitäten leisten:
- kontrollierte Offenlegung und Freigabe der Identität
- Generierung von Pseudonymen
- Umsetzung von Pseudonymen in weitere Pseudonyme
- Umsetzung von Identitäten in Pseudonyme (Pseudonymisierung)
- Umsetzung von Pseudonymen in Identitäten (Depseudonymisierung)
- vorbeugende Mißbrauchsbekämpfung (u.a. durch die erstgenannte Funktionalität)

Zur Realisierung eines Identity Protectors stehen alle oben genannten Hilfsmittel zur Verfügung. Nicht alle diese Techniken müssen aber für jede Ausprägung eines Identity Protectors verwendet werden.
Die Funktionstüchtigkeit und Unveränderbarkeit des Identity Protectors müßte konsequenterweise mittels Zertifizierung und (kryptographischer) Versiegelung durch eine unabhängige Vertrauensstelle sichergestellt werden.

## 6. Zusammenfassung und Handlungsempfehlung

Datenvermeidung und Datensparsamkeit spielen in der Anwendung der IuK-Technologie bisher nur eine untergeordnete Rolle. Um zukünftig den Ansprüchen an Datenschutzfreundlichkeit gerecht zu werden, muß das Streben nach Datensparsamkeit die Entwicklung und den Betrieb von IuK-Systemen genauso beeinflussen wie die Forderung nach Datensicherheit.
Für die Akzeptanz von Multimedia wird die Sicherstellung des Datenschutzes und der Privatheit des Einzelnen von entscheidender Bedeutung sein. Es ist absehbar, daß in Zukunft Produkte und Dienstangebote bei im übrigen gleicher Qualität und gleichem Preis Wettbewerbsvorteile haben werden, wenn sie datenschutzfreundlicher als die anderen sind. Ein Produkt oder Dienstangebot, das mit möglichst wenig personenbezogenen Daten seiner Nutzer auskommt, wird dem anderen vorgezogen, das umfangreiche Datenspuren erzeugt.
Die Datenschutzbeauftragten des Bundes und der Länder wollen diesen Prozeß beschleunigen und in Zusammenarbeit mit Herstellern und Anbietern auf datenschutzgerechte Lösungen hinarbeiten.
Neue Informations- und Kommunikationssysteme sollten folgende Grundsätze beachten:
- IuK-Systeme sollten so gestaltet werden, daß keine personenbezogenen Daten erhoben, gespeichert und verarbeitet werden, d. h. daß eine anonyme Nutzung möglich ist.
- In den Systemteilbereichen, in denen für einen definierten Zeitraum personenbezogene Daten für die spezifische Funktionalität unabdingbar sind, sollte festgelegt werden, ob und wann eine Anonymisierung, oder falls dies nicht möglich ist, eine Pseudonymisierung erfolgen kann.

Um diese Grundsätze bei der Entwicklung oder Modifizierung von IuK-Systemen in ausreichendem Maße berücksichtigen zu können, ist folgende Vorgehensweise empfehlenswert:
Zunächst müssen datenverarbeitende Systeme und Teilsysteme einschließlich ihrer Schnittstellen definiert werden. Bei dieser Definition muß auch eine Unterscheidung derjenigen Systeme und Teilsysteme erfolgen, in denen
1. ohne personenbezogene Daten gearbeitet werden kann,

2. personenbezogene Daten anonymisiert werden können,
3. personenbezogene Daten pseudonymisiert werden können bzw.
4. der direkt herstellbare Personenbezug unvermeidlich ist.

Ist eine Anonymisierung oder eine Pseudonymisierung erforderlich, so ist für das jeweilige System/Teilsystem eine entsprechende Prozedur zu finden,

- die die personenbezogenen Daten frühestmöglich anonymisiert bzw. pseudonymisiert,
- die nicht unzulässig beeinflußt werden kann (Integrität),
- die aus dem System/Teilsystem nicht mit geringem Aufwand wieder entfernt werden kann (Rücknahmefestigkeit),
- die den Betroffenen in einer hinreichend großen Menge möglicher Betroffener verbirgt und
- die die Verkettbarkeit von Einzeldaten oder Transaktionen zu Datenspuren unterdrückt.

Stellt sich heraus, daß die vorhandenen Risiken mit dem so konstruierten System nicht hinreichend reduziert werden können, so müssen ggf. Teile des Definitionsprozesses und Teile des Gestaltungsprozesses wiederholt werden.

Bereits heute ist eine Reihe von Technologien und Hilfsmitteln zur Erreichung von verbessertem Datenschutz durch Technik verfügbar. Die Technologie, die dafür gesorgt hat, daß personenbezogene Daten gespeichert, genutzt und weitergegeben werden können, ist auch zur Wahrung der Privatheit des Einzelnen nutzbar. Diese Möglichkeiten der modernen Datenschutztechnologie, die mit dem Begriff *„Privacy enhancing technology (PET)“* eine Philosophie der Datenvermeidung und der Datensparsamkeit beschreibt und ein ganzes System technischer Maßnahmen umfaßt, sollten genutzt werden.

Verbraucher sollten durch gezielte Nachfrage die Verwendung datenschutzfreundlicher Technologien in IuK-Systemen fordern und fördern.

Auch der Gesetzgeber muß die Verwendung datenschutzfreundlicher Technologien fordern und fördern.

An Industrie und Dienstleistungsanbieter ergeht der Appell, für den Verbraucher transparentere Systeme zu schaffen und datenschutzfreundliche Technologien verstärkt in ihre Systeme einzubauen.

Anlage 1

*Literaturverzeichnis*


[BD776] Entschließung zu der Empfehlung an den Europäischen Rat „Europa und die globale Informationsgesellschaft“ und zu der Mitteilung der Kommission „Europas Weg in die Informationsgesellschaft: Ein Aktionsplan“, Bundesrat, Drucksache 776/96, 10.10.1996, Bonn

[BO96] John Borking: Der Identity Protector; Datenschutz und Datensicherheit (DuD) 11/96, Verlag Vieweg, Wiesbaden, 1997, S. 654-658

[BlSch] Bleumer, G., Schunter, M.: Datenschutzorientierte Abrechnung medizinischer Leistungen; Datenschutz und Datensicherheit (DuD) 2/97, Verlag Vieweg, Wiesbaden, 1997, S. 88-97

[CC] http://www.cybercash.com

[DIGI] http://www.digicash.com

[FV] http://www.fv.com

[FHK95] Dirk Fox, Patrick Horster, Peter Kraaibeek: Grundüberlegungen zu Trust Centern; In: Patrick Horster (Hg.): Trust Center - Grundlagen, rechtliche Aspekte, Standardisierung und Realisierung; DuD Fachbeträge, Braunschweig/Wiesbaden Vieweg 1995, S. 1-10

[FJKP 95] Hannes Federrath, Anja Jerichow, Dogan Kesdogan, Andreas Pfitzmann: Technischer Datenschutz in öffentlichen Mobilkommunikationsnetzen; Wissenschaftliche Zeitschrift der TU Dresden 44/6 (1995) 4ff.

[GZ96] Grimm, R.; Zangeneh, K: Cybermoney im Internet. Ein Überblick über neue Bezahlsysteme im Internet (Gesellschaft für Mathematik und Datenverarbeitung, Institut für Telekooperationstechnik); Darmstadt, Januar 1996

[IuKDG] Gesetz zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste (Informations- und Kommunikationsdienste-Gesetz - IuKDG), Deutscher Bundesrat, Drucksache 420/97, 13.06.97, Bonn

[KOM97] Kommissionsvorschlag zum 5. Rahmenprogramm für Forschung und technologische Entwicklung, KOM (97)142 und Mitteilung der Kommission zum elektronischen Handel, KOM (97)157, http://www.cordis.lu/esprit/src/ecomcom.htm

[MDStV] Staatsvertrag über Mediendienste (Mediendienste-Staatsvertrag), 12.02.97, (Unterzeichnung vom 20.01.-12.02.1997)

[MON] http://www.mondex.com

[RaPM 96] Kai Rannenberg, Andreas Pfitzmann, Günter Müller: Sicherheit, insbesondere mehrseitige IT-Sicherheit; it+ti 38/4 (1996), S. 7-10

[RGB95] H. van Rossum, H. Gardeniers, J. Borking u.a.: „Privacyenhancing Technologies, The path to anonymity“, Volume I u. II, Achtergrondstudies en Verkenningen 5b, Registratiekamer, The Netherlands & Information and Privacy Commissioner/Ontario, Canada, August 1995

[RDLM 95] Kai Rannenberg, Herbert Damker, Werner Langenheder, Günter

Müller: Mehrseitige Sicherheit als integrale Eigenschaft von Kommunikationstechnik; In: Kubicek, Müller, Neumann, Raubold, Roßnagel (Hg.): Jahrbuch Telekommunikation & Gesellschaft, 1995, R. v. Decker's Verlag, Heidelberg, 1995, S. 254 - 260

[SigG] Signaturgesetz, Art. 3 des Gesetzes zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste (Informations- und Kommunikationsdienste-Gesetz - IuKDG), Deutscher Bundesrat, Drucksache 420/97, 13.06.97, Bonn

[SiKT97] CeBIT-Sonderseite des Kollegs „Sicherheit in der Kommunikationstechnik", http://www.iig.uni-freiburg.de/dbskolleg/cebit97/, März 1997

[SSONET] Das SSONET-Projekt: „Sicherheit und Schutz in offenen Netzen (SSONET)", TU Dresden, 27.08.96, http://mephisto.inf.tu-dresden.de/RESEARCH/ssonet/ssonet.html

[ZWIS] Zwissler, S.: Risikoreduktion bei elektronischer Auslieferung; Datenschutz und Datensicherheit (DuD), 7/97, Verlag Vieweg, Wiesbaden, 1997, S. 411-415

[95/46/EG] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten sowie zum freien Datenverkehr, Amtsblatt Nr. L 281, S. 31

Anlage 2,
*Anwendungsmöglichkeiten und Einsatzfelder*

## 1. Datenschutz im Medienbereich

### 1.1 Allgemeines

Die „Informationsgesellschaft“ umfaßt sowohl den Freizeitbereich als auch die Arbeitswelt. „Multimedia“ ist das Schlagwort, das die verschiedenen Medientypen wie Text, Ton, Bild und Video zusammenführt, ohne eine neue Technologie an sich zu bilden.
Multimedia-Angebote mit besonderer Datenschutzrelevanz sind die Tele- und Mediendienste.

*Teledienste* sind elektronische Informations- und Kommunikationsdienste, die für eine individuelle Nutzung von kombinierbaren Daten wie Zeichen, Bilder oder Töne bestimmt sind und denen eine Übermittlung mittels Telekommunikation zugrunde liegt [IuKDG], z. B. Telebanking, elektronischer Datenaustausch, Datendienste, Internet, Online-Dienste, Telespiele, Teleshopping, Telemedizin, Telearbeit.

*Mediendienste* sind an die Allgemeinheit gerichtete Informations- und Kommunikationsdienste in Text, Ton oder Bild, die unter Benutzung elektromagnetischer Schwingungen ohne Verbindungsleitung oder längs oder mittels eines Leiters verbreitet werden [MDStV]. Sie bestehen aus Verteil- und Abrufdiensten. Beispiele für Mediendienste sind Pay-TV, elektronische Presse, Teletext.

In der Praxis dürfte sich eine strikte Abgrenzung von Telediensten und Mediendiensten als äußerst schwierig erweisen.
Die zur Zeit entwickelten Angebote erstrecken sich von Bildtelefon und Videokonferenzen über Lernprogramme, digitale Nachschlagewerke und Informationssysteme bis zu interaktiven Spielen, Video-on-Demand (Videofilme auf Anforderung), Teleshopping, Online-Diensten und Telemedizin - alles von zu Hause aus zugänglich. Das Fernsehen wandelt sich vom Massenmedium zum individualisierten Informations- und Unterhaltungsmedium mit „Rückkanal“.
Bei Inanspruchnahme der elektronischen Informations- und Kommunikationsdienste entstehen personenbezogene Daten, die nicht nur für Zwecke der Abrechnung nutzbar sind. Sie könnten auch für die Programmanbieter unter Marketingaspekten interessant sein. Es ließen sich detaillierte Informationen gewinnen, wann welcher Nutzer welche Fernsehsendungen, Videos oder elektronische Zeitungsartikel abgerufen, welche Produkte er beim Teleshopping bestellt, wohin er Reisen elektronisch gebucht oder welche Abfragen er in Informationssystemen vorgenommen hat. Das Kommunikations- und Konsumverhalten der Kunden könnte ausgewertet und persönliche Lebensgewohnheiten erforscht werden.
Das Informations- und Kommunikationsdienste-Gesetz des Bundes [IuKDG] und der Mediendienste-Staatsvertrag der Länder [MDStV] haben den Grundsatz der Datensparsamkeit für die Anbieter von Online-Diensten und Internet-Zugängen festgelegt. Eine Registrierung des Nutzerverhaltens ist unzulässig. Die Anbieter von Multimedia-Diensten sind verpflichtet, auch die anonyme Inanspruchnahme und Bezahlung von Informationsdiensten als Option anzubieten, soweit dies technisch möglich und wirtschaftlich zumutbar ist.

Soweit personenbezogene Daten unbedingt erhoben werden müssen, dürfen sie nur mit Einwilligung des Nutzers zu anderen Zwecken, z. B. für Werbung, verwendet werden. Die Nutzer müssen ausführlich über den Umgang mit ihren Daten informiert werden.
Da die elektronischen Informations- und Kommunikationsdienste auf der Telekommunikation beruhen, muß die datenschutzfreundliche Ausgestaltung der Technologie bereits dort ansetzen.

## 1.2 Verfahren und Projekte

- Beim digitalen Fernsehen ist für den Kunden vor allem die Möglichkeit neu, nur für die Programmangebote zu bezahlen, die auch wirklich gesehen wurden. Diese *Pay-per-View-Angebote* werden grundsätzlich verschlüsselt übertragen und müssen für den Empfang dekodiert werden. Hierzu benötigt man eine sogenannte Set-Top-Box, in die der Kunde seine Chipkarte einführt. Für die Freischaltung werden zur Zeit verschiedene technische Verfahren eingesetzt:
- Bei der zentralen Freischaltung muß der Kunde zunächst dem Sender mitteilen, welche Sendung er sehen möchte. Zusammen mit dem Sendesignal werden dann die Nutzernummern der Interessenten unverschlüsselt übertragen, deren Decoder freigeschaltet werden soll.
- Für die lokale Freischaltung durch den Nutzer wird jede Sendung mit einer elektronischen Entgeltinformation (Token) gekoppelt. Die an einer Sendung interessierten Kunden geben ihren Wunsch mit der Fernbedienung an ihre Set-Top-Box weiter, die die Kosten für das Programmangebot von der Guthaben-Chipkarte im Decoder abbucht und die Sendung freischaltet.
  Während bei der zentralen Freischaltung das vom Kunden gewünschte Programmangebot zu Abrechnungszwecken beim Sender gespeichert wird und durch die unverschlüsselte Übertragung der Nutzernummern sogar im gesamten Netz mit geringem Aufwand ausgewertet werden kann, braucht der Kunde bei der lokalen Freischaltung keine personenbezogenen Daten aus der Hand zu geben.
- Für einige Internet-Dienste, z. B. E-Mail, News oder WWW, stehen mehrere Pseudo-Anonymous-Server zur Verfügung, die die Absenderkennung durch ein Referenz-Pseudonym ersetzen. Bei den Mixmaster-Remailern wird die Zuordnung des Pseudonyms zum Benutzer nicht gespeichert, so daß keine Reidentifizierung des Absenders vorgenommen werden kann.
- Der Identity Protector von John Borking, Niederlande, ist ein Instrument zum Schutze der Privatsphäre, das die Identität von Personen innerhalb der verschiedenen Prozesse in einem Informationssystem anonymisiert oder pseudonymisiert [RGB95]. Näheres hierzu siehe Grundlagenpapier, Abschnitt 5.7 „Der Identity Protector“.
- Bei dem Projekt Sicherheit und Schutz in offenen Netzen (SSONET) an der Technischen Universität Dresden geht es um den Entwurf, die Implementierung und die Validierung eines Prototyps für mehrseitige Sicherheit [SSONET]. Die zu entwickelnde Sicherheitsarchitektur soll konkret für Internet, Mobile Computing, Teledienste und Workflow-Systeme detailliert untersucht und umgesetzt werden. Das Projekt läuft vom 01.05.96 bis zum 30.04.1999.
- Ebenfalls an der TU Dresden ist in einer Studienarbeit eine Software für ein

Videokonferenzsystem entwickelt worden, mit der sich geheime Informationen unbemerkbar von abhörenden Dritten in die Bewegtbildübertragung einbetten lassen (rechnergestützte Steganografie).

- Auf der CeBIT ´97 hat das interdisziplinäre Ladenburger Kolleg „Sicherheit in der Kommunikationstechnik“ (gefördert von der Gottlieb Daimler- und Karl-Benz-Stiftung), in dem Teilnehmer aus Hochschulen, öffentlichen und privaten Forschungseinrichtungen sowie führenden Unternehmen der Branche mitarbeiten, u. a. innovative und datensparsame Protokolle und Topologien für eine Netz- und Dienstestruktur vorgestellt [SiKT97]. Durch eine dezentrale Ansiedlung von Vertrauensinstanzen und sensitiven Daten in Kommunikationsnetzen soll das Risiko des Mißbrauchs reduziert und den Nutzern die Möglichkeit gegeben werden, selbst auszuwählen, welchen Instanzen sie vertrauen.

## 2. Datenschutz bei elektronischem Geld

### 2.1 Fälschungssicherheit versus Anonymität

Fälschungssicherheit und Anonymität scheinen zwei Anforderungen an elektronisches Geld zu sein, die sich auf den ersten Blick grundlegend widersprechen. Daß es dennoch möglich ist, beide Aspekte zu integrieren und somit datenschutzfreundliche Technologien im elektronischen Zahlungsverkehr zu implementieren, wird im folgenden gezeigt.

Kauf- und Zahlungsvorgänge zeichnen sich dadurch aus, daß sowohl der Käufer als auch der Verkäufer die Ware bzw. das Entgelt weitgehend betrugsfrei erhalten. Während beim Handel mit höherwertigen Gütern die Betrugsmöglichkeiten dadurch reduziert werden, daß beide Handelspartner ihre Identität bewußt preisgeben, um ggf. nachträgliche Forderungen besser durchsetzen zu können, erfolgt die Bezahlung niederwertiger Güter traditionell anonym mittels Bargeld. Das Betrugsrisiko ist aufgrund des niedrigen Warenwerts und aufgrund der Anwesenheit beider Handelspartner recht gering.

Geringwertige Güter und Dienstleistungen werden zunehmend nicht mehr mit Bargeld bezahlt, sondern mittels elektronischem Geld als dessen digitale Ausdrucksform. Während sich Bargeld dadurch auszeichnet, daß es während des Bezahlvorgangs intuitiv auf Echtheit überprüft wird, läßt sich elektronisches Geld nicht durch den Empfänger verifizieren. Das Bezahlen erfolgt mittels digitaler Daten, die fälschbar sind. Digitales Geld ist zum einen leicht zu duplizieren, zum anderen sind die Duplikate von den Originalen nicht zu unterscheiden.

Beim Bezahlen im Internet sind zudem der Zahlende und der Entgeltempfänger räumlich voneinander getrennt. Ihre Kommunikation ist normalerweise flüchtig, ungesichert und nicht beweiskräftig. Beim Bezahlen von Informationen ergibt sich zudem die Schwierigkeit, daß der Austausch *Information gegen Geld* nicht zeitgleich erfolgt, sondern in der Regel zuerst die Information übertragen wird (nach dem Grundsatz: „zuerst die Ware, dann das Geld“), so daß sich der Dienstleister nicht unbedingt auf das Bezahlversprechen des in der Regel anonym agierenden Kunden verlassen kann. In umgekehrter Reihenfolge riskiert aber der Kunde, im voraus für etwas zu bezahlen, das er anschließend in der erwarteten Form nicht erhält [ZWIS].

Das erhöhte Manipulationsrisiko von elektronischem Geld wird meistens dadurch kompensiert, daß der Entgeltempfänger die Identität des Zahlenden überprüft (beispielsweise mittels PIN) und dessen Identitätsdaten speichert, um sich im Miß-

brauchsfalle nachträglich noch an den Kunden wenden zu können. Damit wird im Gegensatz zu Bargeld die Anonymität des Kunden aufgehoben, sofern er sich nicht bereits anderweitig offenbart hat, beispielsweise durch Angabe seiner Lieferanschrift oder seiner Internet- oder Electronic-mail-Adresse.
Bleibt das Bezahlen mit elektronischem Geld nicht anonym, besteht die Gefahr, daß die Zahlungsdaten zu detaillierten Nutzungs- bzw. Kundenprofilen ausgewertet werden.
Die Anonymität beim Bezahlen setzt voraus, daß der Kunde nicht nur gegenüber dem Händler oder seiner Bank, sondern gegenüber sämtlichen an der Zahlungsabwicklung beteiligten Akteuren anonym bleibt. Falls die Identität des Kunden durch eine gezielte Zusammenarbeit von Händler und Bank aufgehoben werden kann, kann nicht mehr von Anonymität gesprochen werden.
Durch den Einsatz von Referenz-Pseudonymen (s. Abschnitt 4.2 Hauptteil) kann zumindest die Identität des Kunden gegenüber einzelnen Instanzen, beispielsweise gegenüber dem Händler, verborgen werden. Der Kunde agiert somit nicht vollständig anonym, aber gegenüber einzelnen Akteuren zumindest pseudonym.
Solche Referenz-Pseudonyme sind Voraussetzung für eine arbeitsteilige Datenhaltung. So ist es möglich, daß der Händler zwar Kenntnis über die pseudonym abgewickelten Kaufvorgänge hat, aber den Namen des Käufers nicht kennt. Umgekehrt weiß die Bank zwar den Namen des Kunden, kennt jedoch nur die Kaufsumme und den Händler, wenngleich häufig auch aus dem Händlernamen bereits Kaufvorlieben von Kunden abgeleitet werden können.
Unabhängig davon, ob Zahlungsverfahren eingesetzt werden, die anonymes Bezahlen ermöglichen, ist darauf zu achten, daß die über das Internet übertragenen personenbezogenen Daten zumindest vertraulich bleiben. Ist dies nicht sichergestellt, besteht die Gefahr, daß beispielsweise Kreditkartennummern von Außenstehenden mitgelesen und zur Überweisung auf fremde Konten mißbräuchlich genutzt werden. Dies beeinträchtigt zwar nicht unmittelbar die Datenschutzinteressen des Kunden, kann aber beträchtlich dessen Bankkonto „erleichtern“. Da das Abhörrisiko im Internet sehr hoch ist, läßt sich Vertraulichkeit im Internet nur dadurch garantieren, daß sicherheitsrelevante Zahlungsdaten verschlüsselt übertragen werden.

## 2.2 Klassifizierung von elektronischem Geld

Elektronisches Geld unterscheidet sich durch mehrere Merkmale. Diese etwas ausführlicher zu behandeln ist insofern interessant, als sämtliche Ausprägungen nicht nur die Manipulationssicherheit prägen, sondern auch entscheidenden Einfluß auf die Anonymität der Zahlungsverfahren haben [GZ96]:

*Art der Zahlung*
Das elektronische Geld kann gegenüber der herausgebenden Bank entweder im voraus vor der Weitergabe an den Händler gekauft (Prepaid-Verfahren) oder erst nach der Einlösung der Händlerforderung verrechnet werden (Postpaid-Verfahren). Während Postpaid-Verfahren kein anonymes Bezahlen ermöglichen, da der Kunde zumindest der Bank bekannt sein muß, sind Prepaid-Verfahren hierzu geeignet. Dies setzt jedoch voraus, daß der Kunde auch bei der Verrechnung der Geldeinheiten (Clearing) nicht identifiziert werden kann.

*Art des Wertetransfers*
Elektronisches Geld kann in Form von Transaktionen oder in Form von Bargeld transferiert werden. Transaktionsorientierte Verfahren orientieren sich an Lastschriftverfahren. Geldbeträge werden dabei unter Angabe des Absenders und des Empfängers transferiert, so daß der Zahlungsvorgang nicht mehr anonym ist. Ob die Zahlungsvorgänge nur temporär zur Zahlungsabwicklung oder über einen längeren Zeitraum auch zur Verteilung von Geldwerten auf einzelne Konten benötigt werden, hängt wiederum vom Stellenwert dritter Instanzen ab, beispielsweise Clearingstellen. Bargeldorientierte Verfahren sind aus datenschutzrechtlicher Sicht zu favorisieren, da keine Geldbeträge übermittelt werden, sondern ein Bündel von einzelnen Geldeinheiten. Die Fälschungssicherheit wird durch digitale Signierung jeder Geldeinheit realisiert. Das Bezahlen mit bargeldorientierten Verfahren ist jedoch nur dann vollständig anonym, wenn nicht zwecks Geldflußanalysen auf dem elektronischen Geldschein vermerkt wird, durch wessen Hände er gegangen ist. Geldflußanalysen sind hinsichtlich der Manipulationssicherheit, aber auch hinsichtlich der Überprüfung von unerlaubter Geldwäsche von Bedeutung.

*Art des Geldkreislaufs*
Die meisten Zahlungsverfahren stellen einen geschlossenen Kreislauf zwischen dem Kunden, dem Händler sowie der Kunden- und Händlerbank dar. Jede Forderung, die der Händler gegenüber dem Kunden aufgrund einer ausgelieferten Ware oder einer erbrachten Dienstleistung hat, wird direkt über die Händler- und Kundenbank eingelöst. Das Manipulationsrisiko ist aufgrund der Abgeschlossenheit des Verfahrens zwar relativ gering. Dennoch ist jede erworbene Ware oder getätigte Dienstleistung grundsätzlich von den dazwischengeschalteten Banken nachvollziehbar. Es ist allerdings möglich, das Bezahlen arbeitsteilig derart zu gestalten, daß einerseits der Händler keine Kenntnis über die Identität des Kunden hat, andererseits die Bank, die im Auftrag des Kunden dem Händler den Geldbetrag ausbezahlt, jedoch keine Kenntnis über die getätigten Dienstleistungen erhält.
Datenschutzfreundlicher sind *Face-to-Face*-Verfahren, bei denen das elektronische Geld auch von Kunde zu Kunde bzw. von Händler zu Händler ohne Zwischenschaltung einer Bank weitergegeben werden kann. Der Zeitpunkt, zu dem elektronisches Geld in Giralgeld umgewandelt wird, bleibt dabei jedem Kunden selbst überlassen. Da derartige Verfahren in der Regel bargeldorientiert sind, können die mit dem elektronischen Geld bezahlten Dienstleistungen nicht mehr zentral, sondern lediglich dezentral beim Kunden oder beim Händler bzw. auf einem von ihnen verwalteten Medium (z. B. Chipkarte) gespeichert werden.

*Art der Geldbörsenplattform*
Elektronische Zahlungsverfahren sind entweder hardwaregestützt (z. B. auf Basis von Chipkarten) oder hardwareunabhängig. Chipkartengestützte Zahlungssysteme sind aufgrund von Hardwaremechanismen wesentlich manipulationssicherer als hardwareunabhängige Verfahren, die ausschließlich auf softwarebasierten Verschlüsselungstechniken basieren. Somit wäre eigentlich zu vermuten, daß bei chipkartengestützten Verfahren tendenziell weniger personenbezogene Daten erhoben werden. Diese Einschätzung läßt sich anhand der im Einsatz befindlichen Verfahren jedoch nicht bestätigen.

Bei chipkartengestützten und zugleich transaktionsorientierten Verfahren empfiehlt es sich, möglichst personenungebundene Chipkarten, sogenannte *White Cards*, zu verwenden. Sonst besteht die Gefahr, daß durch Auswertung von Verrechnungskonten die Anonymität des Kunden aufgehoben wird.

## 2.3 Elektronische Zahlungsverfahren

Im folgenden werden sechs elektronische Zahlungsverfahren dargestellt. Den Verfahren werden für die Betrachtung relevante Merkmale zugeordnet (siehe Abbildung), deren Ausprägungen auch eine Basis für eine datenschutzgerechte Einschätzung bilden.

| | Zahlung | | Wertetransfer | | Geldkreislauf | | Geldbörsen-plattform | | Zahlungsvorgang insgesamt | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | post-paid | pre-paid | trans-aktions-orien-tiert | bar-geld-orien-tiert | ge-schlos-sen | facto-face | chip-karten-ge-stützt | hard-ware-unab-hängig | an-onym | pseud-onym gegen-über dem Händ-ler | mittels Treu-händer |
| Ecash | | x | | x | x | | | x | x | | |
| Cyber-cash | x | | x | | x | | | x | | x | x |
| First Virt-ual | x | | x | | x | | | x | | x | x |
| SET | x | | x | | x | | | x | | x | |
| Geld-karte | | x | x | | x | | x | | | x | |
| Mon-dex | | x | | x | | x | x | | | x | |

Elektronische Zahlungsverfahren im Vergleich

### 2.3.1 Ecash

Ecash [DIGI] ist eine bestimmte Form digitaler Geldmünzen (Cyberbucks), die hardwareunabhängig ohne ein körperliches Trägermedium ihrem Besitzer die Durchführung von Zahlungsvorgängen über öffentliche Computernetze so ermöglichen, als

würde dieser mit echten Münzen bezahlen. Das Ecash zugrunde liegende technologische Verfahren, das vom niederländischen Kryptologen David Chaum entwickelt wurde und das von der Firma DigiCash angeboten wird, ist schon in den USA und Finnland im Einsatz. Auch die Deutsche Bank hat eine Lizenz für Ecash erworben und testet das Zahlungsverfahren in einem Pilotprojekt.
Ecash ist ein bargeldorientiertes Prepaid-Verfahren, das jedoch an ein Buchgeldguthaben gekoppelt ist, beispielsweise auf einem herkömmlichen Girokonto. Vergleichbar mit regulären Banknoten besitzt jede digitale Münze eine einmalige Seriennummer, die zur Überprüfung der Einmaligkeit des elektronischen Geldes dient. Im Gegensatz zu Bargeld werden bei Ecash die digitalen Münzen nur einmal in Umlauf gebracht und nach dem Kauf vom Händler sofort bei der Bank eingelöst, um ein unerlaubtes Erstellen von Münz-Duplikaten zu erschweren. Ecash ist somit ein geschlossenes Verfahren, das zur Zeit noch keinen Face-to-Face-Umlauf erlaubt. Um zu verhindern, daß die Bank über die Seriennummer einen direkten Bezug von Käufer und Händler ableiten und daraus entsprechende Kundenprofile erzeugen kann, kommt bei Ecash die sogenannte *blinde digitale Signatur* (s. Abschnitt 5.2 Hauptteil) zum Einsatz.

Um mit Ecash zu zahlen, muß der Käufer gegen Belastung seines Kontos zunächst digitale Werteinheiten (Münzen) von seinem Bankinstitut in seine *Geldbörse* auf dem PC laden. Mittels einer speziellen Software, die der Ecash-Teilnehmer auf seinem PC vorhält, erzeugt er einen Datensatz, der u. a. den gewählten Betrag und eine nach dem Zufallsprinzip generierte Seriennummer enthält. Diese Seriennummer wird mittels eines mathematischen Verfahrens mit einer Zufallszahl (Blendungsfaktor) verdeckt. Anschließend werden die Daten verschlüsselt an die Bank übermittelt. Die vom Kunden verdeckte Seriennummer kann die Bank nach der Entschlüsselung nicht identifizieren, da sie nicht den Blendungsfaktor kennt. Somit wird sichergestellt, daß die Bank im nachhinein nicht feststellen kann, welchem Kunde welche Münze mit welcher Seriennummer ausgegeben wurde.
Die Bank bucht den Betrag vom Konto des Käufers ab, validiert den Datensatz mit ihrer digitalen Signatur und übermittelt diesen in verschlüsselter Form wieder auf den PC des Käufers. Unter erneutem Einsatz des Blendungsfaktors wird hier die Seriennummer in ihrer ursprünglichen Form wieder hergestellt.
Mit Ecash kann über das Internet bei allen Händlern Ware bezahlt werden, die sich Ecash angeschlossen haben. Der Käufer transferiert die Geldmünzen verschlüsselt über das Netz zum Händler. Dieser läßt die Echtheit und Originalität der ihm angebotenen Münzen online von der ausstellenden Bank mittels digitaler Signatur prüfen. Da sich die Bank die Seriennummer merkt, würde eine zum zweitenmal eingereichte Münze als ungültig zurückgewiesen.
Nach Prüfung und positiver Bestätigung durch die Bank kann schließlich der Händler die Vertragserfüllung realisieren. Das vom Händler eingezahlte Ecash wird von der Bank auf herkömmlichem Weg seinem Konto gutgeschrieben, oder er erhält dafür wiederum erneut einen äquivalenten elektronischen Wert als Münze mit einer neuen Seriennummer.

Ecash erlaubt als Prepaid-Verfahren anonyme Zahlungen sowohl gegenüber der Bank als auch gegenüber dem Händler. Der Einsatz der blinden Signatur stellt sicher, daß

die der elektronischen Münze zugeordnete Seriennummer keine Rückschlüsse auf den Kunden ermöglicht. Damit kann das Kaufverhalten eines Kunden nicht nachvollzogen werden, denn er bezahlt wie bei Bargeld ohne Datenspuren zu hinterlassen. Ecash unterscheidet sich damit wesentlich von anderen Online-Zahlungsverfahren.
Die Anonymität des Käufers ist natürlich nur soweit gewährleistet, wie der Kunde nicht beim Verkäufer Ware bestellt, die auf dem herkömmlichen Weg zugesandt werden muß. In diesem Fall muß sich der Käufer aber nur gegenüber dem Verkäufer identifizieren. Die Bank kann den Weg der Münzen auch weiterhin nicht bis zum Kunden zurückverfolgen, obwohl sie letztendlich dessen Zahlungsverkehr abrechnet. Die Zahlungsdaten werden zudem verschlüsselt übertragen, so daß auch die Vertraulichkeit der Transaktion gegenüber Dritten gewährleistet ist.

### 2.3.2 Cybercash

Cybercash ist ein netzfähiges Zahlungssystem auf der Basis von Kreditkarten. Der Zahlungsvorgang wird vermittelt und unterstützt durch sogenannte Treuhänder, die die Verrechnung durch Kreditkarte oder ein Bankeinzugsverfahren durchführen. Cybercash wurde als reales System im Jahr 1994 in den USA eingeführt und realisiert alle Transaktionen über das Internet.
Sowohl Käufer als auch Händler sind Vertragspartner des Cybercash-Treuhänders. Jeder Cybercash-Teilnehmer erhält eine spezielle Software, mit der ein eigenes Schlüsselpaar generiert wird, bestehend aus einem privaten und einem öffentlichen Schlüssel. Der Käufer übermittelt dem Cybercash-Treuhänder seinen öffentlichen Schlüssel sowie seine mit dem öffentlichen Schlüssel von Cybercash chiffrierte Kreditkartennummer. Damit ist der Kunde bei Cybercash registriert und kann bei allen Cybercash angeschlossenen Händlern über das Internet einkaufen.
Auf eine Kaufanfrage erhält der Kunde vom Händler ein entsprechendes Angebot. Hat sich der Kunde zum Kauf entschlossen, gibt er dem Händler hierüber eine Bestätigung. Diese Bestätigung, die unter anderem die mit dem öffentlichen Schlüssel von Cybercash verschlüsselte Kreditkartennummer des Kunden und seine Produktauswahl beinhaltet, ist vom Kunden digital signiert. Damit wird der Kaufwunsch des Kunden im Rahmen von Cybercash verbindlich und nachweisbar. Der Händler kann die ihm übermittelte Kreditkartennummer nicht entschlüsseln und sendet diese ergänzt um weitere Angaben, wie beispielsweise den Kaufbetrag, an den Cybercash-Server. Dieser nimmt nach der Entschlüsselung der Daten direkt Verbindung zu der entsprechenden Kreditkartengesellschaft des Käufers auf, um das Clearing einschließlich der Authentisierung des Käufers einzuleiten. Das Ergebnis dieser Aktion wird dem Händler mitgeteilt, der dem Käufer wiederum bei Vorliegen einer positiven Bestätigung eine von ihm digital signierte Quittung als Beweis der Kauftransaktion übermittelt.

Cybercash arbeitet nach dem Postpaid-Verfahren; ein Kaufauftrag führt immer zur Belastung des Kundenkontos. Eventuelle Reklamationen können nur außerhalb des Cybercash-Verfahrens bearbeitet werden.
Der Käufer bleibt bei Cybercash nicht anonym, da zahlreiche Daten über den Kaufvorgang gespeichert werden. Der Käufer agiert jedoch mittels verschlüsselter Kreditkartennummer zumindest gegenüber dem Händler pseudonym.
Der Treuhänder besitzt neben dem Namen und der Anschrift des Kunden dessen

Kreditkartennummer, die er zur Verrechnung der Kaufbeträge bei der Kreditkartengesellschaft benötigt. Die Kreditkartengesellschaft kennt ebenfalls den Kunden, weiß aber nicht, was er gekauft hat.
Personenbezogene Kundenprofile können nur erstellt werden, wenn sämtliche Akteure ihre jeweiligen Datenbestände untereinander austauschen. Da der Händler die Kreditkartennummer nur in verschlüsselter Form kennt, können Händler und Kreditkartengesellschaft ohne den Treuhänder keine Kundenprofile generieren. Insofern setzt ein Datenmißbrauch ein treuwidriges Verhalten aller Beteiligten voraus.
Fälschungssicherheit und Vertraulichkeit der übermittelten Zahlungsdaten wird bei Cybercash durch den Einsatz kryptographischer Funktionen sichergestellt. Die Zahlungsdaten werden sowohl verschlüsselt übertragen als auch verschlüsselt auf dem Rechner des Händlers gespeichert. Da der Käufer bei der Transaktion seinen Kaufauftrag zusätzlich mit seiner digitalen Signatur versieht, ist sein Auftrag zudem nachträglich beweisbar.

### 2.3.3 First Virtual

First Virtual [FV] ist ein mit Cybercash vergleichbares kreditkartengestütztes Abrechnungssystem, das in den USA zum Einkaufen im Internet eingesetzt wird. Artikel, Bücher, Zeitschriften, Bilder, Nachrichten, Software etc., aber auch Waren außerhalb des Internets können über First Virtual gekauft und bezahlt werden.
Es basiert auf gewöhnlichen Internetdiensten wie E-Mail, FTP und WWW. Das System erfordert somit seitens der Kunden keine spezielle Software, um Produkte im Internet anzubieten bzw. diese zu kaufen.
First Virtual übernimmt in der Abrechnung zwischen Käufer und Händler die Treuhänder- bzw. die Vermittlerfunktion, analog Cybercash. Die Belastung des Kunden erfolgt über dessen Kreditkarte, wobei im Gegensatz zu Cybercash bei der Transaktion die Kreditkartennummer nicht mit übertragen wird. Dem Anbieter der Leistung schreibt First Virtual den Betrag auf beliebigem Wege gut.
Jeder Kunde meldet seine Teilnahme über den entsprechenden WWW-Server von First Virtual an und erhält von First Virtual eine vertrauliche Benutzerkennung zugesandt. Über dieses Pseudonym wird jede zukünftige Kauftransaktion des Kunden abgewickelt. Der Kunde übermittelt seine Kreditkartennummer unverschlüsselt per Brief oder Telefon an First Virtual. Die Kreditkartennummer wird von First Virtual auf einem nicht mit dem Internet verbundenen Rechner gespeichert; per E-Mail wird dem Kunden die Freischaltung der Zugangsberechtigung bestätigt.
Ein Zahlungsvorgang wird bei First Virtual dadurch in Gang gesetzt, daß der Kunde einen Kaufantrag mit seiner Benutzerkennung per elektronischer Post abschickt. First Virtual fragt beim Käufer zurück, ob er das Produkt tatsächlich bestellt hat und ob er es auch bezahlen möchte. Erst nach einer positiven Bestätigung durch den Käufer wird dessen Kreditkartenkonto letztendlich belastet. Durch eine negative Bestätigung kann sich der Käufer sowohl vor einer schlechten Produktqualität als auch vor Fehlbestellungen schützen, die Unbefugte in seinem Namen auslösen können. Diese Vorgehensweise schützt den Kunden auch dann, wenn ein Verdacht auf illegale Benutzung seiner Kreditkarte besteht. In einem solchen Fall stellt First Virtual Nachforschungen an, ändert die Benutzerkennung und überweist dem Verkäufer kein Geld.
Da der Kunde in der Regel über das Bezahlen erst dann entscheidet, nachdem er die

Informationsprodukte gelesen hat, setzt dieses Verfahren Vertrauen in die Ehrlichkeit der Kunden voraus und bedeutet damit ein gewisses Risiko für den Informationsanbieter. Obwohl diese Verfahrensweise seitens First Virtual durch seine Gründer bewußt angestrebt wurde, ist aber auch eine Notbremse gegen allzuhäufige Stornierungen eingebaut. Wer zu häufig die Zahlung verweigert, verliert seine Benutzerkennung.
First Virtual ist ein hardwareunabhängiges, transaktionsorientiertes Postpaid-Verfahren mit geschlossenem Geldkreislauf. First Virtual ist ebenso wie Cybercash kein anonymes Zahlungsverfahren; es ermöglicht dem Käufer jedoch, pseudonym gegenüber dem Händler aufzutreten.
Das System First Virtual verzichtet auf den Einsatz kryptographischer Mittel. Die Kommunikationsinhalte der Transaktionen werden unverschlüsselt über das Internet übertragen; allerdings erfolgt keine Übermittlung der Kreditkartennummer des Kunden. Durch Einsatz der Benutzerkennung erübrigt sich auch die Übertragung persönlicher Identifikationsangaben des Kunden.
Die übermittelten Daten sind daher nur soweit vor unbefugtem Zugriff gesichert, wie dies die Internetdienste Electronic Mail, FTP und WWW zulassen, auf die das System zurückgreift. Ein Schutz vor Verlust der Vertraulichkeit der übertragenen Nachrichten ist somit nicht gegeben.
Auch die Fälschungssicherheit ist aufgrund fehlender Sicherheitsmechanismen nicht gewährleistet. Das gleiche trifft auf den Kaufvorgang zu, der nicht beweisbar ist und keinem Kunden eindeutig zugeordnet werden kann, da hierfür der Einsatz entsprechender Mechanismen, wie z. B. der digitalen Signatur, fehlt. Da First Virtual dem Käufer jedoch das Recht einräumt, vom Kauf Abstand zu nehmen, kann dieser dennoch eventuelle Nachteile zu seinen Ungunsten abwenden.

### 2.3.4 SET-Standard

Für das Bezahlen mit Kreditkarten im Internet werden dem Verfahren SET (Secure Electronic Transaction) als zukünftigem Zahlungsverkehrsprotokoll große Chancen eingeräumt. Microsoft, Visa und Mastercard haben beschlossen, SET zu einem allgemeinen Standard zu entwickeln. Mit SET sollen die Protokolle SEPP (Secure Electronic Payment Protocol) von Mastercard, Cybercash, IBM und Netscape sowie STT (Secure Transaction Technology) von Visa und Microsoft abgelöst werden. SET verwendet sowohl symmetrische als auch asymmetrische Verschlüsselungsverfahren; die Schlüssel werden durch entsprechende Instanzen zertifiziert.
Der Kunde zahlt durch Angabe seiner Kreditkartennummer, die er am PC eingibt. Die SET-Software verschlüsselt die Kreditkartendaten und leitet sie zusammen mit einer digitalen Signatur an den Verkäufer weiter. Dieser kann die verschlüsselten Kartendaten nicht lesen und leitet sie ergänzt um den Kaufbetrag an das Kreditkartenunternehmen weiter. Das Kreditkartenunternehmen bestätigt dem Verkäufer die Solvenz des Kunden und schreibt dem Händler den Betrag gut.
Der SET-Standard ermöglicht zwar kein anonymes, jedoch ein pseudonymes Einkaufen. Während der Händler nur über das gekaufte Produkt und den Preis informiert ist, nicht aber den Namen des Käufers weiß, kennt die Kreditkartengesellschaft die Identität des Käufers sowie den bezahlten Betrag, erhält aber keine Information über

das gekaufte Produkt.
Im Gegensatz zu Cybercash tritt bei SET allerdings kein Treuhänder als Vermittler zwischen Händler und Kreditkartenunternehmen auf. Somit kennt das abrechnende Kreditkartenunternehmen den Händler, bei dem der Kunde einkauft, so daß zumindest kundenbezogene Teilprofile erstellt werden können.
Der SET-Standard gewährleistet die Vertraulichkeit und Fälschungssicherheit der Transaktionsdaten sowie die Authentizität zwischen Käufer und Verkäufer, so daß Kaufvorgänge nicht abgestritten werden können.

### 2.3.5 Geldkarte

Zum Bezahlen im Internet eignet sich grundsätzlich auch die seit Anfang des Jahres bundesweit im Einsatz befindliche Geldkarte des deutschen Kreditwesens, wenngleich das Bezahlen und Aufladen zur Zeit noch spezielle Händler- und Bankterminals voraussetzt. Denkbar wäre es jedoch auch, das Bezahlen über Netze mittels Geldkarte zu realisieren - entsprechende Planungen liegen in den Schubladen der Entwickler. Die Transaktionen werden dann nicht mehr über Händler- und Bankterminals transportiert, sondern per Internet direkt von der Geldkarte vom Kunden zum Händler bzw. von der Bank zum Kunden. Die Realisierung dieses Szenarios setzt voraus, daß die in den Terminals implementierten Mechanismen zur Manipulationssicherheit durch geeignete Instrumente auf Netzebene, beispielsweise Verschlüsselungsmaßnahmen, ersetzt werden.
Aus datenschutzrechtlicher Sicht ist der Einsatz der Geldkarte insofern problematisch, als ein sehr komplexes Clearingverfahren konzipiert wurde, das kartenbezogen jede einzelne Zahlungstransaktion erfaßt. Die von den Händlern eingereichten Umsätze werden zunächst in Börsenevidenzzentralen auf Echtheit und Doppeleinreichungen geprüft und anschließend mit Börsenverrechnungskonten verrechnet, die von den Banken für jeden Kunden eingerichtet worden sind. Während das Börsenverrechnungskonto nur Auskunft über den Saldo einer jeden Karte gibt, führen die Börsenevidenzzentralen zusätzlich für jede Karte eine Börsenumsatzdatei, die sämtliche mit einer Karte getätigten Umsätze bzw. Transaktionen festhält. Der Transaktionsdatensatz enthält nicht nur den Kaufbetrag, das Kaufdatum und die Kaufzeit sowie einen identifizierbaren Händlerschlüssel, sondern auch das zum Kaufzeitpunkt aktuelle Kartensaldo. Die Börsenumsatzdatei stellt somit ein Schattenkonto dar, das sämtliche mit der elektronischen Geldkarte getätigten Kaufvorgänge parallel mitverfolgt. Da die Geldkarte in der Regel auf der EC-Karte untergebracht ist, sind die Kontoauszüge nicht nur kartenbezogen, sondern zugleich personenbezogen.
Das Führen von Schattenkonten hat hauptsächlich zwei Gründe:
- Zum einen ist das Vertrauen der Kreditwirtschaft in die Fälschungs- und Revisionssicherheit des Verfahrens nicht groß genug, um auf ein einzelfallbezogenes kartenbezogenes Clearing verzichten zu wollen. Durch die Schattenkonten wird doppelte Sicherheit zu erreichen versucht.
- Zum anderen sollen dem Bankkunden bereits vorausbezahlte, aber noch nicht ausgegebene Geldwerte erstattet werden können. Elektronische Geldwerte sollen dem Bankkunden jedoch nur bei technischem Defekt der Geldbörse, nicht jedoch bei deren Verlust zurückgegeben werden.

Da die Geldkarte eine vorausbezahlte Geldbörse ist, besteht normalerweise keine

Notwendigkeit, personenbezogene Zahlungsdaten zu Buchungszwecken zu erheben und zu speichern. Es ist daher zu hoffen, daß langfristig auf das Führen von Schattenkonten verzichtet wird und nur noch Schattensalden - wie das bereits bei der österreichischen EC-Karte praktiziert wird - gespeichert werden.

### 2.3.6 Mondex

Ein hardwaregestütztes Verfahren stellt das von der Westminster Bank und der Midland Bank zusammen in Großbritannien herausgegebene Mondex dar [MON]. Mondex erlaubt nicht nur die Übertragung elektronischen Geldes im geschlossenen Kreislauf zwischen Kunde, Händler und Bank, sondern auch *face-to-face* zwischen einzelnen Kunden. Außerdem kann Mondex zum Online-Bezahlen über öffentliche Netze eingesetzt werden. Mondex ist somit auch zum Bezahlen im Internet geeignet, wenngleich hierzu noch einige Ergänzungen notwendig sind.
Das Bezahlen per Mondex geschieht mittels Chipkarte und zusätzlicher *Wallets*, die für die sichere Übertragung der Geldtransaktionen zuständig sind. Bei Bedarf kann sich der Kunde über das Wallet auch die letzten zehn getätigten Transaktionen anzeigen bzw. ausdrucken lassen.
Mondex ist aus datenschutzrechtlicher Sicht insofern interessant, als beim Einkaufen mittels Mondex weniger personenbezogene Daten gespeichert werden als bei der vergleichbaren Geldkarte des deutschen Kreditwesens. Anstatt sehr aufwendig den mit jeder Geldbörse getätigten Umsatz nachzuvollziehen, um hierüber flächendeckend für jede im Umlauf befindliche Geldbörse Mißbrauchsfälle sofort erkennen zu können, wird bei Mondex zunächst nur überprüft, ob mehr elektronisches Geld im Umlauf ist, als seinerzeit herausgegeben wurde. Dabei wird - wie bei Papiergeld - ein gewisser Prozentsatz von gefälschtem Geld sogar in Kauf genommen.
Um den Anteil von falschem elektronischen Geld zu ermitteln, werden stichprobenartig für einzelne Schnittstellen im Zahlungssystem detaillierte Geldflußanalysen erstellt. Die Geldflußanalysen basieren auf Zahlungsdaten, die erhoben werden, wenn die Wallets über das Mondex-Kommunikationssystem mit der Betreiberbank verbunden sind.

## 2.4 Hardwarebasierende Sicherheitslösung - MeCHIP

Das MeCHIP-System der Firma ESD bei Leipzig stellt eine hardwarebasierte Sicherheitslösung für den Datentransfer zwischen dem Kunden-PC (MeCLIENT) und dem Rechnersystem (MeSERVER) des Anbieters (z. B. einer Bank) dar. Es verkörpert kein neues Zahlungssystem. Hiermit wird die bei softwarebasierenden Sicherheitssystemen existierende Sicherheitslücke beim Kunden-PC abgedeckt. Ausgangspunkt eines Angriffes auf den Kunden-PC könnte beispielsweise ein für den Benutzer unbemerkter, durch Shareware, Spiele oder direkt aus einem öffentlichen Netz eingeschleuster Virus sein, der im Datenspeicher des PC abgelegte und noch nicht verschlüsselte sicherheitsrelevante Daten (Paßwort, Schlüsselwörter, Kreditkarten-Nr., Konto-Nr. etc.) manipuliert oder ausliest und an einen fremden Zielrechner sendet. Beim MeCHIP-System kommen sowohl asymmetrische als auch symmetrische Ver- und Entschlüsselungsmethoden (RSA- und Standard-DES-Verfahren mit Modifikationen) zum Einsatz.
Kern dieser Schutztechnologie ist der sogenannte MeCHIP, der auf Seiten des

MeClient als Hardware sowie beim MeServer als Softwarelösung eingesetzt wird und alle sicherheitsrelevanten Aktionen realisiert. Die Benutzung des MeCHIP ist paßwortgesichert. Jeder Chip verkörpert ein Unikat, indem der Schaltkreis verschieden ist. Somit ist es möglich, jedem Benutzer eine eindeutige Identifikation zuzuordnen, eine Art digitale Identität. Der MeCHIP besitzt einen direkten Anschluß an die Tastatur des MeClient. Somit werden alle sicherheitsrelevanten Daten, die am absendenden PC mittels Tastatur oder anderer externer Eingaben in der Regel unverschlüsselt eingegeben werden, direkt in den MeCHIP übertragen. Dort werden sie signiert und spezifisch verschlüsselt, d. h., der mit einem Zufallsgenerator erzeugte eigentliche Schlüssel wird vor der Verschlüsselung der Daten noch mit dem eindeutigen und hardwareabhängigen Schlüssel des MeCHIP verschlüsselt. Letzterer Schlüssel ist nur noch dem MeServer bekannt, weshalb nur dieser Daten für einen bestimmten MeCHIP ent- und verschlüsseln kann.
Die signierten und verschlüsselten Daten werden anschließend über offene Netze mit dem MeTransportprotokoll zum Zielsystem übertragen. Hier werden vom MeServer chipspezifisch die Daten entschlüsselt sowie die Signatur überprüft und eventuelle Datenmanipulationen erkannt. Nach der erfolgreichen Überprüfung wird die Transaktion vom MeServer bestätigt. Damit sichert der MeCHIP den Informationsfluß von der Eingabe am MeClient bis zur Entschlüsselung auf dem MeServer. Das eingesetzte Transaktionsprotokoll ist paketorientiert und unabhängig von der gewählten Transportschicht. Hier involvierte Sicherheitsmechanismen sollen u. a. das unbemerkte Einfügen, Entfernen und Wiedereinspielen von Datenpaketen verhindern.
Das MeCHIP-System kann unabhängig vom Übertragungsweg (bspw. Internet, T-Online), vom übertragenen Inhalt und von der eingesetzten Zahlungsart (bspw. Kreditkarte, Ecash) eingesetzt werden.
Die Hamburger Sparda-Bank verwendet das MeCHIP-System beim Homebanking. Der MeCHIP wird auf den Druckeranschluß des Kunden-PC gesteckt und mit der Tastatur verbunden. Somit verschlüsselt er alle über die Tastatur eingegebenen Kundendaten, bevor sie in den RAM des PC gelangen. Die vom traditionellen Online Banking gewohnten Transaktionsnummern entfallen. Der Kunde muß sich nur noch seine PIN merken.
Die MeCHIP-Technik ermöglicht dem Empfänger, den Absender eindeutig zu identifizieren. Das Verfahren ist so angelegt, daß jedem Benutzer der MeCHIP-Technologie eine eindeutige Identifikation zugeordnet wird. Auf diesem Prinzip beruht das Vertrauen, daß sich Kunde und Anbieter bei diesem System entgegenbringen.
Inwieweit der Kunde allerdings zum „gläsernen“ Konsumenten wird, wenn das MeCHIP-Sicherheitssystem (in eventuell angepaßter Form) zur Absicherung der Transaktionen beim Online-Shopping eingesetzt wird, hängt primär von dem hier verwendeten Zahlungssystem ab.

## 3. Datenschutzfreundliche Technologien im Gesundheitsbereich

Mit der flächendeckenden Einführung der Krankenversichertenkarte (KVK) gemäß § 291 SGB V wurde zwangsläufig in der gesamten Bundesrepublik Deutschland eine Infrastruktur geschaffen, die die elektronische Verarbeitung aller medizinischer Daten (Leistungsdaten, Diagnosedaten, Verlaufsdaten), die ein Leistungserbringer (Arzt, Krankenhaus, Hebamme etc.) über einen Patienten speichert, zur Folge hat.

War vor der Einführung der KVK ein Großteil der Leistungserbringer nicht mit elektronischen Datenverarbeitungsanlagen ausgestattet, so änderte sich dies mit der Einführung schlagartig; fast jeder Leistungserbringer verfügt heute über einen Arbeitsplatzcomputer mit Drucker und Chipkartenlesegerät (Kartenterminal). Der weitere Ausbau wird - schon heute absehbar - in der Vernetzung über moderne Telekommunkationssysteme (ISDN, Internet) vorgenommen werden.
Damit ergeben sich zwei Themenbereiche:
- die (digitale) Kommunikation über medizinische Daten, insbesondere auch über moderne Telekommunikationssysteme (ISDN, Internet)
- die zunehmend automatisierte bzw. rechnergestützte Verarbeitung personenbezogener Daten im Rahmen von Behandlung und Forschung.

### 3.1 Vernetzung / Netze

Derzeit wird im Gesundheitsbereich in folgende Richtung argumentiert:
Die Nutzung der vorhandenen Infrastruktur nur zum Zweck der Abrechnung scheine auf die Dauer nicht wirtschaftlich, ließen sich doch durch den Einsatz der Technik ein Großteil der im Gesundheitswesen vorhandenen Informations- und Kommunikationsdefizite beheben. Diese wirkten sich bei der Qualität der Patientenversorgung aus und verursachten in nicht unerheblichen Maße Zusatzkosten für die Versichertengemeinschaft. Typische Beispiele für die vorhandenen Defizite seien:
- Bei der Überweisung vom Haus- zum Facharzt, vom Haus- oder Facharzt ins Krankenhaus etc. werden oftmals keine Befunde oder Ergebnisse von Voruntersuchungen mitgeliefert, so daß verschiedene Untersuchungen (Röntgen, EKG, Labortests) erneut durchgeführt werden. Dies stellt nicht nur für den Patienten eine erhebliche Belastung, z. B. durch wiederholtes Röntgen dar, sondern trägt darüber hinaus zur Steigerung der Kostenbelastungen bei.
- Arztbriefe, die bei einer Krankenhausentlassung dem nach- oder weiterbehandelnden Arzt als Basisinformation dienen sollen, erreichen zum Teil erst nach Wochen ihren Empfänger. Die zumeist handschriftlichen, häufig schwer lesbaren Niederschriften wären oftmals ohne Rückfragen und den damit verbundenen Zeitverzug für eine Fortsetzung der Behandlung nicht geeignet.
- Wichtige Informationen, wie etwa solche über besondere Vorerkrankungen, Risikofaktoren, Allergien, oder Arzneimittelunverträglichkeiten, stehen zwar oftmals dem Hausarzt zur Verfügung, aber nicht den behandelnden Fachärzten oder gar dem Notfallarzt.
- Gesundheitsvorsorgemaßnahmen sind teilweise nur aufgrund einer breiten Auswertung von vorliegenden Krankheitsverläufen möglich. Hierzu sind zunächst die Daten in einer elektronischen Krankenakte zu führen.
- Epidemiologische Forschungen benötigten regelmäßig institutionsübergreifend Zugriff auf die Daten eines Patienten, um für das Gesundheitswesen fundierte Zahlen und Fakten zu liefern.

An der Verbesserung der Kommunikation wird seit Jahren intensiv in wissenschaftlichen Untersuchungen und Modellprojekten gearbeitet. Zum einen kommen dabei Chipkarten zur Speicherung der wichtigsten Informationen eines Patienten zum Einsatz („Patientenkarten“; Offline-Lösung), zum anderen werden die Möglichkeiten von modernen Telekommunikationsnetzen erprobt. Dies geschieht zur Unterstützung

von Diagnosen durch Spezialisten über weite Entfernungen durch elektronische Übermittlung von Voruntersuchungsergebnissen per Datentransfer oder durch Zugriffe auf Patientendaten, die auf verschiedenen Rechnern - Hausarzt, Facharzt, Krankenhaus etc. - gespeichert werden.
Die Datenschutzbeauftragten stellen sich dieser Diskussion.

## 3.2 Verfahren und Projekte

Das zentrale Problem bei den bisher geplanten oder erprobten Verfahren dreht sich um die Frage, mit welchen Maßnahmen die Daten eines Patienten gegen jeden anderen Zugriff als den der in der konkreten (Behandlungs-)Situation zugriffsberechtigten Person geschützt werden können. Daneben stehen die Forderungen der Krankenkassen und der medizinischen Forschung zur elektronischen Auswertung der gespeicherten Daten zur Qualitätssicherung, Prognosen, Planzahlen und der medizinischen Forschung zur Verbesserung der Versorgung. Dies eröffnet ein breites Feld an möglichen Anwendungen für Anonymisierungs- und Pseudonymisierungsverfahren. Neben der klassischen Behandlungssituation Patient - Arzt, bei der personenbezogene Daten zwangsläufig anfallen (s. o. Spiegelstrich 1 bis 3), gibt es eine Reihe anderer Vorgänge im Gesundheitswesen, bei denen der Personenbezug nicht unbedingt benötigt wird (s. o. Spiegelstrich 3 bis 5). In all diesen Fällen könnten datenschutzfreundliche Technologien einen erheblichen Beitrag leisten, sowohl für das Vertrauen des Patienten bezüglich des Umgangs mit seinen Daten als auch für den Arzt zur Beweis- und Qualitätssicherung.
Praktische Erfahrungen mit dem Einsatz datenschutzfreundlicher Technologien liegen bereits vor:

- Krebsregister (Krebsregistergesetz in Schleswig-Holstein) (vgl. auch Bundeskrebsregistergesetz)
- Pseudonymisierungs-Technik im Bereich der Qualitätssicherung in der Nierenersatztherapie (QuaSiNiere)
- Pseudonymisierung bzw. Anonymisierung im Bereich der epidemiologischen (medizinischen) Forschung (Ursachenforschung)
  Neben diesen konkreten Anwendungen wurden in der Vergangenheit bereits Modelle entwickelt, in denen ebenfalls datenschutzfreundliche Technologien eingesetzt werden könnten. Beispiel hierzu sind:
- Krankenkassenabrechnung [POM] [BlSch]
- Pseudonymisierung von Arztdaten beim Einsatz einer Apothekenkarte (Struif, GMD)
- Einsatz von Gruppenschlüsseln beim Zugriff auf med. Daten in Krankenhäusern [BlSch]
- Führung von Registern, z. B. Herzschrittmacher, künstliche Hüftgelenke etc. (Planungen der Deutschen Krankenhausdachgesellschaft - DKG - zum Führen eines Herzschrittmacherregisters zur Qualitätssicherung dieser Geräte, Pseudonym = Serien-Nummer des Gerätes)
- Diensteanbieter im Gesundheitswesen, z. B. „Home-Care“.

Neben Beratung der Behandlung von kleineren Krankheiten (Schnupfen, Husten)

sollen hier auch Beratungen bezüglich Ernährung, Sucht und im Bereich der Prävention, z. B. Geschlechtskrankheiten oder AIDS, angeboten werden. „Home-Care"-Dienste werden allerdings nur dann angenommen werden, wenn eine gewisse Anonymität des Benutzers gewährleistet ist und die Kostenfrage mit den Kassen geklärt worden ist. Für beide Einsatzgebiete bieten sich Pseudonymisierungs- und Anonymisierungsverfahren an. (Die genauen Vorstellungen werden derzeit im Forum Info 2000 Arbeitsgruppe Gesundheitswesen beraten und präzisiert).
Die Beispiele Krebsregister und QuaSiNiere zeigen die Möglichkeiten und auch die Grenzen für den Einsatz von datenschutzfreundlichen Technologien im Gesundheitswesen.
Wichtige, in Zukunft anstehende Fragen wie nationalstaatenübergreifende Datenübermittlung, Einrichtung einer Treuhänderstelle eventuell auch im Ausland, Sicherheit (Zertifizierung) von Pseudonymisierungsalgorithmen, verfahrenübergreifende Pseudonyme etc. sind allerdings noch nicht in Angriff genommen worden. Hierzu zählen auch Modelle, die im Rahmen der Informationsgesellschaft und zur Senkung der Gesundheitskosten zur Diskussion stehen.

## 4. Datenschutzfreundliche Technologien in der Telekommunikation

Bezüglich des Einsatzes datenschutzfreundlicher Technologien und zugehöriger Bewertungsmodelle wird auf das Papier der Arbeitsgruppe „Datenvermeidung in der Telekommunikation" des Arbeitskreises „Technische und organisatorische Datenschutzfragen" der Datenschutzbeauftragten des Bundes und der Länder verwiesen.
In diesem Papier wird zunächst der Systembegriff für Telekommunikationssysteme (TK-Systeme) präzisiert. Dazu wird unter anderem ein allgemeines TK-Datenmodell eingeführt. In diesem Zusammenhang können auch die Begriffe Datenvermeidung, Anonymisierung und Pseudonymisierung näher definiert und ein Bewertungsmodell entwickelt werden. Mit den zuvor entworfenen Hilfsmitteln werden anschließend einige gebräuchliche TK-Verfahren untersucht. Um Wege zur Minimierung der in diesen Verfahren anfallenden personenbezogenen Daten aufzuzeigen, werden einige besonders geeignete Technologien näher vorgestellt.

## 5. Datenschutzfreundliche Technologien im Bereich Transport und Verkehr

Im Bereich Transport und Verkehr gibt es folgende alte und neue Entwicklungen mit Relevanz für den Datenschutz:

### 5.1 „Klassische" EDV

Der „klassische" Einsatz von EDV im Bereich Transport und Verkehr entspricht dem EDV-Einsatz in anderen Bereichen. Als Beispiele seien hier die dv-gestützten Verfahren zur Kfz-Zulassung, zur Verwaltung von Führerscheinen, zur Verkehrskontrolle, zur Unfallaufnahme und zur Verwaltung von Daten über Kunden und Personal von Verkehrsbetrieben genannt. Soweit datenschutzfreundliche Technologien hier einsetzbar sind, wäre dies auch für viele andere Bereiche von Bedeutung. Durch mehr Datensparsamkeit sind sicherlich vielfach datenschutzfreundlichere Verfahren möglich. Dies hat aber seine Grenzen. So ist die Führung einer Kfz-Führer-

Sünderdatei unter Pseudonymen zwar weitgehend möglich und wird bei Nutzung relationaler Datenbanksysteme auf technischer Ebene sogar praktiziert. Letztendlich muß aber die Zusammenführung der Sünder-Daten mit den Personendaten immer möglich sein.

## 5.2 Chipkarteneinsatz bei Benutzung von Verkehrsmitteln

Zur Zeit werden an vielen Stellen im Öffentlichen Personennahverkehr (ÖPNV) und im Fährverkehr Chipkarten zur Bezahlung von Fahrkarten oder als Fahrkartenersatz eingeführt (z. B. in Skandinavien, Pilotprojekte in Deutschland). Es werden im wesentlichen folgende Einsatzmöglichkeiten erprobt:

a) Postpaid-Karte, Speicherung aller Fahrten, Ermittlung des günstigsten Tarifs (Bestpreisermittlung), Bezahlung über Lastschriftverfahren
b) Prepaid-Karte, Aufladung eines Geldbetrages, von dem der Fahrpreis abgebucht wird. Prepaid-Karten sind entweder
   b.1 anonym (nur einmal benutzbare Karten wie Telefonkarten oder mit Bargeld aufladbare Karten),
   b.2 oder die Aufladung erfolgt personenbezogen durch Überweisung vom Girokonto, die Abbuchung des Fahrpreises erfolgt anonym vom aufgeladenen Geldbetrag.

Häufig wird, zum Teil aufgrund von Forderungen der Datenschutzbeauftragten, neben der Postpaid-Karte auch die Prepaid-Karte alternativ angeboten. Neben diesen Unterscheidungen gibt es viele weitere Unterscheidungsmerkmale der chipkartengestützten Fahrkartensysteme wie kontaktlose oder nicht kontaktlose Chipkarten und Multifunktionskarten.
Beispiele für geplante und eingeführte Systeme oder Projekte:

- EC-Karte (zu b.2): Abbuchung vom Girokonto Anbieter: Banken und Sparkassen/ ÜSTRA in Hannover u. a.
- Pay-Card (alternativ b.1 oder b.2): Abbuchung über Telefonrechnung oder Barzahlung Anbieter: Telekom/DB, ÖPNV in Hamburg, Stuttgart, München, Rhein-Main
- FAHRSMART (alternativ a oder b.1): Abrechnung und Abbuchung durch Terminals des ÖPNV Anbieter: KVG Lüneburg, Oldenburg
- NORDERNEY-Card (im wesentlichen b.1): Fährticket nach Norderney, multifunktionale Berechtigungskarte für Kureinrichtungen, ÖPNV auf Norderney usw.; zumindest die Gästekarte kommt ohne jeglichen Personenbezug aus, weil jeder Gast eine Karte erwerben und diese beim Verlassen der Insel vorzeigen muß. Es ist möglich, Schattenkonten ohne personenbezogene Daten zu führen, die bei einer Zerstörung und u. U. auch bei einem Verlust der Karte die Erstellung eines Duplikats ermöglichen. Anbieter: Kurverwaltung, Reederei, Stadt Norderney u. a.

Neben Dauerkarten wie Monats- oder Jahreskarten sind Prepaid-Karten eine datenschutzfreundliche Alternative. Prepaid-Karten sind in der Verwendung allerdings umständlicher als Postpaid-Karten, so daß möglicherweise viele Kunden auf diese Alternative verzichten. Deshalb sollte auch das Postpaid-Verfahren möglichst datenschutzgerecht gestaltet werden. Bei Postpaid-Verfahren ist durch eine strikte Trennung von Kontoabbuchung und Fahrpreisberechnung eine datenschutzfreundliche Technologie möglich. Das Kreditinstitut übernimmt die Ausgabe der Postpaid-Chip-

karten an die Kunden, speichert die Personalien und das zugehörige Konto. Es bekommt den Gesamtpreis der monatlichen oder vierteljährlichen Fahrtkosten vom Verkehrsbetrieb übermittelt und übernimmt die Überweisung des Gesamtpreises an den Verkehrsbetrieb. Bei der Überweisung an den Verkehrsbetrieb wird ein kartenbezogenes Pseudonym verwendet, der Verkehrsbetrieb erfährt somit nicht, wem die Karte gehört. Der Verkehrsbetrieb speichert für jedes Pseudonym die für die Abrechnung erforderlichen Daten (Fahrpreisdaten, Bestpreisermittlung usw.), gibt aber nur den ermittelten Gesamtpreis an das Kreditinstitut weiter.

### 5.3 Zahlungs- und Überwachungssysteme für die Benutzung von Verkehrsstraßen

Die politischen Ziele und Kriterien, die mit der Erhebung von strecken- und zeitbezogenen Straßenbenutzungsgebühren (road-pricing) im Zusammenhang mit Autobahnmaut, Citymaut oder Parktickets verfolgt werden, sind u. a.
- Verkehrslenkung,
- gerechte Anlastung der Wegekosten,
- private Finanzierungsmöglichkeiten,
- Verbesserung der Infrastruktur Autobahn, Schienenverkehr und
- Umweltschutz (Schadstoffemission, Rohstoffverbrauch),
  wobei die Gewichtung für Autobahn-Maut-Systeme sich von der für City-Maut-Systeme durchaus unterscheidet.

Erprobt wurden solche Systeme u. a.
- mit dem Feldversuch des baden-württembergischen Verkehrsministeriums auf der B 27 in Stuttgart,
- mit dem Feldversuch des Bundesverkehrsministeriums auf der A 555 zwischen Bonn und Köln.

Die Forderungen der Datenschützer zur Anonymität, Vertraulichkeit, Integrität, Transparenz und Rücknahmefestigkeit haben sich von den Herstellerfirmen nicht umfassend realisieren lassen.
Einige der Forderungen waren umsetzbar. Unter dem Aspekt der Datenschutzfreundlichkeit lassen sich insbesondere folgende Erkenntnisse festhalten:
- Prepaid-Karten bieten bessere Voraussetzungen zur Wahrung der Anonymität als Postpaid-Karten
- Offene Systeme können datenschutzfreundlicher gestaltet werden als geschlossene Systeme, weil sie ohne Speicherung von Zu- und Abfahrt auskommen, indem beim Vorbeifahren an einer Maut-Stelle die Gebühr fällig bzw. abgebucht wird
- Dezentrale Speicherung im Bereich des Benutzers (z. B. auf einer Chipkarte) könnte zur Vermeidung von Bewegungsprofilen genutzt werden

Größere Probleme wurden bei den Kontrollverfahren sichtbar. Es dürfte schwierig sein, ein Kontrollverfahren zu entwickeln, das einerseits hinreichend beweissicher ist und andererseits den Anforderungen des Datenschutzes genügt.
Beide Feldversuche wurden beendet, ohne daß eine Umsetzung für einen Echtbetrieb erfolgt wäre. Für den Autobahn-Maut-Versuch hat dies neben offenen Datenschutzfragen sicher u. a. auch mit der Systeminfrastruktur und ihren Kosten sowie mit der Durchsetzbarkeit solcher Verfahren zu tun.
In der Diskussion ist immer wieder die streckenbezogene Autobahn-Maut für LKW.

Hier sind die technischen Gegebenheiten (z. B. Nutzung von GPS und Mobilfunk) anders als im Bereich von PKW und Motorrädern. Ob und inwieweit wirklich der Persönlichkeitsschutz in diesem Bereich der fast ausschließlich beruflichen Nutzung weniger beeinträchtigt wird, muß spätestens kurz vor der Einführung solcher Systeme geklärt werden.
Für den PKW-Bereich wird spätestens dann die Maut-Diskussion neu geführt werden,
- wenn die Elektronik und Computerisierung im Fahrzeug sowie die (Mobil-) Kommunikation mit dem Fahrzeug weiter fortgeschritten ist,
- wenn Systeme der Verkehrstelematik größere Verbreitung gefunden haben (u. a. Stauumfahrung, Leitsysteme mit elektronisch gespeicherten Straßenkarten, Diebstahlschutz bzw. Ortung von (gestohlenen) Fahrzeugen, Notruf, elektronische Geldbörse etc. für Park(haus)gebühren und
- wenn damit geringere (zusätzliche) Infrastrukturkosten entstehen.

## 5.4 Sonstige Überwachungssysteme für Verkehrsmittel

Als Beispiele für sonstige Überwachungssysteme für Verkehrsmittel seien hier die Systeme zur Verkehrslenkung, zur Standortbestimmung und zur Ermittlung, Verarbeitung und Weitergabe anderer Daten, z. B. bei Taxiunternehmen, Autovermietern, Speditionen, Bussen und Privatfahrzeugen, genannt.
Eine Überwachung von Verkehrsmitteln ist auf vielfältige Weise möglich:
- Videoüberwachung (z. B. an verkehrsreichen Kreuzungen),
- Überwachung durch andere elektronische Einrichtungen außerhalb der Fahrzeuge (z. B. Induktionsschleifen, Lichtschranken),
- Einrichtungen im Fahrzeug, die bei Bedarf zu Hilfe genommen werden (Fahrtenschreiber),
- Einrichtungen im Fahrzeug, die über Funk abgefragt werden können (Standortbestimmungen über Bakensysteme oder GPS, Funksprechverkehr, sonstige Daten wie Geschwindigkeit, Motorkontrolle usw.)

Von besonderer Bedeutung sind neuere Entwicklungen zu Einrichtungen im Fahrzeug, die über Funk abgefragt werden können (z. B. bei Taxizentralen in Hamburg oder Kassel). Alternative, datenschutzfreundlichere Technologien, die den erforderlichen Funktionsumfang abdecken, sind nicht erkennbar. Vielmehr muß im Einzelfall überprüft werden, ob der Funktionsumfang tatsächlich erforderlich ist. So ist zu prüfen, ob tatsächlich eine Überwachung per Funk durch die Zentrale notwendig ist oder ob eine passive Nutzung etwa von GPS durch den Fahrer ausreicht. Ebenso ist zu erfragen, ob Videoüberwachungen tatsächlich erforderlich sind oder ob eine Überwachung durch Induktionsschleifen usw. ausreicht.

# 16 Materialien

## 16.1 Entschließungen der Konferenz des Datenschutzbeauftragten des Bundes und der Länder

### 16.1.1 Entschließung der 54. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 23./24. Oktober 1997 in Bamberg zur Novellierung des Bundesdatenschutzgesetzes und zur Modernisierung des Datenschutzrechts

Die fristgerechte Harmonisierung des Datenschutzes entsprechend den Vorgaben der europäischen Datenschutzrichtlinie vom 24. Oktober 1995 droht zu scheitern. Die von dieser Richtlinie gesetzte Dreijahresfrist wird heute in einem Jahr ablaufen. Eine gründliche Beratung im Deutschen Bundestag wird durch den baldigen Ablauf der Legislaturperiode in Frage gestellt.

Noch immer gibt es keinen Kabinettsbeschluß; die Bundesregierung hat bisher noch nicht einmal einen abgestimmten Referentenentwurf vorgelegt. Sie gefährdet dadurch die rechtzeitige Umsetzung der Richtlinie und riskiert ein Vertragsverletzungsverfahren vor dem Europäischen Gerichtshof.

Für die Entwicklung des Datenschutzes ist diese Lage höchst nachteilig:

– Verbesserungen des Datenschutzes der Bürger, z.B. durch genauere Information über die Verarbeitung ihrer Daten, verzögern sich;

– dem Datenschutzrecht droht Zersplitterung, weil den Ländern eine Orientierung für die Anpassung der Landesdatenschutzgesetze fehlt.

Die Datenschutzbeauftragten des Bundes und der Länder appellieren daher an die Bundesregierung, für eine fristgerechte Umsetzung der Richtlinie Sorge zu tragen.

Zur Harmonisierung des europäischen Datenschutzrechts empfehlen die Datenschutzbeauftragten der Bundesregierung und dem Gesetzgeber folgende Grundsatzentscheidungen:

– weitgehende Gleichbehandlung des öffentlichen und des privaten Bereichs bei gleichzeitiger Verbesserung der Datenschutzkontrolle, insbesondere durch generell anlaßunabhängige Kontrolle und durch die ausdrückliche Festlegung der völligen Unabhängigkeit der Aufsichtsbehörden und die Erweiterung ihrer Eingriffsbefugnisse;

– Bestellung weisungsfreier Datenschutzbeauftragter auch bei öffentlichen Stellen mit dem Recht, sich jederzeit an den Bundes- oder Landesbeauftragten für den Datenschutz zu wenden;

– Bürgerfreundlichkeit durch einfache und verständliche Formulierung des BDSG, z. B. durch einen einheitlichen Begriff der Verarbeitung personenbezogener Daten entsprechend der Richtlinie;

– Gewährleistung eines einheitlichen, hohen Datenschutzniveaus durch Beibehaltung der Funktion des BDSG und der Landesdatenschutzgesetze als Querschnittsgesetze sowie durch Vermeidung eines Gefälles zwischen den Bereichen, die der EG-Datenschutzrichtlinie unterfallen, und den übrigen Gebieten, deren Datenschutzregelungen nicht verschlechtert werden dürfen;

– Sonderregelungen für Presse und Rundfunk nur, soweit zur Sicherung der Meinungsfreiheit notwendig.

Als ebenso vordringlich betrachten die Datenschutzbeauftragten eine Anpassung der noch von der Großrechnertechnologie der siebziger Jahre bestimmten gesetzlichen Regelungen an die heutige Informationstechnologie und an die Verhältnisse der modernen Informationsgesellschaft. Dazu gehören insbesondere folgende Punkte:

– Verbindliche Grundsätze für die datenschutzfreundliche Gestaltung von Informationssystemen und -techniken, so zur Datensparsamkeit, zur Anonymisierung und Pseudonymisierung, zur Verschlüsselung und zur Risikoanalyse;

– mehr Transparenz für die Verbraucher und mehr Eigenständigkeit für die Anbieter durch Einführung eines Datenschutzaudits;

– Erweiterung des Schutzbereichs bei Bild- und Tonaufzeichnungen, Regelung der Video-Überwachung;

– Sonderregelungen für besonders empfindliche Bereiche, wie den Umgang mit Arbeitnehmerdaten, Gesundheitsdaten und Informationen aus gerichtlichen Verfahren;

– Einführung einer Vorabkontrolle für besonders risikoreiche Datenverarbeitung, namentlich bei Verarbeitung sensitiver Daten;

– Regelungen für Chipkarten-Anwendungen;

– Verstärkung des Schutzes gegenüber Adressenhandel und Direktmarketing, unter anderem auch mindestens durch die Festlegung von Hinweispflichten hinsichtlich der Möglichkeit des Widerspruchs; vorzuziehen ist in jedem Fall eine Einwilligungsregelung;

– Verstärkung des Schutzes gegenüber der Einholung von Selbstauskünften vor Abschluß von Miet-, Arbeits- und ähnlich existenzwichtigen Verträgen;

– Datenexport nach Inlandsgrundsätzen nur bei angemessenem Schutzniveau im Empfängerstaat; Festlegung, unter welchen Voraussetzungen ein Mitgliedstaat Da-

ten, die er im Anwendungsbereich der Richtlinie (also nach Inlandsgrundsätzen) erhalten hat, außerhalb ihres Anwendungsbereichs verwenden darf;

– möglichst weitgehende Ersetzung der Anmeldung von Dateien bei der Aufsichtsbehörde durch Bestellung weisungsfreier Datenschutzbeauftragter; Beibehaltung des internen Datenschutzbeauftragten auch bei Sicherheitsbehörden;

– Stärkung der Kontrollrechte des Bundesbeauftragten und der Landesbeauftragten für den Datenschutz durch uneingeschränkte Kontrollbefugnis bei der Verarbeitung personenbezogener Daten in Akten einschließlich solcher über Sicherheitsüberprüfungen.

Die Konferenz weist ferner auf die Rechtspflicht der Länder hin, ihr Datenschutzrecht ebenfalls der EG-Richtlinie fristgerecht anzupassen.

### 16.1.2 Entschließung der 54. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 23./24. Oktober 1997 in Bamberg zur Informationellen Selbstbestimmung und zu Bild-Ton-Aufzeichnungen bei Vernehmungen im Strafverfahren

Überlegungen des Gesetzgebers und eine beginnende öffentliche Diskussion, moderne Dokumentationstechnik der Wahrheitsfindung und dem Zeugenschutz in gerichtlichen Verfahren nutzbar zu machen, liegen auch im Interesse des Datenschutzes. Dabei ist allerdings zu beachten, daß Bild-Ton-Aufzeichnungen von Vernehmungen im Strafverfahren einen erheblichen Eingriff in das Persönlichkeitsrecht darstellen. Sie spiegeln die unmittelbare Betroffenheit der Beschuldigten oder Zeugen in Mimik und Gestik umfassend wider. Zweck und Erforderlichkeit dieses Eingriffs bedürfen einer sorgfältigen Begründung durch den Gesetzgeber. Sie bildet den Maßstab, der über Möglichkeiten, Grenzen und Verfahren der Videotechnologie im Strafprozeß entscheidet. Erkennbar und nachvollziehbar sollte sein, daß der Gesetzgeber die Risiken des Einsatzes dieser Technologie, insbesondere die Verfügbarkeit der Aufzeichnungen nach den allgemeinen Vorschriften über die Beweisaufnahme bedacht und bewertet hat. Ferner sollte erkennbar und nachvollziehbar sein, daß Alternativen zur Videotechnologie, namentlich die Verwendung von Tonaufzeichnungen, in die Erwägungen des Gesetzgebers aufgenommen wurden.

Nach Auffassung der Datenschutzbeauftragten des Bundes und der Länder sollten die vorliegenden Gesetzentwürfe des Bundesrates (BT-Drs. 13/4983 vom 19.06.1996) sowie der Fraktionen der CDU/CSU und F.D.P. (BT-Drs. 13/7165 vom 11.03.1997) in einem umfassenderen Bedeutungs- und Funktionszusammenhang diskutiert werden. Zunehmend tritt das Anliegen der Praxis hervor, Bild-Ton-Aufzeichnungen auch mit anderer Zielsetzung zu verwerten:

Bild-Ton-Aufzeichnungen ermöglichen eine vollständige und authentische Dokumentation nicht nur des Inhalts, sondern auch der Entstehung und Begleitumstände einer Aussage. Die Beurteilung ihres Beweiswerts wird dadurch deutlich verbessert. Zugleich dient eine nur einmalige Vernehmung, die möglichst zeitnah zum Tat-

geschehen durchgeführt und aufgezeichnet wird, der Wahrheitsfindung und erhöht die Qualität der gerichtsverwertbaren Daten („Vermeidung kognitiver Dissonanzen“). Ausgehend von diesen Überlegungen, hat der Gesetzgeber unter Einbeziehung von Erkenntnissen der Vernehmungspsychologie zu prüfen, ob und inwieweit eine wortgetreue Abfassung von Vernehmungsniederschriften ausreicht und eine Aufzeichnung der Aussage nur im Wort auf Tonband für die Zwecke des Strafverfahrens in ihrer Beweisqualität der Videotechnologie sogar überlegen ist.

Für Videoaufzeichnungen des Betroffenen, die zu seinem Schutz gefertigt werden sollen, ist dessen Einwilligung unverzichtbare Voraussetzung für die Zulässigkeit einer Bild-Ton-Aufzeichnung im Strafverfahren. Sofern der Betroffene nicht in der Lage ist, die Bedeutung und Tragweite einer Bild-Ton-Aufzeichnung und ihrer Verwendungsmöglichkeiten hinreichend zu beurteilen, hat der Gesetzgeber festzulegen, wer anstelle des Betroffenen die Einwilligung erteilen darf. Vor Abgabe der Einwilligungserklärung ist der Betroffene umfassend aufzuklären, insbesondere auch über alle zulässigen Arten der weiteren Verwertung und über die Möglichkeit des Widerrufs der Einwilligung für die Zukunft. Die Aufklärung ist zuverlässig zu dokumentieren. Entsprechendes gilt für die Herausgabe von Videoaufzeichnungen.

Die Datenschutzbeauftragten des Bundes und der Länder fordern wirksame Vorkehrungen zum Schutz des Persönlichkeitsrechts bei Verwendung von Bild-Ton-Aufzeichnungen im Strafverfahren. Unabhängig von der Frage, welche Zielsetzung mit Bild-Ton-Aufzeichnungen im Strafverfahren verfolgt werden soll, sind hierbei insbesondere folgende Gesichtspunkte von Bedeutung:

1. Es ist sicherzustellen, daß der Eindruck des Aussagegeschehens z. B. durch Zeitlupe, Zeitraffer, Einzelbildabfolge, Standbild und Zoom nicht gezielt verfremdet oder verzerrt wird.

2. Einsatz und Verwertung von Bild-Ton-Aufzeichnungen sind so zu regeln, daß gesetzliche Zeugnisverweigerungsrechte gewahrt bleiben. Insbesondere ist eine weitere Nutzung der Aufnahme, auch zum Zwecke des Vorhalts, ausgeschlossen, wenn sich ein Zeuge auf sein Zeugnisverweigerungsrecht beruft.

3. Vorbehaltlich des o. g. Einwilligungserfordernisses darf eine Übermittlung von Videoaufzeichnungen an Stellen außerhalb der Justiz, wenn überhaupt, nur in Ausnahmefällen erlaubt sein, da nur so ein wirksamer Schutz vor Mißbrauch, etwa durch kommerzielle Verwertung, gewährleistet werden kann. Soweit der Gesetzgeber aus Gründen eines fairen, rechtsstaatlichen Strafverfahrens die Weitergabe von Videokopien an Verfahrensbeteiligte zuläßt, müssen jedenfalls wirksame Vorkehrungen gegen Mißbrauch gewährleistet sein, z. B. sichtbare Signierung und strafbewehrte Regelungen über Zweckbindungen und Löschungsfristen.

4. Eine Verwertung der Aufzeichnungen im Rahmen eines anderen Strafverfahrens ist nur zulässig, soweit sie auch für die Zwecke dieses anderen Verfahrens hätten angefertigt werden dürfen.

5. Soweit eine Verwertung in einem anderen gerichtlichen Verfahren - etwa zur Vermeidung erneuter Anhörung kindlicher Zeugen vor dem Familien- oder Vormundschaftsgericht - zugelassen werden sollte, sind in entsprechenden Ausnahmeregelungen präzise Voraussetzungen hierfür abschließend zu bestimmen und enge Verwendungsregelungen zu treffen.

6. Spätestens mit dem rechtskräftigen Abschluß des Strafverfahrens sind grundsätzlich die Aufzeichnungen unter Aufsicht der Staatsanwaltschaft zu vernichten. Der Betroffene ist davon zu benachrichtigen. Soweit der Gesetzgeber ausnahmsweise zur Wahrung vorrangiger Rechtsgüter eine längere Aufbewahrung der Aufzeichnungen zuläßt, müssen Voraussetzungen, Umfang und Fristen der weiteren Aufbewahrung klar und eng geregelt werden.

### 16.1.3 Entschließung der 54. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 23./24. Oktober 1997 in Bamberg zur Erforderlichkeit datenschutzfreundlicher Technologien

Moderne Informations- und Telekommunikationstechnik (IuK-Technik) gewinnt in allen Lebensbereichen zunehmende Bedeutung. Die Nutzer wenden diese Technik z. B. in Computernetzen, Chipkartensystemen oder elektronischen Medien in vielfältiger Weise an und hinterlassen dabei zumeist umfangreiche elektronische Spuren. Dabei fällt in der Regel eine Fülle von Einzeldaten an, die geeignet sind, persönliche Verhaltensprofile zu bilden.

Den Erfordernissen des Datenschutzes wird nicht in ausreichendem Maße Rechnung getragen, wenn sich der Schutz der Privatheit des einzelnen lediglich auf eine Beschränkung des Zugangs zu bereits erhobenen, gespeicherten und verarbeiteten personenbezogenen Daten reduziert. Daher ist es erforderlich, bereits vor der Erhebung und Speicherung die zu speichernde Datenmenge wesentlich zu reduzieren.

Datensparsamkeit bis hin zur Datenvermeidung, z. B. durch Nutzung von Anonymisierung und Pseudonymisierung personenbezogener Daten, spielen in den unterschiedlichen Anwendungsbereichen der IuK-Technik, wie elektronischen Zahlungsverfahren, Gesundheits- oder Verkehrswesen, bisher noch eine untergeordnete Rolle. Eine datenschutzfreundliche Technologie läßt sich aber nur dann wirksam realisieren, wenn das Bemühen um Datensparsamkeit die Entwicklung und den Betrieb von IuK-Systemen ebenso stark beeinflußt wie die Forderung nach Datensicherheit.

Die Datenschutzbeauftragten des Bundes und der Länder wollen in Zusammenarbeit mit Herstellern und Anbietern auf datenschutzgerechte Lösungen hinarbeiten. Die dafür erforderlichen Techniken stehen weitgehend schon zur Verfügung. Moderne kryptographische Verfahren zur Verschlüsselung und Signatur ermöglichen die Anonymisierung oder Pseudonymisierung in vielen Fällen, ohne daß die Verbindlichkeit und Ordnungsmäßigkeit der Datenverarbeitung beeinträchtigt werden. Diese Möglichkeiten der modernen Datenschutztechnologie, die mit dem Begriff „Privacy enhancing technology (PET)“ eine Philosophie der Datensparsamkeit beschreibt und ein ganzes System technischer Maßnahmen umfaßt, sollten genutzt werden.

Vom Gesetzgeber erwarten die Datenschutzbeauftragten des Bundes und der Länder, daß er die Verwendung datenschutzfreundlicher Technologien durch Schaffung rechtlicher Rahmenbedingungen forciert. Sie begrüßen, daß sowohl der Mediendienste-Staatsvertrag der Länder als auch das Teledienstedatenschutzgesetz des Bundes bereits den Grundsatz der Datenvermeidung normieren. Der in den Datenschutzgesetzen des Bundes und der Länder festgeschriebene Grundsatz der Erforderlichkeit läßt sich in Zukunft insbesondere durch Berücksichtigung des Prinzips der Datensparsamkeit und der Verpflichtung zur Bereitstellung anonymer Nutzungsformen verwirklichen. Die Datenschutzbeauftragten des Bundes und der Länder bitten darüber hinaus die Bundesregierung, sich im europäischen Bereich dafür einzusetzen, daß die Förderung datenschutzfreundlicher Technologien entsprechend dem Vorschlag der Kommission in das 5. Rahmenprogramm „Forschung und Entwicklung“ aufgenommen wird.

Neben Anbietern von Tele- und Mediendiensten sollten auch die Hersteller und Anbieter von IuK-Technik bei der Ausgestaltung und Auswahl technischer Einrichtungen dafür gewonnen werden, sich am Grundsatz der Datenvermeidung zu orientieren und auf eine konsequente Minimierung gespeicherter personenbezogener Daten achten.

### 16.1.4 Entschließung der 55. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 19./20. März 1998 in Wiesbaden zu Datenschutzproblemen der Geldkarte

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder wiederholt ihre Forderung aus ihrer Entschließung vom 13.10.1995 nach einem anonymen elektronischen Zahlungsverfahren bei elektronischen Geldbörsen. Dies gilt insbesondere für die Geldkarte des deutschen Kreditwesens, bei der in kartenbezogenen „Schattenkonten“ der Evidenzzentralen nicht nur der Kaufbetrag und ein identifizierbarer Händlerschlüssel, sondern auch der Kaufzeitpunkt gespeichert werden. Mit diesen Daten können sämtliche mit der Geldkarte getätigten Kaufvorgänge jahrelang nachvollzogen werden, wenn die Daten mit den persönlichen Kundendaten zusammengeführt werden. Diese Geldkarte erfüllt nicht die Forderungen der Datenschutzbeauftragten.

Außerdem werden die Kundinnen und Kunden über diese „Schattenkonten“ noch nicht einmal informiert. Die Herausgeber solcher Karten bzw. die Kreditinstitute haben aber die Pflicht, ihre Kundinnen und Kunden über Art und Umfang der im Hintergrund laufenden Verarbeitungsvorgänge zu informieren.

Unabhängig davon müssen bei der Geldkarte des deutschen Kreditwesens sämtliche Umsatzdaten in den Evidenzzentralen und auch bei den Händlern nach Abschluß der Verrechnung (Clearing) gelöscht oder zumindest anonymisiert werden.

Die Datenschutzbeauftragten fordern die Kartenherausgeber und die Kreditwirtschaft erneut dazu auf, vorzugsweise kartengestützte Zahlungssysteme ohne personenbezo-

gene Daten - sog. White Cards - anzubieten. Die Anwendung ist so zu gestalten, daß ein karten- und damit personenbezogenes Clearing nicht erfolgt.

Der Gesetzgeber bleibt aufgerufen sicherzustellen, daß auch in Zukunft die Möglichkeit besteht, im wirtschaftlichen Leben im gleichen Umfang wie bisher bei Bargeldzahlung anonym zu bleiben.

### 16.1.5 Entschließung der 55. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 19./20. März 1998 in Wiesbaden zum Datenschutz beim digitalen Fernsehen

Die Datenschutzbeauftragten des Bundes und der Länder machen darauf aufmerksam, daß bei elektronischen Diensten immer umfangreichere Datenspuren über das Verhalten der Einzelnen entstehen. Mit der Digitalisierung der Fernseh- und Hörfunkübertragung entsteht die technische Infrastruktur dafür, daß erstmals auch das individuelle Mediennutzungsverhalten registriert werden kann. Sie bekräftigen deshalb ihre Forderung, daß auch bei der Vermittlung und Abrechnung digitaler Fernsehsendungen eine flächendeckende Registrierung des individuellen Fernsehkonsums vermieden wird. Im digitalen Fernsehen („Free TV“ und „Pay TV“) muß die unbeobachtete Nutzung des Mediums ohne Nachteile möglich bleiben.

Die Datenschutzbeauftragten begrüßen es deshalb, daß die Staats- und Senatskanzleien Vorschläge für die Änderung des Rundfunkstaatsvertrags vorgelegt haben, mit denen Belangen des Datenschutzes Rechnung getragen werden soll. Besonders hervorzuheben sind folgende Punkte:

- Die Gestaltung technischer Einrichtungen muß sich an dem Ziel ausrichten, daß so wenige personenbezogene Daten wie möglich erhoben, verarbeitet und genutzt werden;
- die Rundfunkveranstalter müssen die Nutzung und Bezahlung von Rundfunkangeboten anonym oder unter Pseudonym ermöglichen, soweit dies technisch möglich und zumutbar ist;
- personenbezogene Daten über die Inanspruchnahme einzelner Sendungen dürfen für Abrechnungszwecke nur gespeichert werden, wenn ein Einzelnachweis verlangt wird;
- wie bereits im Mediendienstestaatsvertrag enthält auch der Entwurf des Rundfunkstaatsvertrags eine Vorschrift zum Datenschutzaudit, d. h. Veranstalter können ihr Datenschutzkonzept und ihre technischen Einrichtungen von unabhängigen Gutachtern prüfen und das Prüfungsergebnis veröffentlichen lassen.

Die Datenschutzbeauftragten halten diese Grundsätze für geeignet, eine datenschutzgerechte Nutzung digitaler Fersehangebote zu ermöglichen. Die technischen Möglichkeiten, diesen datenschutzrechtlichen Vorgaben zu entsprechen, sind gegeben. Die Datenschutzbeauftragten konnten sich bereits 1996 hiervon praktisch überzeugen. Die Systementscheidung von Veranstaltern für einen Decodertyp, der möglicherweise weniger geeignet ist, die Datenschutzanforderungen zu erfüllen, kann kein Maßstab für die Angemessenheit dieser Anforderungen sein, wenn zugleich andere Geräte ihnen ohne Probleme genügen.

Der Forderung von Inhabern von Verwertungsrechten, einen Nachweis über die Inanspruchnahme von pay-per-view-Angeboten vorzulegen, kann ohne Personenbezug - etwa durch zertifizierte Zähleinrichtungen oder den Einsatz von Pseudonymen - entsprochen werden.

Die Datenschutzbeauftragten bitten deshalb die Ministerpräsidentin und die Ministerpräsidenten der Länder, an den datenschutzrechtlichen Regelungen des Entwurfs festzuhalten. Damit würden das bisherige Datenschutzniveau für die Fernsehnutzung im digitalen Zeitalter abgesichert und zugleich die Vorschriften für den Bereich des Rundfunks und der Mediendienste harmonisiert.

Die Datenschutzbeauftragten fordern die Rundfunkveranstalter und Hersteller auf, den Datenschutz bei der Gestaltung von digitalen Angeboten schon jetzt zu berücksichtigen.

## 16.2 Sonstiges

### 16.2.1 Personalbogen des Sächsischen Staatsministeriums des Innern

<table>
<tr><td colspan="2">Personalbogen</td><td>1</td><td>Personalnummer[1]</td><td rowspan="3">Lichtbild<br><br>Jahr der Aufnahme des Lichtbildes:</td></tr>
<tr><td>2</td><td colspan="3">Familien- (Geburts-) Name[2], akademischer Grad</td></tr>
<tr><td>3</td><td colspan="3">Vornamen (Rufnamen unterstreichen)</td></tr>
<tr><td>4</td><td colspan="4">Geburtsdatum, Geburtsort, Kreis, Land</td></tr>
<tr><td>5</td><td colspan="5">Anschrift (Straße, Hausnummer, PLZ, Gemeinde)</td></tr>
<tr><td>6</td><td colspan="2">Schwerbehinderung/Gleichstellung<br><br>☐ ja ☐ nein ☐ ja ☐ nein</td><td>7</td><td colspan="2">Staatsangehörigkeit</td></tr>
<tr><td>8</td><td colspan="2">Inhaber eines Eingliederungs- oder Zulassungsscheins[3]<br><br>☐ ja ☐ nein</td><td>9</td><td colspan="2">Religiöses Bekenntnis<br>- nur bei Lehrern und Lehramtsbewerbern für das Lehrfach "Religion"</td></tr>
<tr><td>10</td><td colspan="5">Familienstand<br><br>☐ nicht verheiratet ☐ verheiratet</td></tr>
<tr><td>11</td><td colspan="5">Kinder[4]<br><br>Anzahl Geburtsjahr(e)</td></tr>
<tr><td>12</td><td colspan="5">Nur bei minderjährigen Bewerbern: Eltern, sonst. gesetzliche Vertreter<br>Familien- (Geburts-) Name Vornamen Anschrift (nur wenn von Nr. 5 abweichend)</td></tr>
</table>

[1] Wird von der Dienststelle ausgefüllt

[2] Ggf. auch frühere Familiennamen angeben

[3] § 9 des Soldatenversorgungsgesetzes (gilt nicht für ehemalige NVA-Soldaten)

[4] Angaben nur erforderlich, sofern Unterhaltspflicht besteht

| | | | | | |
|---|---|---|---|---|---|
| **13** | Schulbildung, Studium, Fernstudium | | | | |
| | Schulart, Studienrichtung<br>Ausbildungsstätte | von / bis | Abschlußprüfung (auch Promotion usw.)<br>Art | Datum | Ergebnis |
| | | | | | |
| **14** | Berufsbezogene Ausbildungs-, Laufbahn-, Weiterbildungs- und sonstige Prüfungen | | | | |
| | Art | | | Datum | Ergebnis |
| | | | | | |
| **15** | Besondere Kenntnisse und Fähigkeiten (Sprachkenntnisse, EDV-Kenntnisse usw.) | | | | |
| **16** | Wehrdienst, Zivildienst | | vom | bis | |
| | Vom Wehrdienst / Zivildienst vorzeitig beurlaubt | | vom | bis | |

| **17** | Berufliche Tätigkeit (einschl. Berufsausbildung)<br>Lückenlose Darstellung in zeitlicher Reihenfolge außerhalb und innerhalb des öffentlichen Dienstes (auch Lehrzeiten, Zeiten im Angestellten- und Arbeiterverhältnis, berufliche Lehrgänge, Zeiten ohne Berufstätigkeit);<br>Versetzungen, Abordnungen, Beurlaubungen, Freistellungen, Teilzeitbeschäftigungen | | |
|---|---|---|---|
| | vom / bis | Arbeitgeber / Dienststelle / Selbständiger | Art / Umfang der Tätigkeit / Maßnahme |
| | | | |

| | | | |
|---|---|---|---|
| **18** | Laufbahnrechtlicher Werdegang (einschl. Vorbereitungsdienst) | | |
| | Ernennung / Amtsübertragung | am | mit Wirkung vom |
| | | | |
| **19** | Bemerkungen (z. B. Nebentätigkeiten im Zeitpunkt der Bewerbung) | | |
| | | | |

Ort / Datum

Unterschrift

## 16.2.2 Bewerbungsbogen für die Bestellung von Bürgern zu Angehörigen der Sächsischen Sicherheitswacht[1]

<table>
<tr><td colspan="4">Hinweise nach § 11 Abs. 2 Sächsisches Datenschutzgesetz (SächsDSG):<br>Die Angaben sind erforderlich, um zu prüfen, ob die Voraussetzungen für die Bestellung zur Sicherheitswacht im Sinne des Sächsischen Sicherheitswachterprobungsgesetzes vorliegen.</td></tr>
<tr><td colspan="3">1) Familien- (Geburts) Name[2], akademischer Grad</td><td rowspan="3">Lichtbild<br><br>Jahr der Aufnahme des Lichtbildes:</td></tr>
<tr><td colspan="3">2) Vornamen (Rufnamen unterstreichen)</td></tr>
<tr><td colspan="3">3) Geburtsdatum, Geburtsort, Kreis, Land</td></tr>
<tr><td colspan="4">4) Anschrift (Straße, Hausnummer, PLZ, Gemeinde)</td></tr>
<tr><td>5) Staatsangehörigkeit</td><td colspan="2">6) Schwerbehinderung/Gleichstellung<br>☐ ja ☐ nein ☐ ja ☐ nein</td><td>7) Brillenträger<br>☐ ja ☐ nein</td></tr>
<tr><td colspan="4">8) Familienstand<br>☐ nicht verheiratet ☐ verheiratet</td></tr>
<tr><td colspan="4">9) Schulabschluß/Berufsausbildungen</td></tr>
<tr><td>Art</td><td>Schule, Ausbildungs-stätte</td><td>Datum der Abschluß-prüfung</td><td>Ergebnis</td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
</table>

[1] Füllen Sie bitte den Bewerbungsbogen vollständig in Druckschrift oder mit Schreibmaschine aus. Beantworten Sie die einzelnen Frangen erschöpfend. Reicht der Raum des Vordrucks dafür nicht aus, so setzen Sie die Beantwortung unter Bezugnahme auf die Nummer auf einem Einlegeblatt fort. Nur die richtige, vollständige und erschöpfende Beantwortung der Fragen gestattet eine zügige Bearbeitung.

[2] Ggf. auch frühere Familiennamen angeben.

10) Derzeit ausgeübte Berufe/Tätigkeiten

| Art | Umfang | Ort |
|---|---|---|
| | | |

11) Tätigkeiten im öffentlichen Dienst

| Art | Dienststelle | von/bis | Ggf. Grund der Beendigung |
|---|---|---|---|
| | | | |

Mit der Einsichtnahme in meine Personalunterlagen bin ich einverstanden.

12) Besondere Kenntnisse und Fähigkeiten (z. B. Sprachkenntnisse, Maschinenschreiben, Jagdschein, waffenrechtl. Erlaubnis, Sportabzeichen)

**Hinweis gem. § 11 Abs. 2 SächsDSG:** Die Angaben unter Nummer 12 sind freiwillig. Sie können von diesen Angaben absehen, ohne Nachteile befürchten zu müssen. Eine datenmäßige Speicherung erfolgt nicht.

13) Bewerbung

Ich bewerbe mich um die Bestellung zur Sicherheitswacht und gebe dazu folgende Erklärung ab:

Ich erkläre hiermit,
- daß ich in geordneten wirtschaftlichen Verhältnissen lebe,
- daß mir nicht bekannt ist, daß gegen mich ein Strafverfahren oder ein strafrechtliches Ermittlungsverfahren anhängig ist,
- daß mir nicht bekannt ist, daß ein den o. g. Verfahren entsprechendes ausländisches Verfahren anhängig ist bzw. eine Maßnahme in einem solchen Verfahren gegen mich verhängt worden ist,
- daß ich mit einer Abfrage im Polizeilichen Auskunftssystem Sachsen (PASS)/Informationssystem der Polizei (INPOL) zu meiner Person einverstanden bin und
- daß ich mit der Durchführung der ggf. notwendigen ärztlichen Untersuchungen zur Beurteilung meiner Diensttauglichkeit einverstanden bin.

Ferner erkläre ich mein Einverständnis mit der Heranziehung und Nutzung etwaiger über mich vorhandener personenbezogener Daten aus
- den Unterlagen der Zentralen Beweis- und Dokumentationsstelle der Landesjustizverwaltungen in Salzgitter (seinerzeit mit der Erfassung von strafrechtlich relevanten Menschenrechtsverletzungen in der DDR beauftragt) und
- den Unterlagen des ehemaligen Ministeriums für Staatssicherheit/Amt für Nationale Sicherheit der DDR zum Zweck der Einsichtnahme durch den Freistaat Sachsen entsprechend dem Stasi-Unterlagen-Gesetz (StUG).

Mir ist bekannt, daß mir ein durch das Bestellungsverfahren entstehender Verdienstausfall nicht erstattet werden kann.

Ich versichere, daß ich die vorstehenden Fragen vollständig und nach bestem Wissen und Gewissen beantwortet habe. Ich weiß, daß eine falsche Angabe die Einstellung des Bewerbungsverfahrens bzw. den Widerruf der Bestellung (Entlassung) nach sich ziehen kann.

| Ort, Datum | Unterschrift der Bewerberin / des Bewerbers |
|---|---|