Sächsischer Landtag
3. Wahlperiode

DRUCKSACHE 3/4541

Schutz des Persönlichkeitsrechts im öffentlichen Bereich

9. Tätigkeitsbericht

des

Sächsischen Datenschutzbeauftragten

Dem Sächsischen Landtag

vorgelegt zum 31. März 2001

gemäß § 27 des Sächsischen Datenschutzgesetzes

Eingegangen am: 23. August 2001 Ausgegeben am: 23. August 2001

Vorbemerkung zum Sprachgebrauch in diesem Bericht:

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

Beim Datenschutz wird der einzelne Mensch ganz groß geschrieben (im übertragenen Sinne). Dem soll die Rechtschreibung entsprechen: Mit dem Bundesverfassungsgericht - und bisher gegen den Duden - schreibe ich den „Einzelnen" groß. Dies betont seine Individualität, nie den Individualismus. Neuerdings habe ich die reformierte Rechtschreibung in diesem Punkt auf meiner Seite.

Herausgeber: Der Sächsische Datenschutzbeauftragte
Dr. Thomas Giesen
Bernhard-von-Lindenau-Platz 1 Postfach 12 09 05
01067 Dresden 01008 Dresden
Telefon: 0351/4935401
Telefax: 0351/4935490

Besucheranschrift: Devrientstraße 1
01067 Dresden

Vervielfältigung erwünscht.

Herstellung: OTTO Verlag & Druckerei OHG
Gedruckt auf chlorfreiem Papier.

Inhaltsverzeichnis

Abkürzungsverzeichnis

Vorschriften

Nachstehend werden Gesetze und andere Vorschriften nach der alphabetischen Reihenfolge der *amtlichen, in Ausnahmefällen auch nichtamtlichen Abkürzung*, ersatzweise der *amtlichen Kurzbezeichnung* aufgeführt.
Die genaue Fundstelle und Angabe der letzten Änderung sind bei bekannteren Bundesgesetzen (die in den gängigen Gesetzessammlungen leicht zu finden sind) weggelassen worden.

AgrStatG	Gesetz über Agrarstatistiken (Agrarstatistikgesetz) in der Fassung der Bekanntmachung vom 25. Juni 1998 (BGBl. I S. 1635)
AO	Abgabenordnung
ArbSchG	Arbeitsschutzgesetz vom 7. August 1996 (BGBl. I S. 1246), zuletzt geändert durch Gesetz vom 27. Dezember 2000 (BGBl. I S. 2048)
AuslG	Gesetz über die Einreise und den Aufenthalt von Ausländern im Bundesgebiet (Ausländergesetz) vom 9. Juli 1990 (BGBl. I S. 1354, 1356), zuletzt geändert durch Gesetz vom 2. August 2000 (BGBl. I S. 1253)
BArchG	Gesetz über die Sicherung und Nutzung von Archivgut des Bundes (Bundesarchivgesetz) vom 6. Januar 1988 (BGBl. I S. 62), zuletzt geändert durch das Gesetz zur Änderung des Bundesarchivgesetzes vom 13. März 1992 (BGBl. I S. 506)
BeamtVG	Gesetz über die Versorgung der Beamten und Richter in Bund und Ländern (Beamtenversorgungsgesetz) vom 24. August 1976 (BGBl. I S. 2485, 3839), zuletzt geändert durch Gesetz vom 19. Dezember 2000 (BGBl. I S. 1786)
BDSG	Gesetz zur Fortentwicklung der Datenverarbeitung und des Datenschutzes (Bundesdatenschutzgesetz)
BGB	Bürgerliches Gesetzbuch
BRRG	Beamtenrechtsrahmengesetz
BSHG	Bundessozialhilfegesetz in der Fassung der Bekanntmachung vom 23. März 1994 (BGBl. I S. 646, ber. S. 2975), zuletzt geändert durch Art. 15 des Gesetzes vom 19. Juni 2001 (BGBl. I S. 1046)

BStatG	Gesetz über die Statistik für Bundeszwecke (Bundesstatistikgesetz) vom 22. Januar 1987 (BGBl. I S. 462, 565), zuletzt geändert durch Art. 3 des Gesetzes vom 21. Dezember 2000 (BGBl. I S. 1857)
BtBG	Gesetz über die Wahrnehmung behördlicher Aufgaben bei der Betreuung Volljähriger (Betreuungsbehördengesetz) vom 12. September 1990 (BGBl. I S. 2002, 2025), zuletzt geändert durch Art. 3 des Gesetzes vom 25. Juni 1998 (BGBl. I S. 1580)
BtG	Gesetz zur Reform des Rechts der Vormundschaft und Pflegschaft für Volljährige (Betreuungsgesetz) vom 12. September 1990 (BGBl. I S. 2002)
BtMG	Gesetz über den Verkehr mit Betäubungsmitteln (Betäubungsmittelgesetz) in der Fassung der Bekanntmachung vom 1. März 1994 (BGBl. I S. 358), zuletzt geändert durch Art. 4 des Gesetzes vom 26. Januar 1998 (BGBl. I S. 160)
BtMVV	Verordnung über das Verschreiben, die Abgabe und den Nachweis des Verbleibs von Betäubungsmitteln (Betäubungsmittel-Verschreibungsverordnung) vom 20. Januar 1998 (BGBl. I S. 74), zuletzt geändert durch Art. 23 des Gesetzes vom 19. Dezember 1998 (BGBl. I S. 3853)
BVerfGG	Bundesverfassungsgerichtsgesetz
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 Gesetzes vom 21. Dezember 2000 (BGBl. I S. 1983)
BZRG	Gesetz über das Zentralregister und das Erziehungsregister (Bundeszentralregistergesetz) in der Fassung der Bekanntmachung vom 21. September 1984 (BGBl. I S. 1229, ber. 1985 S. 195), zuletzt geändert durch Gesetzes vom 17. Dezember 1999 (BGBl. I S. 2662)
EStG	Einkommensteuergesetz
EG-Datenschutz-Richtlinie	Richtlinie 95/46/EG des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbebezogener Daten und zum freien Datenverkehr vom 24. Oktober 1995 (Abl. EG L 281 vom 23. November 1995, S. 31)

FeV	Verordnung über die Zulassung von Personen zum Straßenverkehr (Fahrerlaubnisverordnung) vom 18. August 1998 (BGBl. I S. 2214)
FlurbG	Flurbereinigungsgesetz in der Fassung der Bekanntmachung vom 16. März 1976 (BGBl. I S. 546), zuletzt geändert durch Art. 27 des Gesetzes vom 18. Juni 1997 (BGBl. I S. 1430)
FPStatG	Gesetz über die Statistik der öffentlichen Finanzen und des Personals im öffentlichen Dienst (Finanz- und Personalstatistikgesetz) in der Fassung der Bekanntmachung zur Neufassung vom 8. März 2000 (BGBl. I S. 206), zuletz geändert durch Gesetz vom 21. Dezember 2000 (BGBl. I S. 1857)
GefHundG	Gesetz zum Schutze der Bevölkerung vor gefährlichen Hunden vom 24. August 2000 (GVBl. S. 358)
GemKVO	Verordnung des SMI über die Kassenführung der Gemeinden des Freistaates Sachsen (Gemeindekassenverordnung) vom 8. Januar 1991, geändert durch Art. 2 der Verordnung zur Änderung des kommunalen Haushalts- und Kassenrechts vom 3. Dezember 1996 (GVBl. S. 498)
GemPolVO	Verordnung des Sächsischen Staatsministeriums des Innern über die Wahrnehmung polizeilicher Vollzugsaufgaben durch gemeindliche Vollzugsbedienstete vom 19. September 1991 (GVBl. S. 355)
GewO	Gewerbeordnung
GG	Grundgesetz für die Bundesrepublik Deutschland (Grundgesetz)
IfSG	Gesetz zur Verhütung und Bekämpfung von Infektionskrankheiten beim Menschen (Infektionsschutzgesetz) vom 20. Juli 2000 (BGBl. I S. 1045)
IHK-G	Gesetz zur vorläufigen Regelung des Rechts der Industrie- und Handelskammern vom 18. Dezember 1956 (BGBl. I S. 920), zuletzt geändert durch Gesetz vom 23. Juli 1998 (BGBl. I S. 1887, 3158)
InsO	Insolvenzordnung vom 5. Oktober 1994 (BGBl. I S. 2866), zuletzt geändert durch Art. 2 des Gesetzes vom 8. Dezember 1999 (BGBl. I S. 2384)

IuKDG	Gesetz zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste (Informations- und Kommunikationsdienstegesetz - IuKDG) vom 22. Juli 1997 (BGBl. I S. 1870)
JArbSchG	Gesetz zum Schutz der arbeitenden Jugend (Jugendarbeitschutzgesetz) vom 12. April 1976 (BGBl. I S. 965), zuletzt geändert durch Art. 36 des Gesetzes vom 21. Dezember 2000 (BGBl. I S. 1983)
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. 9 des Gesetzes vom 2. August 2000 (BGBl. I S. 1253)
KomWG	Gesetz über die Kommunalwahlen im Freistaat Sachsen (Kommunalwahlgesetz - KomWG) vom 18. Oktober 1993 (GVBl. S. 937), zuletzt geändert durch Gesetz vom 10. Dezember 1998 (GVBl. S. 664)
KHG	Gesetz zur wirtschaftlichen Sicherung der Krankenhäuser und zur Regelung der Krankenhauspflegesätze (Krankenhausfinanzierungsgesetz) vom 29. Juni 1972 (BGBl. I S. 1009), zuletzt geändert durch Art. 2 § 6 des Gesetzes vom 20. Juni 2000 (BGBl. I S. 1045)
LStR	Lohnsteuerrichtlinien
MDStV	Mediendienstestaatsvertrag
MRRG	Melderechtsrahmengesetz in der Fassung der Bekanntmachung vom 24. Juni 1994 (BGBl. I S. 1430)
OWiG	Gesetz über Ordnungswidrigkeiten (Ordnungswidrigkeitengesetz)
PStG	Personenstandsgesetz
SächsArchG	Sächsisches Architektengesetz vom 19. April 1994 (GVBl. S. 765), geändert durch Art. 11 des Gesetzes zur Ausführung des § 305 der Insolvenzordnung und zur Anpassung des Landesrechts an die Insolvenzordnung vom 10. Dezember 1998 (GVBl. S. 662)
SächsArchivG	Archivgesetz für den Freistaat Sachsen vom 17. Mai 1993 (GVBl. S. 449), geändert durch Art. 1 des Gesetzes zur Änderung verschiedener Vorschriften des Sächsischen Landesrechts vom 25. Juni 1999 (GVBl. S. 398)

SächsBG	Beamtengesetz für den Freistaat Sachsen in der Fassung der Bekanntmachung vom 14. Juni 1999 (GVBl. S. 370, berichtigt durch Bekanntmachung vom 16. Dezember 1999 (GVBl. 2000 S. 7)
SächsDSG	Gesetz zum Schutz der informationellen Selbstbestimmung im Freistaat Sachsen (Sächsisches Datenschutzgesetz) vom 11. Dezember 1991 (GVBl. S. 401), geändert durch Gesetz vom 7. April 1997 (GVBl. S. 350)
SächsErwStatG	Gesetz über eine repräsentative Statistik der Erwerbssituation im Freistaat Sachsen vom 12. Februar 1999 (GVBl. S. 49)
SächsFöDaG	Gesetz über Fördermitteldatenbanken im Freistaat Sachsen vom 10. Juni 1999 (GVBl. S. 273)
SächsFöDaVO	Verordnung der Sächsischen Staatsregierung über die Verarbeitung von personenbezogenenen Daten in der Landeseinheitlichen Fördermittel-Datenbank vom 13. Oktober 2000 (GVBl. S. 442)
SächsGemO	Gemeindeordnung für den Freistaat Sachsen in der Fassung der Bekanntmachung vom 14. Juni 1999 (GVBl. S. 345)
SächsHG	Gesetz über die Hochschulen im Freistaat Sachsen (Sächsisches Hochschulgesetz) vom 11. Juni 1999 (GVBl. S. 294)
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), geändert durch Art. 6 des Gesetzes vom 10. Dezember 1998 (GVBl. S. 662)
SächsIHKG	Gesetz zur Ausführung und Ergänzung des Rechts der Industrie- und Handelskammer im Freistaat Sachsen vom 18. November 1991 (GVBl. S. 380), geändert durch Art. 5 des Gesetzes zur Ausführung des § 305 der Insolvenzordnung und zur Anpassung des Landesrechts an die Insolvenzordnung vom 10. Dezember 1998 (GVBl. S. 662)
SächsKAG	Sächsisches Kommunalabgabengesetz vom 16. Juni 1993 (GVBl. S. 502), geändert durch Art. 3 des 1. Gesetzes zur Eurobedingten Änderung des sächsischen Landesrechts vom 19. Oktober 1998 (GVBl. S. 505)

SächsKHG	Gesetz zur Neuordnung des Krankenhauswesens (Sächsisches Krankenhausgesetz) vom 19. August 1993 (GVBl. S. 675), zuletzt geändert durch Art. 4 des Gesetzes zur Änderung verschiedener Vorschriften des sächsischen Landesrechts vom 25. Juni 1999 (GVBl. S. 398)
SächsKomZG	Sächsisches Gesetz über die kommunale Zusammenarbeit vom 19. August 1993 (GVBl. S. 815, berichtigt GVBl. 1993 S. 1103), zuletzt geändert durch Art. 7 des Gesetze zur Änderung verschiedener Vorschriften des Sächsischen Landesrechts vom 25. Juni 1999 (GVBl. S. 398)
SächsMG	Sächsisches Meldegesetz in der Fassung der Bekanntmachung vom 11. April 1997 (GVBl. S. 377), geändert durch Art. 4 des Gesetzes zum 4. Staatsvertrag rundfunktrechtlicher Staatsverträge vom 16. März 2000 (GVBl. S. 89)
SächsPersVG	Sächsisches Personalvertretungsgesetz in der Fassung der Bekanntmachung vom 25. Juni 1999 (GVBl. S. 430)
SächsPolG	Polizeigesetz des Freistaates Sachsen in der Fassung der Bekanntmachung vom 13. August 1999 (GVBl. S. 466)
SächsRettDG	Gesetz über Rettungsdienst, Notfallrettung und Krankentransport für den Freistaat Sachsen vom 7. Januar 1993 (GVBl. S. 9), geändert durch Art. 11 des Sächsischen Aufbaubeschleunigungsgesetzes vom 4. Juli 1994 (GVBl. S. 1261)
SächsSparkG	Sparkassengesetz des Freistaates Sachsen vom 3. Mai 1999 (GVBl. S. 190)
SächsStatG	Sächsisches Statistikgesetz vom 17. Mai 1993 (GVBl. S. 453), zuletzt geändert durch Art. 2 des Gesetzes von 12. Februar 1999 (GVBl. S. 49)
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 19. Juli 2000 (GVBl. S. 390)
SächsVerf	Verfassung des Freistaates Sachsen vom 27. Mai 1992 (GVBl. S. 243)
SächsVSG	Gesetz über den Verfassungsschutz im Freistaat Sachsen (Sächsisches Verfassungsschutzgesetz) vom 16. Oktober 1992 (GVBl. S. 459)

SächsVwVfG	Vorläufiges Verwaltungsverfahrensgesetz für den Freistaat Sachsen vom 21. Januar 1993 (GVBl. S. 74)
SächsVwZG	Verwaltungszustellungsgesetz für den Freistaat Sachsen vom 21. April 1993 (GVBl. S. 362 berichtigt in GVBl. 1995 S. 182)
SBO	Verordnung des Sächsischen Staatsministeriums für Kultus über den Besuch öffentlicher Schulen im Freistaat Sachsen (Schulbesuchsordnung) vom 12. August 1994 (GVBl. S. 1565)
SchulG	Schulgesetz für den Freistaat Sachsen vom 3. Juli 1991 (GVBl. S. 213), zuletzt geändert durch Gesetz vom 29. Juni 1998 (GVBl. S. 271)
SDÜ	Schengener Durchführungsübereinkommen
SeuchRNeuG	Gesetz zur Neuordnung seuchenrechtlicher Vorschriften (Seuchenrechts-Neuordnungsgesetz) vom 20. Juli 2000 (BGBl. I S. 1045)
SGB I	Sozialgesetzbuch - Allgemeiner Teil - vom 11. Dezember 1975 (BGBl. I S. 3015), zuletzt geändert durch Art. 2 des Gesetzes vom 19. Juni 2001 (BGBl. I S. 1046)
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 vom 19. Juni 2001 (BGBl. I S. 1046)
SGB IV	Sozialgesetzbuch - Gemeinsame Vorschriften für die Sozialversicherung - vom 23. Dezember 1976 (BGBl. I S. 3845), zuletzt geändert durch Art. 4 des Gesetzes vom 19. Juni 2001 (BGBl. I S. 1046)
SGB V	Sozialgesetzbuch - Gesetzliche Krankenversicherung - vom 20. Dezember 1988 (BGBl. I S. 2477), zuletzt geändert durch Art. 5 des Gesetzes vom 19. Juni 2001 (BGBl. I S. 1046)
SGB VI	Sozialgesetzbuch - Gesetzliche Rentenversicherung - vom 18. Dezember 1989 (BGBl. I S. 2261, ber. BGBl. 1990 I S. 1337), zuletzt geändert durch Art. 6 des Gesetzes vom 19. Juni 2001 (BGBl. I S. 1046)
SGB VIII	Sozialgesetzbuch - Kinder- und Jugendhilfe - in der Fassung der Bekanntmachung vom 8. Dezember 1998 (BGBl. I S. 3547), zuletzt geändert durch Art. 8 des Gesetzes vom 19. Juni 2001 (BGBl. I S. 1046)

SGB X	Sozialgesetzbuch - Sozialverwaltungsverfahren und Sozialdaten - in der Fassung vom 18. Januar 2001 (BGBl. I S. 130), zuletzt geändert durch Art. 9 des Gesetzes vom 19. Juni 2001 (BGBl. I S. 1046)
SigG	Signaturgesetz vom 22. Juli 1997 (BGBl. I S. 1872 Art. 3 des Gesetzes zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste (Informations- und Kommunikationsdienste-Gesetz - IuKDG)
SigV	Signaturverordnung vom 22. Oktober 1997 (BGBl. I S. 2498)
StGB	Strafgesetzbuch
StPO	Strafprozeßordnung
StVG	Straßenverkehrsgesetz
StVO	Straßenverkehrs-Ordnung
StVollzG	Gesetz über den Vollzug der Freiheitsstrafe und der freiheitsentziehenden Maßregeln der Besserung und Sicherung (Strafvollzugsgesetz) vom 16. März 1976 (BGBl. I S. 581, ber. S. 2088 und 1977 I S. 436), zuletzt geändert durch Artikel 8 des Gesetzes vom 2. August 2000 (BGBl. I S. 1253)
StVZO	Straßenverkehrs-Zulassungs-Ordnung
TDDSG	Gesetz über den Datenschutz bei Telediensten (Teledienstedatenschutzgesetz - TDDSG) vom 22. Juli 1997 (BGBl. I S. 1870)
TDSV	Telekommunikations-Datenschutzverordnung vom 18. Dezember 2000 (BGBl. I S. 1740)
TKG	Telekommunikationsgesetz vom 25. Juli 1996 (BGBl. I S. 1120), zuletzt geändert durch Art. 2 Abs. 6 des Gesetzes vom 26. August 1998 (BGBl. I S. 2521)
VwGO	Verwaltungsgerichtsordnung
VwVfG	Verwaltungsverfahrensgesetz
VwVPersAktenB	Verwaltungsvorschriften des Sächsischen Staatsministeriums des Innern über die Führung und Verwaltung von Personalakten der Beamten (Verwaltungsvorschrift Personalakten Beamte) vom 11. Dezember 1998 (SächsABl. vom 14. Januar 1999 S. 10)

VwVPersonalakten	Gemeinsame 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 7. Dezember 1996 (SächsABl. vom 6. Februar 1997 S. 145), geändert durch Verwaltungsvorschrift vom 20. Juli 1999 (SächsABl. S. 866)
ZPO	Zivilprozeßordnung

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
BayObLG	Bayerisches Oberstes Landesgericht
BayVBl.	Bayerische Verwaltungsblätter
BayVGH	Bayerischer Verwaltungsgerichtshof
BfA	Bundesanstalt für Artbeit
BfD	Der Bundesbeauftragte für den Datenschutz

BFH	Bundesfinanzhof
BND	Bundesnachrichtendienst
BGBl.	Bundesgesetzblatt
BGH	Bundesgerichtshof
BGHZ	Amtliche Sammlung der Entscheidungen des Bundesgerichtshofs in Zivilsachen
BGS	Bundesgrenzschutz
BHW	Beamtenheimstättenwerk
BKA	Bundeskriminalamt
BKK	Betriebskrankenkasse
BMF	Bundesministerium der Finanzen
BMI	Bundesministerium des Innern
BMJ	Bundesministerium der Justiz
BMFSFJ	Bundesministerium für Familie, Senioren, Frauen und Jugend
BML	Bundesministerium für Ernährung, Landwirtschaft und Forsten
BMVg	Bundesministerium für Verteidigung
BMWi	Bundesministerium für Wirtschaft und Technologie
BSGE	Bundessozialgerichtsentscheidung
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
BVVG	Bodenverwertungs- und verwaltungsgesellschaft GmbH
BZR	Bundeszentralregister
CD-ROM	Compact disc-read only memory
CR	Computer und Recht
DSMeld	Datensatz für das Meldewesen
DVB	Datei Vorkommnisbericht
DVBl	Deutsches Verwaltungsblatt
DVO	Durchführungsverordnung
ed-	erkennungsdienstlich
EG	Europäische Gemeinschaft
EGN	Einzelgesprächsnachweis
EU	Europäische Union
EWG	Europäische Wirtschaftsgemeinschaft
FTP	File transfer protocol
Gauck-Behörde	Der Bundesbeauftragte für die Unterlagen des Staatssicherheitsdienstes der ehemaligen Deutschen Demokratischen Republik
GEZ	Gebühreneinzugszentrale der öffentlich-rechtlichen Rundfunkanstalten der Bundesrepublik Deutschland
GKR	Gemeinsames Krebsregister
GMBl.	Gemeinsames Ministerialblatt, hrsg. vom Bundesministerium des Innern
GVBl.	Sächsisches Gesetz- und Verordnungsblatt
GWZ 1995	Gebäude- und Wohnungszählung 1995

HIV	human immunodeficiency virus (Aidserreger)
IKK	Innungskrankenkasse
INPOL	Polizeiliches Informationssystem des Bundes und der Länder
IM	Inoffizieller Mitarbeiter (des MfS/AfNS)
ISD	Internationaler Suchdienst Arolsen
ISDN	Integrated services digital network
JVA	Justizvollzugsanstalt
KAN	Kriminalaktennachweis
KBA	Kraftfahrtbundesamt in Flensburg
KGSt	Kommunale Gemeinschaftsstelle für Verwaltungsvereinfachung
KIN-S	Kommunales Informationsnetz - Sachsen
KPI	Kriminalpolizeiinspektion
KV	Kassenärztliche Vereinigung
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
LVA	Landesversicherungsanstalt

MDR	Mitteldeutscher Rundfunk
MedR	Medizinrecht (Zeitschrift)
MfS	Ministerium für Staatssicherheit
MPU-Stelle	Medizinisch-Psychologische Untersuchungsstelle
NJW	Neue Juristische Wochenschrift
NVwZ	Neue Zeitschrift für Verwaltungsrecht
ÖbV	Öffentlich bestellter Vermessungsingenieur
OFD	Oberfinanzdirektion
OLG	Oberlandesgericht
OVG	Oberverwaltungsgericht
PASS	Polizeiliches Auskunftssystem
PersR	Zeitschrift Personalvertretungsrecht
PIN	Personal identification number (Persönliche Identifikationsnummer)
PersV	Die Personalvertretung (Zeitschrift)
RDV	Recht der Datenverarbeitung (Zeitschrift)
RG	Reichsgericht
RGBl.	Reichsgesetzblatt
RP	Regierungspräsidium
RPA	Rechnungsprüfungsamt
SächsABl.	Sächsisches Amtsblatt
SächsJMBl.	Sächsisches Justizministerialblatt
SächsOVG	Sächsisches Oberverwaltungsgericht
SAKD	Sächsische Anstalt für Kommunale Datenverarbeitung

SLFS	Sächsisches Landesamt für Familie und Soziales
SächsVerfGH	Verfassungsgerichtshof des Freistaates Sachsen
SK	Sächsische Staatskanzlei
SLT	Sächsischer Landkreistag e. V.
SMF	Sächsisches Staatsministerium der Finanzen
SMI	Sächsisches Staatsministerium des Innern
SMJus	Sächsisches Staatsministerium der Justiz
SMK	Sächsisches Staatsministerium für Kultus
SMS	Sächsisches Staatsministerium für Soziales, Gesundheit, Jugend und Familie
SMUL	Sächsisches Staatsministerium für Umwelt und Landwirtschaft
SMWA	Sächsisches Staatsministerium für Wirtschaft und Arbeit
SMWK	Sächsisches Staatsministerium für Wissenschaft und Kunst
SSG	Sächsischer Städte- und Gemeindetag e. V.
StaLA	Statistisches Landesamt
StUFA	Staatliches Umweltfachamt
TB	Tätigkeitsbericht
TCP/IP	Transmission control protocol/Internet protocol
TdL	Tarifgemeinschaft deutscher Länder
TK-Anlage	Telekommunikationsanlage
TÜ	Telefonüberwachung
TÜV	Technischer Überwachungsverein
VG	Verwaltungsgericht
VIZ	Zeitschrift für Vermögens- und Investitionsrecht

VO	Verordnung
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

In diesem Jahr lege ich meinen Tätigkeitsbericht mit einer mehrwöchigen Verspätung vor. Dies ist auf die besondere Arbeitsbelastung meiner Behörde zurückzuführen. Wenn wir uns ansehen, wie stark die Ausgaben der öffentlichen Hand für Hard- und Software in der automatischen Datenverarbeitung gestiegen sind und wenn wir uns vergegenwärtigen, dass jede Behörde, ja fast jeder Mitarbeiter im öffentlichen Dienst im Freistaat Sachsen von morgens bis abends personenbezogene Daten verarbeitet, dann wird deutlich, dass meine 18 Mitarbeiter und ich nicht dazu in der Lage sind, die ca. 250.000 Bediensteten in der Staatsverwaltung, in der Kommunalverwaltung, in der Hochschulverwaltung und in den Kammern und Stiftungen umfassend und effizient zu beraten und zu kontrollieren. Mit anderen Worten: Die Arbeit wächst uns über den Kopf. Ich werde deshalb in nächster Zeit bei den zuständigen Stellen darum bitten, dass meine Personalausstattung angemessen angehoben wird.

Aber nicht nur diese steigende Arbeitsbelastung, sondern auch gravierende und leichtfertige Verstöße gegen datenschutzrechtliche Vorschriften haben unsere Arbeitskraft gebunden und uns nicht selten Kopfzerbrechen bereitet. Um so nachdrücklicher bedanke ich mich beim Präsidenten des Landtags und bei seiner Verwaltung, die uns nach wie vor in unserer Arbeit unterstützen und in wichtigen Dingen den Rücken freihalten, und vor allem bei den Mitarbeitern meiner Behörde für ihren unermüdlichen und sachbezogenen Einsatz.

Ich kann in diesem Jahr - auch beim besten Willen und trotz des erfolgreichen Bemühens vieler Behörden, in Datenschutzfragen sensibel zu agieren - insgesamt keine gute Bilanz ziehen: Denn im Berichtszeitraum, also vom 1. April 2000 bis zum 31. März 2001 hat die Staatsregierung überraschend klar zum Ausdruck gebracht, dass ihr die Anliegen, die ich zu vertreten habe, zweitrangig erscheinen:

In meiner gesamten Amtszeit und auch schon als Aufstellungsstab Datenschutz, also in der Zeit ab Frühjahr 1991, habe ich gravierende datenschutzrechtliche Verstöße beanstandet und diese Beanstandungen mit dem zugrunde liegenden Sachverhalt öffentlich gemacht. Insbesondere dann, wenn Spitzen der Verwaltung im Einzelfall nachhaltig und manchmal unbelehrbar mit personenbezogenen Daten rechtswidrig umgegangen waren, musste ich auch deren Verhalten im Einzelnen öffentlich darstellen und beleuchten. Eine effektive Datenschutzkontrolle ist nur dann gewährleistet, wenn gerade die Verantwortlichen an exponierter Stelle nicht nur ein Gefühl für das Persönlichkeitsrecht und den besonderen Stellenwert des Rechts auf informationelle Selbstbestimmung entwickeln, sondern, dass sie sich auch dann an die dazu verbindlichen Rechtsregeln halten, wenn sie meinen, die politische Konstellation würde ihr - durch Gesetz nicht gedecktes Verhalten - rechtfertigen. Hier muss ein Datenschutzbeauftragter unabhängig und unerschrocken tätig werden und den Finger in die Wunde legen. Dies gilt immer dann, wenn es sich um strukturelle Fehlhaltungen oder um gravierende Persönlichkeitsrechtsverletzungen handelt. Die Öffentlichkeitswirksamkeit der Beanstandungen hat meinem Amt eine - wie ich feststellen darf - angemessene Reputation gesichert und sicherlich auch manchen Datenschutzverstoß verhindert, der ohne die Existenz meiner Behörde geschehen wäre.

Als merkwürdige, aber in gewisser Weise verständliche Reaktion empfinde ich es, dass gegen mich persönlich ein staatsanwaltschaftliches Ermittlungsverfahren - auf Weisung von oben - eingeleitet wurde und es mir zum Vorwurf gemacht wird, dass ich den Vorgang einer rechtswidrigen Verarbeitung personenbezogener Daten durch den damaligen Justizminister öffentlich gemacht und beanstandet habe. Das Konstrukt, dadurch sei ein „Geheimnis verraten“ und dem Freistaat Sachsen „ein Schaden zugefügt“ worden, wird in sich zusammenfallen. Ich sehe darin den untauglichen Versuch, mit den letzten zu Gebote stehenden Mitteln die Unabhängigkeit des Datenschutzbeauftragten und seine Arbeit zu diskreditieren.

Ich habe - selbstverständlich - die Tätigkeit der Justiz als Rechtsunterworfener hinzunehmen. Ich kündige aber an, dass ich diese Grundsatzfrage nötigenfalls zum Gegenstand einer letztverbindlichen Entscheidung machen werde. Wo kommen wir hin, wenn der Datenschutzbeauftragte Mängel feststellt und dann verpflichtet ist, über sie zu schweigen? Dies widerspricht dem Geist einer lebendigen, nicht nur formalen Demokratie, zu der eben auch die öffentliche Kontrolle der Machtausübung gehört.

Am gleichen Tag, als mich die Nachricht von der Anklage erreichte, wurde mir auch ein Referentenentwurf zur Anpassung des Sächsischen Datenschutzgesetzes an die EG-Datenschutzrichtlinie 1995 zugestellt. Dieses vom Kabinett verabschiedete und zur Anhörung freigegebene Gesetzesvorhaben ist mit tragenden Grundsätzen des Datenschutzrechts nicht zu vereinbaren. Ich habe deshalb unverzüglich dem damaligen Chef der Staatskanzlei meine Auffassung in dem nachstehend abgedruckten Schreiben zum Ausdruck gebracht.

„Sehr geehrter Herr Staatsminister,

am 2. Januar 2001 wurde mir ein Referentenentwurf zur Neufassung des Sächsischen Datenschutzgesetzes zugeleitet, der vom sächsischen Kabinett mit Beschluss vom 20. Dezember 2000 zur Anhörung freigegeben worden sei. Gemeinsam mit dem Sächsischen Städte- und Gemeindetag e. V., dem Sächsischen Landkreistag und anderen Stellen habe ich Gelegenheit zur Abgabe einer Stellungnahme bis zum 28. Februar 2001.

§ 13 Abs. 5 Satz 4 der Geschäftsordnung der Sächsischen Staatsregierung schreibt vor, dass meine Behörde vor einer ersten Vorlage an die Staatsregierung offiziell zu beteiligen ist, soweit der Umgang mit personenbezogenen Daten berührt wird. Diese Beteiligung hat in dem Verfahrensstadium stattzufinden, in dem die Mitzeichnung des Ressorts erfolgt; sie ist von der späteren Beteiligung Außenstehender i. S. d. § 13 Abs. 7 GeschOSReg zu unterscheiden. Dies setzt voraus, dass mir der ‘letzte Stand der Dinge’ zur Kenntnis und Stellungnahme gegeben wird. Ausweislich des beigefügten Schriftwechsels fand zuletzt am 13. Februar 1998 ein Kontakt zwischen dem SMI und meiner Behörde statt. Der damalige Entwurf entsprach aber in den nachstehenden wesentlichen Punkten nicht dem nun vorgelegten Inhalt. Die gebotene Beteiligung hat folglich nicht stattgefunden.
Ich muss darauf bestehen, dass die Geschäftsordnung der Sächsischen Staatsregierung eingehalten wird, weil meine Beteiligungsrechte davon berührt werden.

Ein erster Blick auf den nunmehr zugesandten Entwurf zeigt, wie wichtig die Einhaltung dieser Verfahrensvorschrift gewesen wäre:

1. Es darf in der Verwaltung des Freistaats Sachsen keine datenschutz-kontrollfreien Räume geben.
2. Der Datenschutzbeauftragte hat „völlig unabhängig“ zu sein.
3. Der Datenschutzbeauftragte muss mit „wirksamen Einwirkungsbefugnissen“ arbeiten.
4. Die Datenschutzkontrolle im privaten Bereich muss „in völliger Unabhängigkeit“ tätig sein.
5. Die Datenschutzkontrolle hat grundsätzlich anlassfrei stattzufinden.
6. Die materiellen Vorschriften der EG-Datenschutzrichtlinie sind - soweit der EG-Vertrag einschlägig ist - im Freistaat Sachsen durch das Sächsische Datenschutzgesetz zu garantieren.

In allen vorgenannten Punkten ist die Staatsregierung mit diesem Entwurf in der Gefahr, aus verfassungsrechtlichen Gründen und wegen des übergeordneten europäischen Rechts „vor den Baum zu laufen“. Ich schreibe Ihnen diese offenen Worte, um Ihnen deutlich zu machen, dass ich mit Ihnen gemeinsam nach allen Wegen und Mitteln suchen möchte, dem Freistaat Sachsen eine derartige Blamage zu ersparen.

Meine Arbeiten an einer Stellungnahme habe ich zunächst - in Erwartung Ihrer Antwort - bis zum 18. Januar zurückgestellt.

Mit freundlichen Grüßen“

Ich bin sicher, dass - sollte die Staatsregierung ihre Bemühungen um eine Verschlechterung des Datenschutzniveaus fortsetzen - das Verfassungsgericht des Freistaates Sachsen so wie bisher die Fahne des Rechts hochhalten wird.

Natürlich haben diese Aktionen die bundesweite Reputation des Freistaates Sachsen nicht gerade gestärkt. Deutlich genug fiel deshalb auch die einstimmige Entschließung der Datenschutzbeauftragten des Bundes und der Länder aus, die - beispiellos - wie folgt lautet:

> *„Die Datenschutzbeauftragten des Bundes und der Länder sind verpflichtet, Einzelne – wie es die Rechtsprechung des Bundesverfassungsgerichts und die Richtlinie der Europäischen Gemeinschaft zum Datenschutz von 1995 vorsehen – vor rechtswidrigem Umgang mit ihren personenbezogenen Daten wirksam zu schützen. Die damit verbundenen Beratungs- und Kontrollaufgaben verleihen den Datenschutzbeauftragten ein öffentliches Wächteramt, das die Befugnis einschließt, Behördenverhalten auch im Detail und, soweit der Bedeutung der Sache angemessen, auch unter Bezeichnung der Amtsträgerinnen und Amtsträger öffentlich zu rügen.*
>
> *Aus gegebenem Anlass wendet sich die Konferenz der Datenschutzbeauftragten des Bundes und der Länder energisch gegen Versuche im*

Land Sachsen, durch gesetzgeberische Maßnahmen dieses Recht zu beschneiden und die Arbeit des Sächsischen Datenschutzbeauftragten zu behindern.“

2 Parlament

In diesem Jahr nicht belegt.

3 Europäische Union / Europäische Gemeinschaft

In diesem Jahr nicht belegt.

4 Medien

In diesem Jahr nicht belegt.

5 Inneres

5.1 Personalwesen

5.1.1 Zulässigkeit der Weitergabe von Informationen aus der Personalakte eines ehemaligen Beamten an die Rechtsaufsichtsbehörde (Stasi-Belastung)

Ein Polizeipräsidium fragte, ob Informationen aus der Personalakte eines wegen MfS-Mitarbeit entlassenen Polizeibeamten, der jetzt Bürgermeister einer sächsischen Gemeinde sei, an die Rechtsaufsichtsbehörde weitergegeben werden dürfen.

Ich habe dem Polizeipräsidium mitgeteilt, dass nach § 121 Abs. 2 SächsBG Auskünfte aus der Personalakte an Dritte nur mit Einwilligung des (ehemaligen) Beamten erteilt werden dürfen, es sei denn, dass die Abwehr einer erheblichen Beeinträchtigung des Gemeinwohls die Auskunftserteilung zwingend erfordert.

Eine erhebliche Beeinträchtigung des Gemeinwohls ist stets anzunehmen, wenn sich eine Person, die gegen die Grundsätze der Menschlichkeit oder Rechtsstaatlichkeit verstoßen hat oder für das frühere Ministerium für Staatssicherheit/ Amt für nationale Sicherheit der DDR tätig war, bisher unerkannt in einem öffentlich-rechtlichen Dienst- und Treueverhältnis - z. B. als kommunaler Wahlbeamter - befindet (siehe Art. 118 SächsVerf). Denn nach der Rechtsprechung der obersten Gerichte ist das Gemeinwohl u. a. dann gefährdet, wenn Grundsätze der Verfassung unbeachtet bleiben. Der sächsische Verfassungsgeber, also das erste frei gewählte Parlament in Sachsen nach dem Zusammenbruch der DDR, hat großen Wert darauf gelegt, dass Mitarbeiter der Stasi kein Unterkommen im öffentlichen Dienst finden. Dies ist in Sachsen ein Verfassungsgrundsatz.

Um der zuständigen Kommunalaufsichtsbehörde die Prüfung zu ermöglichen, ob der Betroffene kommunaler Wahlbeamter bleiben darf und/oder ob Maßnahmen i. S. v. § 45 Abs. 2 KomWG zu ergreifen sind, halte ich die hierzu erforderlichen Auskünfte aus der Personalakte für zulässig. Allerdings sind dem Betroffenen gemäß § 121 Abs. 2 Satz 2 SächsBG Inhalt und Empfänger der Auskunft schriftlich mitzuteilen (Rechtsweggarantie des Art. 19 Abs. 4 GG).

5.1.2 Einsichtnahme in Personalakten nach Beendigung des Beschäftigungsverhältnisses

Der Personaldezernent einer sächsischen Universität verweigerte einem ehemaligen Beschäftigten die Einsichtnahme in seine Personalakte.

Unter Hinweis auf § 17 Abs. 3 SächsDSG und auf 3/5.1.17 konnte ich den Personaldezernenten überzeugen, dass der Betroffene einen Anspruch auf Einsichtnahme in seine Personalakte - auch nach Ausscheiden - hat. Der Petent wurde entsprechend informiert.

5.1.3 Schülerpraktika an sächsischen Gerichten

Ein Gericht fragte, ob Schüler dort ein Betriebspraktikum unter folgenden Voraussetzungen absolvieren könnten:

1. Sie werden gemäß § 6 SächsDSG auf das Datengeheimnis verpflichtet.
2. Es erfolgt eine Belehrung über ihre Obliegenheiten nach dem Verpflichtungsgesetz.
3. Sie erhalten nur Einsicht in die für die jeweilige Praktikumsarbeit erforderlichen Unterlagen mit personenbezogenen Daten.
4. Mit Fällen besonders sensiblen Inhalts (z. B. Gewaltverbrechen) werden sie nicht befasst.
5. Es wird sichergestellt, dass sie sich nicht unbeaufsichtigt in der Registratur oder Geschäftsstelle aufhalten.

Die von dem Gericht beabsichtigten Maßnahmen betrachte ich als angemessen und geeignet und befürworte insoweit die Durchführung von Schülerpraktika an sächsischen Gerichten ausdrücklich. Als ergänzende Maßnahme habe ich angeregt, bei der Vergabe von Praktikumsplätzen darauf zu achten, dass ein Schüler möglichst nicht bei einem Gericht eingesetzt wird, in dessen Zuständigkeitsbereich er wohnt.

5.1.4 Zum Austausch von Personalbogen

Kein Verständnis hatte ich für das Anliegen eines Personalrats, der sich dagegen wandte, dass die alten, zum Teil noch aus DDR-Zeiten stammenden sowie die in neuerer Zeit verwendeten, jedoch nicht datenschutzgerechten Personalbogen ausgetauscht und in einem verschlossenen Umschlag zur Personalakte genommen werden sollten.

Es ist nicht nur das Recht, sondern die Pflicht einer öffentlichen Stelle, solche Personalbogen auszutauschen. Wenn die Beschäftigten im Zuge der Austauschaktion gebeten werden, einen neuen Personalbogen auszufüllen, so ist die damit verbundene Datenerhebung im Sinne von § 31 Abs. 1 SächsDSG erforderlich und somit zulässig. Die Befugnis zu dieser Maßnahme hat der Dienstherr bzw. Arbeitgeber aufgrund seines Organisationsrechts.

Warum aber darf der alte Personalbogen nicht an den Beschäftigten zurückgegeben oder vernichtet werden?

Personalakten haben vollständig zu sein, d. h., dass Unterlagen nur unter den Voraussetzungen des § 122 SächsBG daraus entfernt werden dürfen. Die Grundsätze dieser beamtenrechtlichen Vorschrift gelten, da sie aus der einschlägigen Rechtsprechung entwickelt wurden, für die Personalakten von Arbeitern und Angestellten entsprechend (siehe VwV Personalakten vom 20. Juli 1999 und VwV PersAktenB vom 11. Dezember 1998). Das Schwärzen einzelner Daten in Unterlagen mit Personalaktenqualität (Urkunden) scheidet generell aus.
Datenschutzgerecht ist es, die überholten Personalbogen in einem verschlossenen, entsprechend gekennzeichneten Umschlag bei der jeweiligen Personalakte - oder auch gesondert, so z. B. wie die Unterlagen des BStU - aufzubewahren.

5.1.5 Eine Ergänzung: Aufbewahrung und Löschung von Unterlagen über erfolglose Bewerbungen

Ein kritischer Leser meines Tätigkeitsberichts hat mich darauf aufmerksam gemacht, dass ich in 8/5.1.12 nur die Aufbewahrung und Löschung von Unterlagen über erfolglose Bewerbungen auf eine *Beamtenstelle* behandelt habe. Er fragte, ob die Daten von Bewerbern, die sich erfolglos um eine *Angestellten- oder Arbeiterstelle* im öffentlichen Dienst bemüht hätten, früher gelöscht werden könnten; denn in diesen Fällen hätte das Ablehnungsschreiben nicht die Qualität eines Verwaltungsakts. Deshalb komme auch die Rechtsbehelfsfrist nach § 58 VwGO nicht in Betracht. Dem

abgelehnten Bewerber sei - so Rechtsprechung und Literatur - lediglich eine angemessene Frist einzuräumen, in der er um vorläufigen Rechtsschutz beim Arbeitsgericht nachsuchen könne. Die Auffassungen zu dieser Frist schwankten zwischen zwei Wochen und einem Monat.

Den Hinweis habe ich dankbar aufgenommen und mich wie folgt geäußert:

Gemäß § 31 Abs. 4 Satz 1 SächsDSG sind die vor Beginn eines Dienst- oder Arbeitsverhältnisses erhobenen Daten unverzüglich zu löschen, sobald feststeht, dass ein Dienst- oder Arbeitsverhältnis nicht zustande kommt. Nach Satz 2 dieser Vorschrift ist jedoch von der Löschung abzusehen, wenn Grund zu der Annahme besteht, dass dadurch schutzwürdige Belange des Betroffenen beeinträchtigt werden. Solche schutzwürdigen Belange können vielfältiger Natur sein und sind von vornherein nicht absehbar. Beispiele wären Schadensersatzansprüche oder das Recht des Bewerbers auf Auskunft, wenn ihn ein Ablehnungsschreiben (aus welchen Gründen auch immer) nicht erreicht hat. Vorstellbar ist auch, dass die Rückgabe von Unterlagen verlangt wird, weil sie (versehentlich) nicht oder nicht vollständig zurückgesandt oder mit den Unterlagen eines anderen Bewerbers vertauscht wurden.

Würden die Bewerberdaten bereits einen Monat nach dem Ablehnungsschreiben gelöscht, wäre schon nach kurzer Frist gar nicht mehr festzustellen, ob überhaupt eine Bewerbung eingegangen ist. Deshalb sollten die Unterlagen zur Wahrung der schutzwürdigen Belange vorsorglich für eine gewisse Zeit aufbewahrt werden. Angemessen erscheint mir auch hier eine Frist von 13 Monaten, ausgehend vom Datum des Ablehnungsschreibens.

5.1.6 Vorgesetztenbeurteilung

Der Datenschutzbeauftragte einer Stadtverwaltung fragte, ob eine Spezialfirma mit der Organisation und Durchführung von Vorgesetztenbeurteilungen auf freiwilliger Basis bei zugesicherter Anonymität beauftragt werden dürfe.
So wie ich das Angebot der Firma verstand, dient die Vorgesetztenbeurteilung Zwekken, die gemäß § 31 Abs. 1 SächsDSG zum Aufgabenbereich der Dienststelle gehören (hier z. B. Personalentwicklungskonzept). Soll die Aufgabe auf einen privaten Dritten übertragen werden, gilt es § 31 Abs. 2 SächsDSG mit der Maßgabe zu beachten, dass für personenbezogene Datenübermittlungen an das Unternehmen neben der Freiwilligkeit an der Teilnahme, auch eine „informierte“ Einwilligung zur Datenübermittlung und weiteren Datenverarbeitung (Auswertung mit anschließenden Beratungsgesprächen durch Firmenpersonal) erforderlich ist.

Die von dem Unternehmen zugesicherte Anonymität kann in Bezug auf die zu beurteilenden Vorgesetzten jedenfalls nicht gewährleistet werden. Dies gilt insbesondere im Hinblick auf das „Vorgesetzten-Feedback“, auf die Erörterung des Ergebnisses mit den beurteilenden Mitarbeitern und schließlich auf die zu erwartenden Beratungsgespräche mit Weiterbildungsangeboten durch das Unternehmen. Eine Behörde ist deshalb gut beraten, sich eine vertragliche Bindung an Unternehmen dieser Art gut

zu überlegen. Wenn man sich jedoch zu einem Vertragsabschluss entschließt, sollten zumindest die aus Nr. 7 meiner Bekanntmachung vom 3. November 1993 (siehe Nr. 16.1.4 meines 2. Tätigkeitsberichts) beachtet werden (auch wenn es sich bei der Übertragung der behördlichen Aufgabe auf eine Privatfirma nicht um Datenverarbeitung i. S. v. § 7 SächsDSG handelt).

5.1.7 Verfahren bei Gehaltspfändungen im LfF

Wie in 8/5.1.9 angekündigt, habe ich die Verhandlungen mit dem SMF fortgesetzt und konnte einen akzeptablen Kompromiss, der überflüssige Datenübermittlungen vermeidet, erreichen.

So wird das LfF per Erlass des SMF u. a. angewiesen, die personalverwaltende Stelle erst dann von einem Pfändungs- und Überweisungsbeschluss zu unterrichten, wenn die zugrundliegende Forderung einen Betrag von über 1.000,- DM (511 Euro) überschreitet oder wenn innerhalb eines Jahres mehr als ein Pfändungsbeschluss eingegangen ist. Bisher erfolgte in jedem Fall eines Pfändungsbeschlusses (unabhängig von der Höhe der Forderung) eine Unterrichtung der personalverwaltenden Stelle.

Aus datenschutzrechtlicher Sicht habe ich darauf hingewiesen, dass das LfF auch die erforderlichen Maßnahmen zur Gewährleistung des Datenschutzes (hier insbesondere § 9 Abs. 2 Nrn. 2 und 9 SächsDSG) zu beachten hat, nämlich dass die Mitteilungen als „vertrauliche Personalsache“ ausschließlich in *verschlossenem Umschlag* an die Personalstellen und die Betroffenen (diese erhalten Durchschrift der Mitteilung) zu versenden sind.

5.1.8 Teilnehmereinschätzung im Rahmen der Fortbildung

Eine erneute Erörterung mit dem SMF im August 2000 sowie nachstehende Äußerung der Staatsregierung zu 8/5.1.10 ließen auf eine baldige Erledigung hoffen:

„*Im Ergebnis prüft das Sächsische Staatsministerium der Finanzen vor dem Hintergrund, dass die betroffene weiterführende Fortbildung in den Finanzämtern qualitativ auf sehr hohem Niveau und ausschließlich funktionsbezogen erfolgt, ob die Ausstellung von qualifizierten Teilnehmernachweisen noch weiterhin erforderlich ist.*“

Zur Vermeidung einer denkbaren Ungleichbehandlung gegenüber den Bediensteten anderer Ressorts und sonstiger Behörden (z. B. außersächsischer Dienstherrn, Kommunen), die die Differenzierung „*hat mit Erfolg teilgenommen*“ und „*hat teilgenommen*“ (also ohne Erfolg) nicht kennen, habe ich eine baldige Entscheidung angeraten. Kurz vor Redaktionsschluss erfuhr ich allerdings, dass auf die vom SMF praktizierte Teilnehmereinschätzung nicht verzichtet, sondern die Verfahrensweise vielmehr „aus Gründen der Gleichbehandlung“ auch von den anderen Ressorts übernommen werden soll. Dass die Chancen, in den sächsischen Staatsdienst übernommen zu werden, für Bewerber aus den anderen Bundesländern oder aus dem Kommunalbereich, wo man

solche Differenzierungen nicht kennt, nicht unbedingt steigen, wird nach wie vor wohl nicht bedacht. Enthält nämlich die Personalakte eines solchen Bewerbers in Sachen Fortbildung nur Bescheinigungen mit dem Vermerk „*hat teilgenommen*“, wird man den Bewerber, dessen Fortbildungsbescheinigungen „*hat mit Erfolg teilgenommen*“ aufweisen, den Vorzug geben. Denkbare „Konkurrentenklagen“ werden zeigen, ob die sächsische Verfahrensweise Bestand hat.

Meiner Meinung nach sollte auf eine - für den Außenstehenden in ihrer Bedeutung nicht erkennbare - Differenzierung, ob der Bedienstete ohne Zusatz oder mit Erfolg an einer Fortbildung teilgenommen hat, verzichtet werden. Wenn jemand einer Fortbildung nicht aktiv und mit vollem geistigem Einsatz folgt, so kann das vom Ausbilder im Einzelfall der Beschäftigungsbehörde gemeldet und dann - nach Anhörung des Betroffenen - zu dessen Personalakten genommen werden. Das ist effektiver und vermeidet Begriffsverwirrung.

5.1.9 Belehrung aller Lehrkräfte gemäß §§ 34, 35 Infektionsschutzgesetz

Nach § 35 IfSG sind u. a. Lehrer vor erstmaliger Aufnahme ihrer Tätigkeit und im Weiteren mindestens im Abstand von zwei Jahren von ihrem Arbeitgeber (Dienstherrn) über die gesundheitlichen Anforderungen an Lehrpersonen und ihre Mitwirkungspflichten für den Fall, dass sie an einer Infektionskrankheit leiden, zu belehren. Über die Belehrung ist ein Protokoll zu erstellen, das beim Arbeitgeber (Dienstherrn) für die Dauer von drei Jahren aufzubewahren ist.

Ein Regionalschulamt beabsichtigte, von allen Lehrern seines Zuständigkeitsbereichs folgenden „Belehrungs“-Bogen ausfüllen zu lassen:

Belehrung über gesundheitliche Anforderungen und Mitwirkungspflichten als Lehrer im Schuldienst des Freistaates Sachsen gemäß §§ 34, 35 Seuchenrechtsneuordnungsgesetz
(richtig muss es heißen: Infektionsschutzgesetz)

Hiermit erkläre ich, dass ich über die gesundheitlichen Anforderungen und meine Mitwirkungspflichten gemäß §§ 34, 35 SeuchRNeuG als Lehrer im Schuldienst des Freistaates Sachsen belehrt worden bin.
Sofern eine der in § 34 Abs. 1 bis 3 SeuchRNeuG genannten Krankheiten bei mir auftritt, werde ich meinen Arbeitgeber hiervon unverzüglich informieren.

Ort *Unterschrift*

Ich habe dem Regionalschulamt mitgeteilt, dass das mir vom Personalrat übersandte „Belehrungs“-Formular in verschiedener Hinsicht mit § 35 IfSG nicht zu vereinbaren ist.

Nach § 35 IfSG hat der Arbeitgeber/Dienstherr unter den dort genannten Voraussetzungen über die gesundheitlichen Anforderungen und Mitwirkungspflichten nach § 34 IfSG zu *belehren*.

Das vom Regionalschulamt Dresden verwendete Formular enthält zwar in der Überschrift das Wort „Belehrung“, ist aber tatsächlich ein *Erklärungs- und Verpflichtungsbogen* der Betroffenen.

„Belehren“ bedeutet ein aktives Tätigwerden des Arbeitgebers/Dienstherrn, also eine Aufklärung der Betroffenen über den Inhalt des § 34 IfSG und die daraus resultierenden Mitteilungspflichten. Für Selbsterklärungen und Selbstverpflichtungen lässt § 35 IfSG keinen Raum. Diese ersetzen nämlich nicht die weitere Verpflichtung des Arbeitgebers/Dienstherrn, über seine Belehrungen ein Protokoll zu erstellen, also eine Niederschrift über den Ablauf und den Inhalt der Belehrung.

Beispielsweise könnte ein solches Protokoll wie folgt aussehen:

„*Herr/Frau ... wurde am ... darüber belehrt, dass bei Auftreten einer der in § 34 Abs. 1 bis 3 IfSG genannten Krankheiten nach § 34 Abs. 5 IfSG die Verpflichtung besteht, den Arbeitgeber/Dienstherrn (hier genaue Bezeichnung der verantwortlichen Stelle) unverzüglich zu unterrichten. Ihr/ihm wurde der Text der §§ 33 bis 35 IfSG ausgehändigt.*“

Dieses Protokoll wäre von dem Belehrenden und der/dem Belehrten zu unterschreiben.

Das Regionalschulamt wurde aufgefordert, die rechtswidrige Aktion unverzüglich zu stoppen und bereits abgegebene Erklärungen unverzüglich zu vernichten. Eine entsprechende Zusage habe ich - allerdings erst nach Ankündigung einer förmlichen Beanstandung gemäß § 26 SächsDSG - inzwischen erhalten.

Da nicht auszuschließen ist, dass in den anderen Regionalschulämtern ebenso verfahren wird, habe ich auch das SMK gebeten, dort vorsorglich auf eine rechtmäßige Verfahrensweise hinzuweisen. Dies soll nach Aussage des SMK im Erlasswege erfolgen.
Bezüglich der Aufbewahrung der Belehrungsprotokolle habe ich folgende Verfahrensweise empfohlen:

Die Belehrungsprotokolle werden für die Dauer von drei Jahren (§ 35 IfSG) in *einer* Personal*teil*akte, die beim Regionalschulamt geführt wird, gesammelt. In den Personalgrundakten ist gemäß A I.1 letzter Satz VwVPersAktenB, die lt. VwVPersonalakten auch für Arbeitnehmer gilt, ein Hinweis auf die Existenz dieser Teilakte aufzunehmen. Diese Verfahrensweise wurde mit dem für das Personalaktenrecht federführenden SMI abgesprochen und gewährleistet eine unbürokratische Überwachung der Dreijahresfrist.

5.1.10 Der Arbeitsschutz und die Gefährdungsanalyse im Geschäftsbereich des SMI

Das Arbeitsschutzgesetz verpflichtet den Arbeitgeber, die für die Beschäftigten mit ihrer Arbeit verbundene Gefährdung zu ermitteln und geeignete Gegenmaßnahmen zu treffen (§ 5 Abs. 1 ArbSchG). Das Ergebnis einer solchen Gefährdungsanalyse ist

zu dokumentieren (§ 6 ArbSchG). Dabei hält das Gesetz bei gleichartigen Arbeitsbedingungen die Beurteilung *eines* Arbeitsplatzes oder *einer* Tätigkeit für ausreichend. Das SMI wollte es genau wissen und hat zu diesem Zweck gleich eine Arbeitsschutzsoftware für den gesamten Geschäftsbereich entwickelt, mit der die individuellen Arbeitsbedingungen *aller* Mitarbeiter erfasst und ausgewertet werden können.

Kern der Software sind Fragebogen zu den verschiedenen Arbeitsbereichen, die von den Beschäftigten am PC ausgefüllt und per E-Mail zur Auswertung an die Fachkraft für Arbeitssicherheit gesandt werden.

Von den ca. 40 (!) verschiedenen Fragebogen habe ich mich mit den für die ca. 2000 Bildschirmarbeitsplätze sowie die Schreinerei-Mitarbeiter, Polizeitaucher, Lagerarbeiter und Kraftfahrer vorgesehenen Bogen eingehender beschäftigt.

Abgesehen davon, dass ein automatisiertes Verfahren in der praktischen Durchführung bei Schreinerei-Mitarbeitern, Polizeitauchern, Lagerarbeitern und Kraftfahrern problematisch sein dürfte (ihre Arbeitsplätze sind üblicherweise nicht mit einem PC ausgestattet), habe ich die für sie vorgesehenen Fragebogen kurz gesagt als „unbrauchbar“ bewertet und eine grundlegende Überarbeitung angeregt.

Bei dem Fragebogen für die Bildschirmarbeitsplätze habe ich vor allem die Erhebung so genannter „mentaler Daten“ kritisiert, z. B. folgende Fragen, die mit „ja“ oder „nein“ zu beantworten sind:

- Meine Arbeit erfordert neben der reinen Ausführung auch eigenständige Planung, Koordination und Prüfung von Arbeitsschritten.
- Bei meiner Arbeit wechseln anspruchsvolle Aufgaben mit Routineaufgaben ab.
- Meine beruflichen Kenntnisse und Erfahrungen kann ich in die Arbeit einbringen.
- Ich erhalte ausreichende Rückmeldungen über Arbeitsschritte und Arbeitsergebnisse.
- Die mir übertragenen Aufgaben sind überschaubar und widerspruchsfrei.
- Bei meiner Arbeit muss ich Entscheidungen treffen, die den eigenen Arbeitsfortschritt oder die Arbeit von Kollegen betreffen.

Solche Fragen sind nach meinem Dafürhalten zur Feststellung der Gefährdung an Bildschirmarbeitsplätzen weder geeignet noch erforderlich. Das Argument des SMI, wonach Arbeit krank mache, wenn ein Mitarbeiter unter der Art seiner Aufgabe oder dem Betriebsklima leide, vermag ich zwar nachzuvollziehen, in diesem Zusammenhang überzeugt es mich jedoch nicht von der Erforderlichkeit. Es kann nicht Aufgabe einer Fachkraft für Arbeitssicherheit sein, sich aufgrund einer stichtagsbezogenen, alle zwei Jahre stattfindenden Untersuchung von Bildschirmarbeitsplätzen mit dem mentalen Wohlbefinden von Beschäftigten zu befassen. Schon das Verhältnis von 1:2000 erscheint absurd. Und sollen sich tatsächlich auch Referatsleiter und Abteilungsleiter gegenüber der Fachkraft zu den o. g. Fragen äußern?

Mal im Ernst: Wo liegt eigentlich die Gefährdung eines „mental beeinträchtigten“ Beschäftigten mit einem objektiv sicheren Bildschirmarbeitsplatz - flimmerfreier

Bildschirm, optimale Luft- und Lichtverhältnisse, standsicherer Stuhl etc.? Aus meiner Sicht dürfte sie sich allenfalls in unzureichenden Arbeitsergebnissen niederschlagen. Folglich sind solche Probleme nicht über die Arbeitsplatzsicherheit, sondern über die Fachvorgesetzten herauszufinden und zu lösen.

Das SMI zeigte keine Bereitschaft zur Streichung dieser Fragen. Da kein Konsens zu erzielen war, haben wir uns schließlich darauf verständigt, dass ich mir in ca. einem Jahr die Ergebnisse der Arbeitsplatzuntersuchung ansehe, insbesondere welche Konsequenzen aus „mentalen Daten“ gezogen wurden. Das Resultat dürfte die Erforderlichkeit für die Praxis überzeugend belegen oder widerlegen.

5.1.11 „Büromaterialbeschaffung Online“

Das SMI beabsichtigt die Büromaterialbeschaffung in einem Onlineverfahren so zu gestalten, dass die Mitarbeiter ihre Bestellung vom Bildschirmarbeitsplatz an eine interne „Einkaufszentrale“ übermitteln. Diese leitet die Bestellung per E-Mail an die private Lieferfirma weiter, die sodann das Material direkt an den Arbeitsplatz liefert (Prinzip: Pizza-Express).

Ein solches Verfahren ist nur mit personenbezogenen Beschäftigtendaten möglich, wobei sowohl in der „Einkaufszentrale“ als auch bei den Lieferanten bekannt wird, wer wann was an welchen Arbeitsplatz bestellt hat.

Dem SMI habe ich zu bedenken gegeben, dass eine Übermittlung von Beschäftigtendaten an Stellen außerhalb des öffentlichen Bereichs (hier an die Lieferanten) grundsätzlich nur auf gesetzlicher Grundlage oder mit Einwilligung der Betroffenen zulässig ist (§ 31 Abs. 2 SächsDSG). Außerdem ist der Sächsische Datenschutzbeauftragte gemäß § 31 Abs. 7 SächsDSG bereits vor der Einführung eines solchen Verfahrens zu beteiligen, was unterblieben war. Ohne meine Beteiligung und ohne Schaffung der aus § 31 Abs. 2 SächsDSG resultierenden Voraussetzungen ist das Verfahren, das m. E. auch der Mitbestimmung nach § 80 Abs. 3 Nr. 16 SächsPersVG bedarf (Verhaltenskontrolle: welcher Mitarbeiter bestellt wie oft welches z. B. teure Material), rechtswidrig.

Das SMI hat daraufhin Materialbestellungen im Online-Verfahren an eine adäquate informierte Einwilligung geknüpft und beabsichtigt zu gegebener Zeit, mit mir abgestimmte datenschutzgerechte Verträge mit den in Frage kommenden Lieferanten abzuschließen.

5.1.12 Observation eines Polizeibeamten wegen häufiger Krankschreibungen

Wegen außergewöhnlich zahlreicher Krankschreibungen wies ein Abteilungsführer der Bereitschaftspolizei einen Hundertschaftsführer an, einen Polizeimeister zur Ausbildung an seinem Wohnort durch Beamte der Bereitschaftspolizei beobachten zu lassen, u. a. weil das Gerücht kursierte, der Betroffene baue trotz seiner Krankschreibung an einem Haus. Daraufhin beauftragte der Hundertschaftsführer vier seiner Beamten mit der Observation des Betroffenen. Hierzu bediente man sich eines

zivilen Einsatzfahrzeugs, einer Handvideokamera und eines Fotoapparates. Offiziell wurde die Aktion als „*Unterstützungseinsatz (UE) BGS*“ bzw. als „*BGS-Übung*“ bezeichnet. Nachdem die Beobachtungen ergebnislos verliefen, brach der Hundertschaftsführer - in Absprache mit dem Abteilungsführer - die Aktion nach einem Tag ab.

Dem SMI habe ich den Vorfall sowie meine Einschätzung dazu mitgeteilt. Unabhängig vom Ergebnis liegt der Observation unter Einsatz von ausschließlich für die Erfüllung von Polizeiaufgaben bestimmten Materials (Einsatzfahrzeug, Kameras) eine Anordnung der Vorgesetzten zur (heimlichen) Datenerhebung zugrunde, die nur zulässig hätte sein können, wenn der Anwendungsbereich des Sächsischen Polizeigesetzes berührt gewesen wäre, d. h. der Polizeivollzugsdienst eine Aufgabe im Sinne des § 1 Abs. 1 SächsPolG erfüllt hätte. Dies war jedoch ersichtlich nicht der Fall. Auch war eine Legitimation durch das Sächsische Beamtengesetz und das Sächsische Datenschutzgesetz nicht gegeben. Dessen hätten sich die verantwortlichen Vorgesetzten bewusst sein müssen.

Wegen der mit heimlichen Datenerhebungen (insbesondere mittels Videokamera und Fotoapparat) einhergehenden besonderen Eingriffstiefe in das Persönlichkeitsrecht habe ich den Vorfall für außerordentlich bedeutsam gehalten und vom SMI Konsequenzen und Vorschläge gefordert, wie solche Vorkommnisse künftig von vornherein ausgeschlossen werden können.

Das SMI hat inzwischen das Verhalten der Verantwortlichen missbilligt, die betreffende Dienststelle belehrt und um strikte Beachtung der einschlägigen Vorschriften ersucht.

5.1.13 Kontrolle einer „Beihilfestelle“

Bei der Kontrolle der „Beihilfestelle“ einer Körperschaft des öffentlichen Rechts, die das Recht zur Selbstverwaltung hat, Dienstherreneigenschaft besitzt und Beamte beschäftigt, habe ich u. a. Folgendes festgestellt:

1. *Keine Abschottung der Beihilfebearbeitung von der übrigen Personalverwaltung*

   Gemäß § 118 Satz 3 SächsBG soll die Beihilfeakte in einer von der Personalverwaltung getrennten Organisationseinheit bearbeitet werden; Zugang sollen nur Beschäftigte dieser Beihilfestelle haben. Der Sinn dieser Regelung liegt in der Vermeidung von Interessenkollisionen, die sich bei Personalmaßnahmen daraus ergeben können, dass den Entscheidungsträgern die Beihilfedaten (Diagnosedaten) des Beamten und ggf. seiner beihilfeberechtigten Angehörigen bekannt geworden sind.

   Die gesetzlich vorgesehene Abschottung fehlte; denn die Beihilfeangelegenheiten wurden von Sachbearbeitern des Personalreferats erledigt. Zwar waren deren Befugnisse auf eine selbständige und von der übrigen Personalverwaltung unabhängige Sacharbeit einschließlich der Widerspruchsentscheidungen ausgerichtet,

die Zeichnungsbefugnis endete jedoch bei 5 000 DM (höhere Beträge zeichnete der Referatsleiter).

Ich habe gefordert, die „Beihilfestelle“ aus dem Personalreferat auszugliedern.

Nun sollen zusätzliche Maßnahmen - Erweiterung der Unterschriftsbefugnis für die Sachbearbeiter auf 20.000 DM, Kontrolle durch die Innenrevision, fachliche Unterstützung durch externe Beihilfestellen nach anonymer Fallschilderung - die Beihilfebearbeitung innerhalb des Personalreferats zu einer „eigenen Organisationseinheit“ im Sinne von § 118 SächsBG machen.

Damit kann ich nicht einverstanden sein. An meinen Forderungen halte ich fest.

2. *Der Schriftverkehr mit den Beihilfeberechtigten lief über das Sekretariat des Personalreferats*

Wie wenig die organisatorische Trennung bisher vollzogen wurde, zeigte auch die Behandlung des Schriftverkehrs mit den Beihilfeberechtigten. So fertigte das Sekretariat des Personalreferats die Reinschriften der von den Sachbearbeitern entworfenen Schreiben (Rückfragen, Anforderung von Unterlagen, Widerspruchsentscheidungen) und speicherte sie im referatseigenen Textverarbeitungssystem. Im Briefkopf wurde als Absender „Personalreferat“ angegeben. Dies alles ist datenschutzrechtlich inakzeptabel.

Ich habe gefordert, dass die Sachbearbeiter die Reinschriften selbst fertigen. Auch muss die Angabe „Personalreferat“ im Briefkopf unterbleiben. Diese Absenderangabe veranlasst Beihilfeberechtigte nämlich dazu, Antwortschreiben an diese Stelle zu richten. Da einem so adressierten Brief von außen die Beihilfeangelegenheit nicht anzusehen ist, läuft er vermutlich über den Tisch des Referatsleiters, wo er nichts zu suchen hat.

Inzwischen fertigen die Sachbearbeiter die Reinschriften ihrer Entwürfe selbst. Als Absender erscheint nunmehr „Beihilfestelle“ und ein Standardtext weist die Betroffenen auf die Notwendigkeit dieser Angabe bei der Adressierung ihrer Antworten hin.

3. *An die Vernichtung alter Beihilfeunterlagen hatte noch niemand gedacht*

Unterlagen über Beihilfe sind gemäß § 123 Abs. 2 Satz 1 SächsBG fünf Jahre nach Ablauf des Jahres, in dem die einzelne Beihilfebearbeitung abgeschlossen wurde, aufzubewahren und gemäß § 123 Abs. 4 SächsBG zu vernichten, sofern sie nicht von einem der genannten Archive übernommen werden. Eine Vernichtung von Beihilfeunterlagen erfolgte bisher nicht. Die ältesten Unterlagen stammten aus dem Jahre 1992.

Vorgänge, deren Aufbewahrungsfrist abgelaufen war, wurden inzwischen dem Staatsarchiv angeboten.

4. *Was sollten die Notizen?*

Eine Reihe von Beihilfeakten enthielt ein Vorblatt mit Notizen über Ärzte, Diagnosen und Spezialbehandlungen. Eine Systematik war nicht zu erkennen, auch konnte mir die Erforderlichkeit nicht überzeugend dargelegt werden.

Gemäß § 123 Abs. 2 Satz 2 SächsBG sind Unterlagen, aus denen die Art einer Erkrankung ersichtlich ist, unverzüglich zurückzugeben, wenn sie für den Zweck, zu dem sie vorgelegt worden sind, nicht mehr benötigt werden. Diesem Grundsatz widersprachen die Aufzeichnungen.

Gegen Vorblätter mit beihilferelevanten Aufzeichnungen (z. B. zur Fristüberwachung bei Brillen und Zahnersatz) in „neutraler" Form, also ohne Angabe von Ärzten, Diagnosen, Verordnungen etc., bestehen keine datenschutzrechtlichen Bedenken.

Die Aktenbereinigung wurde mir inzwischen bestätigt.

5.1.14 Überprüfung von Beschäftigten sächsischer Sparkassen auf Stasi-Tätigkeit

Zwischen dem SMI und mir besteht Streit über meine Kontrollzuständigkeit für die Personalverwaltung sächsischer Sparkassen. Zugrunde liegt folgender Fall: Durch eine Eingabe erfuhr ich von der Praxis einer sächsischen Sparkasse, Bewerber mit ihrer Einwilligung und Beschäftigte mit ihrer Kenntnis auf eine vormalige Mitarbeit beim MfS nach § 21 Abs. 1 Nr. 6 Buchstabe d StUG überprüfen zu lassen. Nach dieser Vorschrift ist eine Verwendung von Stasi-Unterlagen zur Feststellung einer MfS-Mitarbeit zulässig, wenn eine Beschäftigung im „Öffentlichen Dienst" in Rede steht. Die Verarbeitung der Daten von Bewerbern und Beschäftigten durch die Sparkasse im Rahmen der BStU-Überprüfung müsste also im Rahmen einer dem Öffentlichen Dienst zuzurechnenden Betätigung der Sparkasse erfolgen. Für eine derartige Datenverarbeitung eines öffentlich-rechtlichen Unternehmens sehe ich meine Kontrollzuständigkeit als gegeben an.

Meine Rechtsauffassung wird vom SMI jedoch nicht geteilt. Das SMI beruft sich auf § 2 Abs. 3 SächsDSG und möchte dieser Vorschrift entnehmen, dass für die gesamte Datenverarbeitung der Sparkassen die Vorschriften des Bundesdatenschutzgesetzes mit Ausnahme des zweiten Abschnittes gälten. Deshalb seien für die datenschutzrechtliche (Anlass-) Kontrolle die Regierungspräsidien als Aufsichtsbehörden über den privaten Bereich zuständig.

Dies kann so jedoch nicht zutreffen: Denn nach § 2 Abs. 3 SächsDSG gelten für öffentlich-rechtliche Unternehmen mit eigener Rechtspersönlichkeit nur, „*soweit*" diese am Wettbewerb teilnehmen, die Vorschriften des Bundesdatenschutzgesetzes mit Ausnahme des zweiten Abschnittes. Wortlaut und Entstehungsgeschichte von § 2 Abs. 3 SächsDSG sprechen im Übrigen hier eine deutliche Sprache: Der Gesetzgeber

hat zwischen den wettbewerblichen und den nicht-wettbewerblichen Tätigkeiten von Wettbewerbsunternehmen unterscheiden wollen. Das Wort „soweit“ ist kein Redaktionsversehen. Es ist im Entstehungsprozess des SächsDSG (DrS 1/523; Interfraktionelle Arbeitsgruppe; Endfassung) trotz des an anderen Stellen verwandten „wenn“ (§ 4 Abs. 1 Nr. 1; § 8 Abs. 2 Satz 1) durchgehend verwandt worden. Es findet schließlich seine Entsprechung in § 27 Abs. 1 Satz 1 Nr. 2 Buchstabe b BDSG („...*soweit* sie als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen ...“).

Somit ist zwischen wettbewerblichem und nicht-wettbewerblichem Handeln der Sparkassen zu unterscheiden. Die Personaldatenverarbeitung sächsischer Sparkassen ist nicht Ausdruck wettbewerblichen Handelns. Sie ist keine Leistung, die dem Kunden in Konkurrenz zu anderen Unternehmen, etwa Banken angeboten wird. Ihr Gegenstand ist nicht der Kunde, sondern der Beschäftigte der Sparkasse, der einer Dienstaufsicht durch einen Dienstvorgesetzten, § 24 Abs. 3 SächsSprkG unterliegt und dessen Vergütung nach BAT-Ostdeutsche Sparkassen, der dem BAT-O entspricht, erfolgt.

Ich werde mich deshalb weiter dafür einsetzen, dass sich das SMI meiner Rechtsauffassung anschließt.

5.1.15 Datenerhebung bei Inanspruchnahme von Elternzeit nach § 16 Abs. 1 Bundeserziehungsgeldgesetz für Arbeitnehmerinnen und Arbeitnehmer

Die Gewährung von Elternzeit (bis zum 31. Dezember 2001 „Erziehungsurlaub“) ist an eine Reihe von Voraussetzungen gebunden, die zum Teil in einem komplizierten Abhängigkeitsverhältnis zueinander stehen. Aus der komplizierten Rechtslage haben sich Antragsformulare entwickelt, in denen zumeist nicht erforderliche Daten über das Kindschaftsverhältnis oder den Ehegatten erhoben und dubiose Bescheinigungen von Ärzten und Krankenversicherungen verlangt wurden.

Aufgrund meiner Kritik wurde in einem Geschäftsbereich des SMK ein Vordruck konzipiert, den ich weiterempfehlen kann. Ein Muster ist unter Nr. 16.2 abgedruckt.

5.2 Personalvertretung

In diesem Jahr nicht belegt.

5.3 Einwohnermeldewesen

5.3.1 Drittes Gesetz zur Änderung des Melderechtsrahmengesetzes (MRRG)

Die Datenschutzbeauftragten des Bundes und der Länder beschäftigen sich seit Mitte 2000 mit Arbeitsentwürfen des BMI zur Änderung des MRRG.

Die Tendenz, das Melderegister in Abkehr von der jetzigen Rechtslage zu einem *öffentlichen* Register zu machen, das für jedermann - auch für ausländische Stellen - auf elektronischem Wege zugänglich ist, ohne dass die Meldebehörden z. B. prüfen können, ob schutzwürdige Interessen der Betroffenen beeinträchtigt werden, wird allenthalben mit Sorge beobachtet (siehe auch Materialien Nr. 16.1.19).

Mit dem SMI bin ich einig, dass den Novellierungsabsichten, die letztendlich zu einem bundesweiten Einwohnerregister - als Folge der elektronischen Verknüpfung - führen würden, mit Nachdruck zu begegnen ist.

Die Entwicklung wird von mir aufmerksam beobachtet.

5.3.2 Veröffentlichung von Jubiläumsdaten

In 8/5.3.2 habe ich darauf hingewiesen, dass Jubiläumsdaten nach § 33 Abs. 2 SächsMG ab dem 70. Geburtstag und ab der goldenen Hochzeit veröffentlicht werden dürfen, falls die Betroffenen dem nicht widersprochen haben.

Trotz des eindeutigen Gesetzeswortlautes stelle ich immer wieder fest, dass die Altersuntergrenze von 70 Jahren nicht beachtet wird und auch Ehejubiläen, die vor der goldenen Hochzeit liegen, veröffentlicht werden. Das damit zum Ausdruck kommende Staatsverständnis - die Obrigkeit als Vater, Mutter, Freund und Vormund - lehne ich ab. Gesellschaftliches Engagement, Fürsorge und gelegentliche Betreuung können in Kirchen und Vereinen, in Nachbarschaften - und vor allem in der Familie - gepflegt werden.

Deshalb möchte ich noch einmal klarstellen:

1. Die Veröffentlichung von Alters- und Ehejubiläumsdaten (§ 33 Abs. 2 SächsMG) ist nur nach Maßgabe des § 33 Abs. 4 SächsMG zulässig. Insbesondere ist mindestens einmal jährlich durch öffentliche Bekanntmachung auf das Widerspruchsrecht hinzuweisen. Adressaten dieser Bekanntmachung sind die Einwohner, die den 70. oder einen späteren Geburtstag sowie die Einwohner, die die goldene Hochzeit oder ein späteres Ehejubiläum begehen.
   Widerspruch bedeutet: Die Veröffentlichung (in den gesetzlichen Grenzen) ist grundsätzlich *zulässig***,** es sei denn, der Betroffene hat widersprochen.

2. Für Personen, die nicht von § 33 Abs. 2 SächsMG erfasst sind (also die unter 70-jährigen und diejenigen, die noch keine goldene Hochzeit haben), gilt dieses Widerspruchsrecht nicht, sondern umgekehrt die Einwilligung (vgl. § 4 Abs. 1 Nr. 2 SächsMG i. V. m. § 4 Abs. 1 Nr. 2, Abs. 2 und 3 SächsDSG).
   Einwilligung bedeutet: Die Veröffentlichung ist grundsätzlich *unzulässig*, es sei denn, der Betroffene erklärt sich vorher ausdrücklich mit ihr einverstanden.

   Da eine Einwilligung immer freiwillig und informiert zu erfolgen hat, müsste sich die Meldebehörde an jeden einzelnen älteren Einwohner wenden und ihn befragen, ob er mit der Veröffentlichung einverstanden ist. Dabei müsste auf denkbare

Folgen hingewiesen werden, die mit einer Veröffentlichung einhergehen, zumal solche Informationen nicht nur regional eine Rolle spielen, sondern vielmehr durch entsprechende Unternehmen auch überregional ausgewertet werden (insbesondere für allerlei Unternehmen - z. B. Veranstalter von Kaffee-Fahrten, aber auch für Betrüger sind Namen und Adressen älterer Einwohner sehr wohl interessant).

Abgesehen von dem nicht zu unterschätzenden Verwaltungsaufwand rate ich deshalb grundsätzlich von solchen Veröffentlichungen ab, zumal § 33 Abs. 2 SächsMG eine Ermessensvorschrift ist („die Meldebehörde darf ...“). Jüngsten Absichten der Bundesregierung zufolge, soll auch das bisherige Widerspruchsrecht durch eine Einwilligungserklärung abgelöst werden, die die Situation vermutlich entscheidend entschärfen wird.

5.3.3 Online-Zugriff der Jagd-, Waffen- und Sprengstofferlaubnisbehörde (Ordnungsamt) auf das Melderegister

Nach § 8 Abs. 3 SächsDSG bin ich vor der Einrichtung eines automatisierten Abrufverfahrens zu unterrichten. Im Vollzug dieser Bestimmung teilte mir eine Stadtverwaltung ihre Absicht mit, dem Ordnungsamt einen Online-Zugriff auf das Melderegister einzurichten.

Das Abrufverfahren sollte folgenden Zwecken dienen:
- Prüfen der örtlichen Zuständigkeit nach Waffen-, Jagd- und Sprengstoffgesetz,
- Regelüberprüfung der Jäger, Sportschützen und Waffenscheininhaber.

Die Einrichtung des automatisierten Abrufverfahrens wurde als erforderlich angesehen, weil regelmäßig die Daten für ca. 1500 bis 2000 Personen geprüft werden müssten.

Ich habe das Vorhaben wie folgt beurteilt:

Nach § 29 Abs. 7 SächsMG ist die Weitergabe (und das Bereithalten zur Einsichtnahme) von Meldedaten innerhalb der Stadtverwaltung u. a. nur zulässig, wenn dies zur Erfüllung der Aufgaben der Meldebehörde oder der empfangenden Stelle *erforderlich* ist. Eine Online-Anbindung an das Melderegister stellt eine besondere (technische) Art der Datenübermittlung dar, für die wegen der damit verbundenen Eingriffstiefe in das Recht auf informationelle Selbstbestimmung dem Erforderlichkeitsgrundsatz sowie dem Grundsatz der Angemessenheit eine herausragende Bedeutung zukommt.

Den mir vorgelegten Unterlagen zufolge sollen die Meldedaten nicht nur lückenlos zur Überprüfung der Angaben in jagd-, waffen- und sprengstoffrechtlichen Anträgen, sondern auch regelmäßig zu turnusmäßigen Überprüfungen der entsprechenden Erlaubnisse vom Ordnungsamt abgerufen werden.

Nach meiner Kenntnis sind die Antragsteller gehalten, wahrheitsgemäße Angaben zu machen sowie ihre Zuverlässigkeit und Sachkunde nachzuweisen. Von solchermaßen

Überprüften ist grundsätzlich nicht zu erwarten, dass sie im Antrag unrichtige Angaben zu ihrer Person machen; erst recht konnte ich nicht erkennen, wie etwa unrichtige Angaben über die regelmäßige Überprüfung der Meldedaten mittels Online-Zugriff entdeckt würden. Zum Nachweis der Identität genügt in der Regel die Vorlage einer aktuellen Meldebescheinigung und/oder des Personalausweises/Reisepasses, so dass nur in begründeten Ausnahmefällen eine Überprüfung der Personalien bei der Meldebehörde infrage kommt. Dies kann in herkömmlicher Weise durch Anfrage im Einzelfall geschehen.

Auch die dem Jagd-, Waffen- und Sprengstoffrecht immanenten Kontrollmechanismen sowie die entsprechenden Pflichten der Erlaubnisinhaber und sonstiger Berechtigter verdeutlichen, dass auch eine turnusmäßige „Regelüberprüfung" der Meldeverhältnisse nicht erforderlich ist.

Dem beabsichtigten Abrufverfahren zugunsten des Ordnungsamtes vermochte ich deshalb nicht zuzustimmen. Die Stadtverwaltung hat dies akzeptiert.

5.4 Personenstandswesen

Unbedachte Offenbarung eines Adoptionsverhältnisses durch eine Standesamtsaufsichtsbehörde

Eine Standesamtsaufsichtsbehörde wandte sich im Zusammenhang eines Namensberichtigungsverfahrens (ein Adliger wollte die Bezeichnung „Freiherr" als Namensbestandteil durchsetzen) an das Deutsche Adelsarchiv (e. V.), um Anhaltspunkte für den behaupteten Freiherrenstand zu erhalten.

Zur Erläuterung führte die Standesamtsaufsichtsbehörde - unter Missachtung des § 61 Abs. 2 PStG - ausführlich aus, wer wann wen adoptiert hatte.

Ich habe die Standesamtsaufsichtsbehörde außer auf § 61 Abs. 2 PStG auch auf § 1758 BGB hingewiesen, wonach Tatsachen, die geeignet sind, die Annahme an Kindes statt und ihre Umstände aufzudecken, ohne Zustimmung des Annehmenden und des Angenommenen nicht offenbart oder ausgeforscht werden dürfen, es sei denn, dass besondere Gründe des öffentlichen Interesses dies erfordern.

Die Standesamtsaufsichtsbehörde war zur Feststellung, ob sich der Betroffene „Freiherr" nennen darf, nicht berechtigt, dem Deutschen Adelsarchiv e. V. Adoptionsdaten mitzuteilen. Da das Personal der Behörde als Konsequenz meiner Ausführungen eindringlich auf die Einhaltung datenschutzrechtlicher Bestimmungen „vergattert" wurde und eine Wiederholung solcher Datenschutzverstöße nicht zu befürchten ist, habe ich gemäß § 26 Abs. 2 SächDSG von einer förmlichen Beanstandung abgesehen.

5.5 Kommunale Selbstverwaltung

5.5.1 Anfrage-, Unterrichtungs- und Akteneinsichtsrechte des Stadtrates

In einer Stadt begehrte ein einzelnes Stadtratsmitglied Einsicht in Unterlagen mit Personalaktenbezug, um festzustellen, ob aufgrund eines Wirtschaftlichkeitsberichts erforderlich gewordene Personalmaßnahmen ordnungsgemäß vollzogen wurden. Der Bürgermeister fragte mich, ob er dem Begehren entsprechen dürfe.

Ich habe ihm mitgeteilt, dass die Anfrage-, Unterrichtungs- und Akteneinsichtsrechte des Stadtrates in § 28 SächsGemO abschließend geregelt sind. Nach § 28 Abs. 4 SächsGemO kann ein Viertel der Stadträte in allen Angelegenheiten der Gemeinde verlangen, dass der Bürgermeister den Stadtrat informiert und diesem oder einem von ihm bestellten Ausschuss Akteneinsicht gewährt. Das nähere Verfahren über die Akteneinsicht kann in der Geschäftsordnung geregelt werden. Aus datenschutzrechtlicher Sicht halte ich es für erforderlich, dass die Akteneinsicht in den Räumen der Verwaltung unter Aufsicht erfolgt. Eine Aktenherausgabe ist nicht vorgesehen und daher unzulässig. Mit der Akteneinsicht sollte nicht der gesamte Stadtrat oder ein kompletter Ausschuss betraut werden, sondern je ein Stadtratsmitglied pro Fraktion als Obmann. Diese können nach erfolgter Akteneinsichtnahme ihre Fraktionskollegen informieren.

Nur unter diesen Voraussetzungen halte ich eine (ggf. auch personenbezogene) Überprüfung des aus dem Prüfbericht der Wirtschaftsprüfungs-Gesellschaft resultierenden Personalabbaus für zulässig, zumal die Stadträte zur Verschwiegenheit verpflichtet sind.

Dem Wunsch eines einzelnen Stadtratsmitgliedes auf Akteneinsicht kann hingegen nicht entsprochen werden. Nach § 28 Abs. 5 Satz 1 SächsGemO kann zwar jeder Stadtrat an den Bürgermeister schriftliche oder in einer Sitzung des Stadtrates mündliche Anfragen über einzelne Angelegenheiten der Stadt richten, die binnen angemessener Frist zu beantworten sind. Das Fragerecht umfasst jedoch nicht das Recht auf Akteneinsicht. Das Nähere ist gemäß § 28 Abs. 5 Satz 2 SächsGemO in der Geschäftsordnung zu regeln. Da mir die Geschäftsordnung der Stadt nicht vorlag, vermochte ich aus datenschutzrechtlicher Sicht nur allgemein auf den Grundsatz der Datensparsamkeit hinzuweisen. Bei den Antworten des Bürgermeisters sollten personenbezogene Beschäftigtendaten grundsätzlich nicht mitgeteilt werden, weil ein einzelnes Stadtratsmitglied keine originären Aufgaben nach der Gemeindeordnung hat und personenbezogene Daten nur mitgeteilt werden dürfen, soweit es zur (rechtmäßigen) Aufgabenerfüllung erforderlich ist.

Es ist aber Aufgabe des gesamten Stadtrates (und eben nicht eines einzelnen Stadtratsmitgliedes) die Ausführung der Stadtratsbeschlüsse zu überwachen und beim Auftreten von Missständen in der Stadtverwaltung für deren Beseitigung durch den Bürgermeister zu sorgen (§ 28 Abs. 2 SächsGemO). Soweit hierfür personenbezogene Daten unerlässlich sind, dürfen sie dem Stadtrat im Rahmen des § 28 Abs. 4 SächsGemO (siehe oben) zur Kenntnis gegeben werden.

5.5.2 Angabe des Grundes der Abwesenheit in Sitzungsniederschriften des Gemeinderats

Eine Stadt hatte bisher aus Gründen des Datenschutzes den Grund der Abwesenheit von Stadtratsmitgliedern, die nicht an einer Sitzung teilnahmen, nicht in der Sitzungsniederschrift angegeben. Dies wurde von der Kommunalaufsicht unter Hinweis auf § 40 Abs. 1 SächsGemO beanstandet. Daraufhin fragte mich die Stadt nach meiner Meinung. Ich antwortete, dass die Sächsische Gemeindeordnung ein verfassungsgemäß zustande gekommenes Gesetz sei, das in § 40 Abs. 1 SächsGemO u. a. vorschreibt, außer den Namen auch den Grund der Abwesenheit der nicht an der Sitzung teilnehmenden Gemeinderäte in der Niederschrift anzugeben. Mit dieser Vorschrift werden also das Erheben und Speichern personenbezogener Daten spezialgesetzlich geregelt. Nach § 2 Abs. 4 SächsDSG gehen besondere Vorschriften den Regelungen im Sächsischen Datenschutzgesetz vor (das SächsDSG ist lediglich ein „Auffanggesetz“, das nur dann Wirkung entfaltet, wenn es keine spezielleren Rechtsvorschriften in anderen Gesetzen gibt).

Da die Verwaltung gemäß Art. 20 Abs. 3 GG, Art. 3 Abs. 3 SächsVerf an Gesetz und Recht gebunden ist, ist die Stadt verpflichtet, auch einen Grund der Abwesenheit in die Niederschrift aufzunehmen, auch wenn damit möglicherweise sensible Informationen (z. B. Krankheit, Auslandsurlaub, Haft, Todesfall, Familienfest) über § 40 Abs. 2 Satz 5 SächsGemO (Einsichtnahme der Einwohner in die Niederschriften des Gemeinderats) in die Öffentlichkeit gelangen.

Aus datenschutzrechtlicher Sicht kann ich nur raten, den Grund der Abwesenheit möglichst neutral so zu gestalten, (z. B. auch „dienstlich/geschäftlich entschuldigt“, „privat entschuldigt“, „nicht entschuldigt“), dass Rückschlüsse auf den Abwesenheitsgrund im Einzelnen zumindest erschwert werden.

5.5.3 „Stationärer Bürgerladen“ - Pilotprojekt in Sachsen

Der SSG informierte mich über ein beabsichtigtes Pilotprojekt, das eine Bündelung kommunaler Aufgaben und privater Dienstleistungen in einer (kommunalen) Hand vorsieht und fragte, ob aus datenschutzrechtlicher Sicht Hinderungsgründe bestehen. Meine Hinweise auf die vom Bundesverfassungsgericht geprägten Grundsätze der „informationellen Gewaltenteilung“ und der Zweckbindung der Daten (BVerfGE 65, 46 und 73) blieben zunächst ebenso unbeachtet wie der Grundsatz der Gesetzmäßigkeit der Verwaltung (Art. 20 Abs. 3 GG, Art. 3 Abs. 3 SächsVerf). Auch meinen Hinweis auf die kommunalen Vorschriften über die wirtschaftliche Betätigung, die ausdrücklich die Rechtfertigung durch einen „öffentlichen Zweck“ verlangen (§ 97 SächsGemO) wurden nicht ernst genommen. Bestärkt durch das SMI, das eine Übertragung zumindest von Sparkassenaufgaben auf gemeindliches Personal als „Auftragsdatenverarbeitung“ i. S. v. § 11 BDSG für zulässig hält, wurde das Projekt rigoros vorangetrieben, wobei meine Kritik einfach unbeachtet blieb.

Erst mein Nachhaken anlässlich eines Gesprächs mit dem verantwortlichen Oberbürgermeister brachten die wahren Hintergründe, die wenig mit Bürgerfreundlichkeit oder Bürgernähe zu tun haben, ans Tageslicht.

Es stellte sich nämlich heraus, dass der Ostdeutsche Sparkassen- und Giroverband (OSGV) beabsichtigt, zunächst in einer sächsischen Stadt als Pilotprojekt tatsächlich Sparkassenaufgaben von städtischer Bediensteten erbringen lassen möchte. Hintergrund sei - sollte sich dieses Projekt bewähren - die flächendeckende Einführung dieser Verfahrensweise überall da, wo sich Sparkassenfilialen nicht mehr rentieren. Der OSGV hat der Stadt für die Durchführung des Pilotprojekts einen Betrag von 200.000,- DM als einmalige Zahlung sowie eine pauschale Beteiligung am laufenden Betrieb in Aussicht gestellt, der dem stark gebeutelten Stadtsäckel als „warmer Regen“ ausgesprochen gut tun dürfte. Wer kann da schon Nein sagen? Wie ein solches „Sponsoring“ haushaltsrechtlich zu bewerten ist, habe ich allerdings nicht zu beurteilen.

Konkretisiert werden die Aufgaben des „Bürgerladens“ (künftig trägt er den Namen „HIER“), in einem Vertrag zwischen der Sparkasse und der Pilotgemeinde.

Gegenstand des Vertrages ist die Durchführung von Aufgaben und Dienstleistungen der Sparkasse durch die Gemeinde als „Erfüllungsgehilfe“ der Sparkasse.

Nach § 2 des Vertrages hat die Pilotgemeinde folgende Dienstleistungen für die Sparkasse zu erbringen:
- Zahlgeschäfte (bare Ein- und Auszahlungen auf Konten und auf Sparbücher)
- Einrichtung, Änderung und Löschung von Daueraufträgen
- Annahme und Weiterleitung von Überweisungen (keine Disposition)
- Annahme und Ausgabe von Schecks (keine Disposition)
- Annahme von Kartenanträgen (ec-Card, Eurocard und S-Card) (keine Genehmigung)
- Antrag auf Eröffnung eines Girokontos für Privatkunden (Entgegennahme und Weiterleitung an die Sparkasse inkl. Legitimationsprüfung)
- Ausgabe von Kontoauszügen
- Vermittlung von Beratungsgesprächen inkl. Terminvereinbarungen

Hierüber habe ich die Oberste Sparkassenaufsichtsbehörde (SMF) informiert. Diese sah allerdings darin keine Hinderungsgründe, die gegen eine Übertragung der Sparkassenaufgaben auf Gemeindepersonal sprechen könnten. Das ebenfalls eingeschaltete SMI befürwortet sogar das Verfahren und hält es für besonders innovativ.

Dass damit dem gemeindlichen Personal Einblick in die finanziellen Verhältnisse der Gemeindebürger, die Sparkassenkunden sind, und in deren Zahlungsgebaren einschließlich der Zahlungsempfänger (z. B. Bußgeldstelle, Gerichte, Krankenhäuser) gewährt wird, und dass hieraus gewonnene Erkenntnisse geeignet sind, kommunale Entscheidungen zu beeinflussen, interessierte offenbar nicht sonderlich.

Vor dem Hintergrund der zu erwartenden Interssenkollisionen dürfte es rechtlich kaum möglich sein, von der gesetzlichen Zulässigkeit des Vorhabens auszugehen, zumal es sich bei der „Erledigung einzelner Sparkassengeschäfte“ durch gemeindliches Personal - wie vom SMI irrtümlich angenommen - eben nicht um eine Datenverarbeitung im Auftrag handelt, sondern um eine Aufgabenübertragung (zu

deren Erfüllung personenbezogene Daten verarbeitet werden müssen). Datenverarbeitung ist keine Aufgabe, sondern ein technisches Hilfsmittel zur Erfüllung der Aufgabe. Die Aufgaben der Gemeinden sind in der SächsGemO, die Aufgaben der Sparkasse im SächsSparkG geregelt. Ich halte eine Übertragung von Sparkassenaufgaben auf eine Gemeinde ebenso für unzulässig wie beispielsweise umgekehrt, die Übertragung von Gemeindeaufgaben auf die Sparkasse (auf eine solche Idee kommt vielleicht auch jemand). Dafür gibt es keine Rechtsgrundlagen (z. B. im SächsKomZG); eine damit einhergehende Datenverarbeitung wäre unzulässig.

Dies gilt ebenso für Postdienstleistungen, die durch gemeindliches Personal erbracht werden sollen. Auch dagegen habe ich Bedenken, weil das kommunale Personal Kenntnis davon erhält, wer mit welchen Stellen korrespondiert (z. B. Paket- oder Briefsendung an den in einer JVA sitzenden Ehegatten; Abholung amtlicher Zustellungen).

Meine datenschutzrechtlichen Bedenken habe ich deshalb dem SMI und dem Oberbürgermeister mitgeteilt und angekündigt, das Projekt gemäß § 26 SächsDSG zu beanstanden, wenn der Vertrag mit der Sparkasse tatsächlich erfüllt wird und evtl. andere private Dienstleistungen (z. B. Postdienstleistungen) durch gemeindliches Personal erbracht werden sollten.

Ungeachtet dessen stand im „Sachsenlandkurier“ 01/01 ein Beitrag des Hauptamtsleiters der Stadt Sebnitz zum Thema „Bürgerladen“, der im Ergebnis festhält, dass gemeinsam mit der Sächsischen Staatsregierung, dem SSG *und mit mir* datenschutzrechtliche Unstimmigkeiten *ausgeräumt* worden seien. Das ist unrichtig, denn ich halte die Bündelung kommunaler Aufgaben und privater (Sparkassen-) Dienstleistungen in einer Hand nach wie vor für unzulässig. Auch das interessierte den Oberbürgermeister nicht sonderlich, denn er teilte mir Mitte März 2001 lakonisch mit, dass das Projekt „Stationärer Bürgerladen“ HIER in Hinterhermsdorf am 12. März 2001 den Probebetrieb aufgenommen hätte.
Weil mich der Oberbürgermeister vor vollendete Tatsachen gestellt hat, werde ich die rechtswidrige Bündelung von kommunalen Aufgaben und privaten Dienstleistungen gemäß § 26 SächsDSG beanstanden.

Die Bürger sollten es sich gut überlegen, ob sie ihre Sparkassenangelegenheiten tatsächlich von Gemeindepersonal erledigt haben wollen.

5.5.4 Datenerhebung bei Stundungsanträgen - Offenlegung der Einkommens- und Vermögensverhältnisse sowie personenbezogene Angaben über Dritte

In letzter Zeit häuften sich die Eingaben betroffener Bürger, die sich durch die bereits in 6/5.5.1 von mir kritisierten Fragen im Zusammenhang mit Stundungsanträgen in ihren schutzwürdigen Interessen beeinträchtigt fühlten.

Ich habe die Angelegenheit wieder aufgegriffen und konnte in einem kooperativen Gespräch mit dem SMI erreichen, dass die kritischen Fragen im Stundungsantrags-

muster (das sachsenweit Verwendung findet) unter Verzicht auf personenbezogene Daten Dritter überarbeitet werden.

Die Daten von Mitbewohnern, Familienmitgliedern oder sonstigen Dritten sind in Stundungsverfahren grundsätzlich irrelevant. Wichtig sind nur Vermögen, Einnahmen und Ausgaben der Abgabenschuldner.

5.6 Baurecht; Wohnungswesen

In diesem Jahr nicht belegt.

5.7 Statistikwesen

5.7.1 Erfahrungen mit dem Sächsischen Erwerbsstatistikgesetz

Die 1999 per Gesetz eingeführte *Statistik der Erwerbssituation im Freistaat Sachsen* (7/5.7.1) hat, wie erwartet, zu vielen Eingaben geführt, allerdings mit deutlich abnehmender Tendenz. Manchen Petenten hat es wohl enttäuscht, zu hören, dass der Sächsische Datenschutzbeauftragte die Statistik nicht für verfassungswidrig hält. Ich wundere mich, mit welchem Ärger manche empfindlichen Zeitgenossen auf die Fragen der Befrager reagieren. Dabei ist eine gute Statistik doch wirklich hilfreich.

Das Widerstreben, welches das sehr umfangreiche und im Bereich von Einkommen, Arbeit und dergleichen doch sehr in die Einzelheiten gehende Erhebungsprogramm auslöst, wird oft schon deutlich vermindert, wenn dem Betroffenen die Möglichkeit bewusst wird, seine Angaben nicht gegenüber dem Erhebungsbeauftragten machen zu müssen. Er kann dann davon ausgehen, dass seine Angaben nur sehr unpersönlich, womöglich von Anfang an ausschließlich maschinell verarbeitet werden. Daher habe ich stark darauf gedrungen, dass das StaLA stärker auf diese nach § 8 Abs. 1 Satz 1 SächsErwStatG, § 17 Abs. 4 SächsStatG bestehende Möglichkeit der rein schriftlichen Beantwortung (unmittelbar gegenüber dem Amt) hinweist. Das StaLA hat durch entsprechende Verbesserungen auf der Rückseite der erwähnten Ankündigungskarte meinem Verlangen stattgegeben, leider allerdings nicht in vollem Umfang. Dahinter steckt wohl die Hoffnung, dass im Interview durch den Erhebungsbeauftragten zuverlässigere Daten gewonnen werden können. Umso deutlicher weise ich Petenten auf diese unpersönlichere Form der Erfüllung der Auskunftspflicht hin.

Daneben hat es einige bemerkenswerte Einzelprobleme gegeben.

Diese betrafen vor allem die *Stichprobenauswahl*.
(1) Einige Eingaben - auch zum Mikrozensusgesetz - haben dabei mit einer nicht ohne weiteres verständlichen Gesetzesformulierung zu tun gehabt, die einfach aus dem Mikro- zensusgesetz (vom 17. Januar 1996, BGBl. I S. 34) in das Sächsische Erwerbstatistikgesetz übernommen worden ist. In beiden Gesetzen heißt es zur Auswahl der zu befragenden Haushalte (diese sind, etwas vereinfacht, die „Erhebungseinheiten“

bei dieser Statistik), also zur Stichprobenauswahl, jeweils in § 2 Abs. 1 Satz 2: *Die Erhebungseinheiten werden durch mathematische Zufallsverfahren auf der Grundlage von Flächen oder vergleichbarer Bezugsgrößen ausgewählt (Auswahlbezirke).*

In Anbetracht dieser Regelung konnte es Befragte verständlicherweise verwundern, wenn sie bemerkten, dass sie in dem von ihnen bewohnten Haus nicht die einzigen waren, die 'es erwischt hatte', sondern dass gleich mehrere Wohnparteien zur Auskunft für die Statistik herangezogen wurden. Es konnte scheinen, dass hier gerade nicht der *mathematische Zufall*, sondern Willkür, Bequemlichkeit oder Nachlässigkeit bei der Stichprobenauswahl am Werke gewesen seien.
Die Erklärung dafür, dass es doch mit rechten Dingen zugegangen ist, hat man der - unscheinbaren, wenig verständlichen und daher leicht zu überlesenden - Formulierung *auf der Grundlage von Flächen oder vergleichbarer Bezugsgrößen (Auswahlbezirke)* zu entnehmen. Sie besagt, dass das Verfahren der mathematischen Zufalls-Auswahl sich nicht, wie man als statistischer Laie erwartet, auf die einzelne Erhebungseinheit (vereinfacht ist das, wie gesagt, der Haushalt) bezieht, sondern auf Ansammlungen von Erhebungseinheiten, die das Gesetz „Auswahlbezirke" nennt (und die durch Ortsnamen, Straßennamen und Hausnummer[n] definiert sind). Ein Auswahlbezirk umfasst mithin mehrere Erhebungseinheiten. Dies geschieht zur Verminderung des Aufwandes für die Erhebungsbeauftragten. Nach Auskunft der Statistiker bleibt dabei die Repräsentativität der Stichprobe gewahrt: Der sog. Klumpeneffekt führe nur zu einer hinnehmbar geringen Vergrößerung des sog. Stichprobenfehlers.
Datenschutzrechtlich bedeutet das: Die Verfahrensweise ist nicht als statistikfachlicher Kunstfehler anzusehen, die damit einhergehende Verarbeitung personenbezogener Daten also nicht infolge Ungeeignetheit rechtswidrig. Der mit dieser Art der Stichprobengewinnung einhergehenden Verarbeitung personenbezogener Daten mangelt es auch nicht an der nötigen bestimmten und klaren gesetzlichen Grundlage, auch wenn es wohl besser gewesen wäre, wenn der Gesetzgeber formuliert hätte: *Sie werden auf der Grundlage von Flächen oder vergleichbarer Bezugsgrößen ausgewählt (Auswahl-bezirke), die durch mathematische Zufallsverfahren bestimmt werden.*

(2) Diese Verfahrensweise führt dann bei der Erstbefragung zu dem ebenfalls auf den ersten Blick den Betrachter sehr befremdenden, irrregulär wirkenden Vorgang, dass der Erhebungsbeauftragte bei seiner sog. Erstbegehung der Auswahlbezirke Namen von Klingelschildern und Wohnungstüren abliest und auf die Briefumschläge schreibt, in denen sich das erste Informationsmaterial, insbesondere auch der Gesetzestext befindet, und auf die dazugehörige sog. Ankündigungskarte, einen DIN A5-Bogen in kräftigerem Papier, auf dem der Erhebungsbeauftragte sich mit Namen, Anschrift und Telefonnummer bekannt macht und einen Termin angibt, zu dem er zur Durchführung des Interviews den Auskunftspflichtigen aufsuchen werde, falls dieser nicht mit ihm einen Ersatztermin vereinbare.
Die Erklärung für diese irrregulär wirkende Vorgehensweise: Ausgewählt ist nur der *Auswahlbezirk*, d. h. eine 'Menge' nahe beieinander liegender Wohnungen; irgendwelche Namen sind dabei noch nicht bekannt, sie müssen vom Erhebungsbeauftragten erst den Wohnungen durch die Begehung zugeordnet werden. Das führt

dann auch dazu, dass sowenig genaue und damit Misstrauen erweckende Adressierungen wie „Familie Müller“ (auch wenn es sich möglicherweise lediglich um einen einzelnen Herrn Müller handelt, der dort wohnt) auf dieser ersten Mitteilung des StaLA stehen können.
Es kann also bei dem Betroffenen recht leicht der Verdacht entstehen, es gehe bei der Stichprobenauswahl nicht mit rechten Dingen zu (was die Rechtswidrigkeit der dann ja ungeeigneten Datenverarbeitung zur Folge hätte). Ich habe - allerdings bisher vergeblich - daher dem StaLA geraten, in seinen Erläuterungen, die es den Befragten am Anfang gibt, dieser Gefahr durch einen entsprechenden kurzen Hinweis vorzubeugen, indem es in die Mitteilung, der betreffende Haushalt sei als einer von ca. 10.000 ausgewählt, die Angabe „*zusammen mit einigen benachbarten Haushalten (sog. statistische Klumpenbildung)*“ einfügt. Insoweit bin ich bisher nicht erfolgreich gewesen, allerdings hat es in letzter Zeit bei mir auch keine diesbezüglichen Beschwerden mehr gegeben.

(3) Vereinzelt hat es auch noch aus einem anderen Grund in diesem Zusammenhang Ärger gegeben:
Die sog. *Klumpung* bei der Stichprobenziehung hat den datenschutzrechtlichen Vorteil, dass man zunächst ohne personenbezogene Daten auskommt. Ausgewählt wird nämlich aus einer Datei, die lediglich Ort, Straße, Hausnummer von Wohngebäuden sowie die Gebäudegrößenklasse, gemessen an der Anzahl der Wohnungen im Gebäude, enthält; in der Regel sieben oder acht benachbarte Wohnungen werden eben zum Auswahlbezirk („Klumpen“) zusammengefasst. Der Nachteil ist aber, dass vielfach das Grundstück durch den Erhebungsbeauftragten betreten werden muss. Denn dieser muss mittels Ablesen des Klingelschildes einer Wohnung dieser einen Bewohner-Namen zuordnen und er muss (zweckmäßigerweise) gleich den Umschlag mit der Ankündigungskarte und den anderen Unterlagen in den dazugehörigen Briefkasten werfen.
Was den ersten Vorgang betrifft, bestehen keine datenschutzrechtlichen Bedenken. Denn die Beschaffung von Hilfsmerkmalen bei der Stichprobengewinnung ist, auch als Erhebung bei Dritten, vom Statistikgesetz gedeckt. § 2 Abs. 1 Satz 1 und 2 SächsErwStatG setzt voraus, dass die Erhebungseinheiten unter Verarbeitung von Namens- und Anschrifts-Daten herangezogen werden. Inwieweit insoweit das Recht zum Betreten des Grundstückes besteht, habe ich nicht zu beurteilen. Für den Eingriff in andere Grundrechte als in das auf informationelle Selbstbestimmung bin ich auch dann nicht zuständig, wenn dieser anderweitige Grundrechtseingriff ausschließlich der Beschaffung personenbezogener Daten dient. Ich habe aber, wegen des engen Sachzusammenhangs, dem StaLA geraten, im Hinblick auch auf diesen Punkt möglicher verständlicher Empfindlichkeit Betroffener („Hausfriedensbruch!“) um Schulung der Erhebungsbeauftragten und Aufklärung der Befragten bemüht zu sein.
Das (ordnungsgemäße, auf das Erforderliche beschränkte) Betreten eines Grundstükkes bis zum Briefkasten dürfte von einer konkludent erklärten Einwilligung desjenigen, der den Kasten vorhält bzw. benutzt, gedeckt sein; auch gibt es wohl eine allgemeine Pflicht jedermanns, sich rechtlich erhebliche Erklärungen - auch in schriftlicher Form - zustellen zu lassen - aber auch das ist zwar noch eine statistikrechtliche, aber nicht mehr eine datenschutzrechtliche Frage. (§ 8 Abs. 1 Satz 2

SächsErwStatG verpflichtet die Auskunftspflichtigen, dem Erhebungsbeauftragten gegenüber auf Verlangen bestimmte Angaben - Name, Anschrift und Lage der Wohnung im Gebäude, Anzahl der Haushalte in der Wohnung und Zahl der Personen im Haushalt - *mündlich* zu machen. Das StaLA sieht in dieser Vorschrift zu recht eine Ermächtigungsgrundlage dafür, dass der Erhebungsbeauftragte erforderlichenfalls das Grundstück betritt.)

(4) Ein weiterer Erklärungsbedarf, der bei Reihenbefragungen, wegen der größeren Zeitabstände (jeweils ein Jahr) aber eher beim Mikrozensus als bei der Sächsischen Erwerbsstatistik, auftaucht, ergibt sich, wenn aufmerksame Befragte bemerken, dass sie - aus welchen Gründen auch immer - innerhalb der Befragungsreihe einmal nicht herangezogen worden sind oder dass sie mit Übernahme einer Wohnung - aufgrund der Wohnungsbezogenheit der Stichprobengewinnung - sozusagen die auf dieser ruhende Auskunftslast geerbt haben. Der Verdacht, dass auf solche Weise für die Statistik unnütze oder sogar schädliche Daten erhoben werden, liegt zumindest für den Statistik-Laien nahe. Statistikfachlich ist es offenbar anders. Die Statistiker buchen eine Wohnung nicht auf ihr Verlustkonto, wenn zu dem einen oder anderen Stichzeitpunkt die Befragung des die Wohnung bewohnenden Haushaltes nicht erfolgreich durchgeführt wird. Solche Ungenauigkeiten verschlechterten zwar die Qualität der Gesamterhebung ein wenig, sie führten aber, so hat man mir versichert, nicht zur Wertlosigkeit der übrigen bzw. weiteren Befragungen des die betreffende Wohnung bewohnenden Haushaltes, und sie führten auch insbesondere nicht dazu, dass die Roh-Stichprobe entsprechend ausgeweitet wird, damit am Ende nur vollständige Reihen von Befragungen zur Verfügung stehen und ausgewertet werden.
Dem Sächsischen Erwerbsstatistikgesetz wie dem Mikrozensusgesetz lässt sich nichts Gegenteiliges entnehmen. Anhaltspunkte dafür, dass diese mit solchen Ungenauigkeiten arbeitende, also nicht perfektionistische Vorgehensweise der Statistikverwaltung fachlich zweifelhaft sein könnte, habe ich nicht. Es handelt sich eben um Massen-Verfahren, man schaut so genau also gar nicht in jedem Fall hin, und dass ist datenschutzrechtlich, betrachtet man es genauer, auch beruhigend.

5.7.2 Nutzung personenbezogener Daten zur Erarbeitung einer Statistik für den sog. 2. Versorgungsbericht der Bundesregierung

Seit einem Gesetz von 1989 (Art. 17 BeamtVGÄndG, BGBl. I S. 2218, 2234, geändert durch Art. 19 Abs. 8 des Gesetzes vom 29. Juni 1998, BGBl. I S. 1666, 1689) ist die Bundesregierung verpflichtet, je Wahlperiode des Bundestages einen Bericht vorzulegen, der die jeweils im Vorjahr erbrachten Leistungen zur Versorgung von Beamten ausweist und die in den nächsten 15 Jahren zu erwartenden Versorgungsleistungsverpflichtungen - nicht nur des Bundes, sondern auch der Länder - berechnet.
Probleme ergeben sich dabei insoweit, als das für die Erarbeitung dieses „Versorgungsberichts“ genannten Zahlenwerkes federführende BMI auch Angaben zu Verfahren verlangt, in denen Beamte vorzeitig in den Ruhestand versetzt worden sind. Dazu soll, wie ich erfuhr, als ich von einem Kollegen aus einem anderen Bundesland auf den Vorgang aufmerksam gemacht worden war, der Amtsarzt, der den Bediensteten auf seine Dienstfähigkeit hin untersucht, einen Vordruck ausfüllen,

auf dem zwar nicht der Name des Beamten, aber doch neben dem Grund der Dienstunfähigkeit (Beispiel: psychische und Verhaltensstörungen) so viele weitere Angaben (Geburtsjahr, Geschlecht, Laufbahngruppe u. a.) erfasst werden sollen, dass die entstehenden Kombinationen von Merkmalsausprägungen sehr individuell sind.

Was zunächst die Datenverarbeitung innerhalb der Verwaltung des Freistaates Sachsen betrifft, ist folgendes zu beachten:

(1) Füllt der im Gesundheitsamt tätige Arzt einen der Vordrucke aus, so ist dies datenschutzrechtlich gesehen eine Nutzung der durch die amtsärztliche Untersuchung gewonnenen personenbezogenen Daten des betroffenen Bediensteten. Zweck dieser Datennutzung ist - der Sache, wenn auch nicht der Bezeichnung nach - die Durchführung einer amtlichen Statistik: Es werden Daten über Massenerscheinungen zu Planungszwecken gewonnen, es werden keine Einzelfälle zum Zwecke des Verwaltungsvollzuges untersucht.
Aus diesem Grund ist Statistikrecht anzuwenden, allgemeines Datenschutzrecht allenfalls insoweit, als das Statistikrecht keine Regelungen enthält. Die genannte bundesrechtliche Vorschrift von 1989 stellt für sich keine ausreichende Rechtsgrundlage für die Datenerhebungen dar; sie ist lediglich eine Aufgabenzuweisung und regelt nicht, welche Daten auf welche Weise erhoben und weiterverarbeitet werden sollen.

(2) Eine solche Datennutzung ist nach der den § 12 Abs. 3 Satz 1 SächsDSG insoweit verdrängenden Regelung des § 7 Abs. 1 SächsStatG zulässig, wenn es sich um eine sog. *Statistik im Verwaltungsvollzug* handelt. Voraussetzung ist, dass die Daten im Geschäftsgang derjenigen Stelle anfallen, welche die Daten zu Statistikzwecken nutzt. Das bedeutet umgekehrt: Nur diejenige Stelle, in deren Geschäftsgang die Daten anfallen, darf diese auch nutzen. Diese Voraussetzung ist im vorliegenden Fall offensichtlich erfüllt. Zusätzlich muss die Statistik jedoch („ausschließlich“) der Erfüllung der Aufgaben gerade derjenigen öffentlichen Stelle dienen (unter Einschluss der jeweils übergeordneten Stelle), in deren Geschäftsgang die Daten angefallen sind. Sieht man von dem nicht unproblematischen Ausschließlichkeitsgebot ab, ist die Frage, um den Geschäftsgang welcher Stelle es sich hier genau handelt, entscheidend dafür, wer die Bögen mit den Einzeldatensätzen zur Aggregierung erhalten darf. Ausnahmsweise ist dies hier nicht die dem Gesundheitsamt übergeordnete Stelle, also das Regierungspräsidium (und danach das SMS, gemäß § 2 Abs. 1 Nr. 2 und 1 SächsGDG), sondern diejenige Stelle, die die personalverwaltende Stelle des untersuchten Bediensteten ist. Das folgt daraus, dass bei der betreffenden Tätigkeit der beim Gesundheitsamt angestellte oder als Beamter tätige Arzt nicht in der üblichen Weise hierarchisch eingebunden, sondern aufgrund eines unmittelbar dem betreffenden Gesundheitsamt von der personalverwaltenden Stelle erteilten ‘Auftrages’ tätig wird. Es handelt sich um eine Art (notwendige) Funktionsübertragung innerhalb der Staatsbehörden. Die Rechtslage ist daher insoweit nicht anders als beim Bund, bei dem es den sog. „Amtsärztlichen Dienst der Obersten Bundesbehörden“ gibt. Dementsprechend nennt auch die VwV „Gutachten und Zeugnisse“ des SMS vom 30. April 1998 (SächsAbl. S. 384) in Nr. 2.4.3, unter Verweisung auf § 52 Abs. 1 Satz 1 SächsBG, als Zweck der einzelnen Feststellungen, die in der

amtsärztlichen Untersuchung zum Gesundheitszustand des Bediensteten getroffen werden, dass sie „der personalverwaltenden Stelle eine umfassende Grundlage für ihre Entscheidung“ über die Dienstfähigkeit des Bediensteten bieten sollen.
Somit ist es aufgabengemäß, wenn der Statistik-Bogen (im verschlossenen Umschlag) der personalverwaltenden Stelle mitgeschickt wird, mit der Folge, dass die betreffende Statistik eben nicht im Geschäftsbereich des SMS durchgeführt wird, sondern z. B. für Lehrer im Geschäftsbereich des SMK, für Richter in demjenigen des SMJ.

(3) Auf dieser Grundlage ergibt sich für die praktische Durchführung:
Die personalverwaltende Stelle darf die Bögen, die im statistikrechtlichen Sinne *Einzelangaben* enthalten (wie aus § 16 Abs. 6 BStatG, § 19 Abs. 5 SächsStatG folgt), nur dann unaggregiert an die nächsthöhere Stelle übermitteln, wenn dies für die Durchführung der Statistik, insbesondere auch im Hinblick auf die gesetzlich vorgeschriebene Lieferung von Statistikdaten an den Bund für den Versorgungsbericht, *erforderlich* ist: § 19 Abs. 1 SächsStatG gilt zwar dem Wortlaut nach nicht für Statistiken im Verwaltungsvollzug des Landes, weil § 2 Abs. 1 SächsStatG diese Statistik nicht unter die Landesstatistik im technischen Sinne fallen lässt. Kraft des Grundsatzes der Verhältnismäßigkeit gilt das Gebot der frühestmöglichen statistikunschädlichen Aggregierung jedoch auch insoweit, nämlich als Gebot der frühestmöglichen Anonymisierung gemäß § 1 Abs. 2 Halbsatz 2, a. E., SächsStatG; siehe dazu schon 5/5.7.12 und 4/10.3.1 (S. 172).
Aufgrund dessen darf eine personalverwaltende Stelle, die in einem Berichtszeitraum nur einen einzigen Fall hat, den vom Amtsarzt ausgefüllten Statistik-Bogen so übersenden, wie er ist; dasselbe gälte dann für ein Ministerium im Verhältnis zu dem die Gesamtstatistik für den Freistaat durchführenden SMF, falls es nur einen einzigen Fall in seinem Geschäftbereich gehabt haben sollte.
Ob die Aggregierung auf jeder Stufe von der einzelnen personalverwaltenden Stelle über das für diese zuständige Ministerium bis zum SMF statistikschädlich wäre, hinge davon ab, ob die Statistiken über eine bloße Summierung der Merkmalsausprägungen hinausgehen, also Korrelationen zwischen einzelnen Merkmalsausprägungen ausweisen oder doch jedenfalls ermöglichen soll (Beispiel: Es soll dem Bericht entnommen werden können, ob „psychische und Verhaltens-Störungen“ anteilmäßig eher im höheren oder im gehobenen Dienst, im Schuldienst oder bei Richtern vorkommen.).

Daneben ist die Weitergabe von Daten an den Bund zu betrachten:
Was eindeutig nicht in Frage kam, das war die Übermittlung von Einzeldatensätzen, also insbesondere eine Überlassung der von den Amtsärzten ausgefüllten Vordrucke oder von Ablichtungen derselben, an nicht-statistische Behörden des Bundes, insbesondere das Bundesministerium der Finanzen oder des BMI. Denn aus einer *Statistik im Verwaltungsvollzug* des Freistaates stammende Einzelangaben dürfen den Verwaltungsvollzug des Freistaates außer im Falle des § 7 Abs. 2 SächsStatG, also in Richtung Statistisches Landesamt, nicht verlassen (Umkehrschluss aus § 7 Abs. 2 und auch aus § 19 Abs. 4 SächsStatG). Aber selbst wenn man nach dieser Vorschrift die statistische Aufbereitung dem Statistischen Landesamt überließe, dürfte es Einzelangaben nur gemäß § 19 Abs. 2 SächsStatG dem Statistischen Bundesamt übermitteln. Für die Übermittlung von Einzelangaben an nicht-statistische Behörden, insbesonde-

re auch des Bundes, fehlt es auf jeden Fall an einer Rechtsgrundlage. Denn nicht einmal die Voraussetzungen, die § 19 Abs. 4 SächsStatG für die bloße Übermittlung von Tabellen mit vereinzelten Einzelangaben durch das Statistische Landesamt aufstellt, sind erfüllt.

Aufgrund dessen habe ich zunächst beim SMF erreicht, dass dieses - wie auch andere Bundesländer es getan haben - die Übermittlung von Einzelangaben an das BMI ausgesetzt hat.

Angesichts dieser Schwierigkeiten hat die Bundesregierung dann von den Mehrheitsfraktionen im Bundestag in einem Gesetzentwurf eine Vorschrift unterbringen lassen, die dann später als Artikel 1 Nr. 7 des Gesetzes zur Neuordnung der Versorgungsabschläge vom 19. Dezember 2000 (BGBl. S. 1786) auch als Gesetz verabschiedet worden ist. Anfang November 2000 habe ich im Hinblick auf den Entwurf - es handelt sich um den neuen § 62 a BeamtVG - verfassungsrechtliche Einwände geltend gemacht, an denen ich festhalte. Die Wiederaufnahme der ausgesetzten Übermittlung der durch die Amtsärzte ausgefüllten Erhebungsvordrucke an das BMI halte ich deswegen unverändert für rechtswidrig. Das ergibt sich im Einzelnen aus folgendem:

(a) Zur rechtlichen Einordnung:
Materiell handelt es sich bei der im Gesetz vorgesehenen Datenverarbeitung um Statistik. Denn zur Gewinnung von Erkenntnissen über Massenerscheinungen - statt über Einzelvorgänge - werden personenbezogene Daten („Einzelangaben“ im Sinne der statistikrechtlichen Terminologie) gesammelt, aufbereitet, erhoben, dargestellt und analysiert (vgl. § 1 Satz 1 BstatG, § 1 Abs. 1 Satz 1 SächsStatG). Dass die Datensammlung im vorliegenden Falle nicht mit der für die Statistik weithin typischen weiten, abstrakten Zweckbestimmung stattfindet, sondern ausschließlich für einen bestimmten, gesetzlich vorgesehenen, den gesetzgebenden Körperschaften von der Bundesregierung zu erstattenden Bericht, steht dem nicht entgegen. Dies folgt aus den geltenden Statistikgesetzen. Denn diese sehen sowohl „Statistiken im Verwaltungsvollzug“ (§ 8 Abs. 1 BstatG, § 7 Abs. 1 SächsStatG) als auch solche Ad-hoc-Statistiken vor, die als Primärstatistiken durchzuführen sind - in den Gesetzen als „Erhebungen für besondere Zwecke“ bezeichnet: § 7 BstatG, § 11 SächsStatG. Ein häufiges Beispiel für (Sekundär-)Statistiken im Verwaltungsvollzug, die nur ganz bestimmten einmaligen Erkenntniszwecken dienen, sind Erhebungen zur Beantwortung einzelner parlamentarischer Anfragen. Die betreffenden Datensammlungen werden in der mir bekannten Praxis immer als Statistik in dem Rechtssinne aufgefasst. Die Ähnlichkeit zum Versorgungsbericht liegt auf der Hand.
Die demgegenüber engere Auffassung vom „Wesen der Statistik“, die sich in einem Passus des Volkszählungsurteils des Bundesverfassungsgerichts findet (E 65,1,47), ist in dem Begründungszusammenhang, in dem sie vom Gericht verwendet wird, nämlich der Legitimierung von „Vorratsspeicherung“, also der Freistellung vom „Gebot einer konkreten Zweckumschreibung“ (a.a.O.), gar nicht erforderlich. Vielmehr ist die gerade erwähnte Einordnung konkret zweckbestimmter Statistiken durch die Statistikgesetze verfassungsrechtlich durch den Grundgedanken des Datenschutzes geboten: Die Zweckbindung, die eine Ver-

wendung für den Verwaltungsvollzug jeder Art verbietet, ist unterschiedslos zu gewährleisten, gleichgültig ob die Massenerscheinungen betreffende Verarbeitung der Daten nun zu einem konkreten - Massenerscheinungen betreffenden - Erkenntniszweck stattfindet oder zu noch unbestimmten derartigen Erkenntniszwecken.

Es wäre wenig sinnvoll, neben Statistik und Verwaltungsvollzug noch einen dritten Rechts-Typus mit besonderen Regeln für die Verarbeitung personenbezogener Daten einzuführen, solange nicht erkennbar ist, dass es aus verfassungsrechtlichen Gründen solcher besonderen Regelungen bedarf - wozu dann insbesondere sicher auch gehörte, dass zur organisatorischen Absicherung der Zweckbindung zusätzliche besondere Stellen, eben für die Datenverarbeitung dieses dritten Typs, geschaffen werden müssten!

Kurzum: Es handelt sich allenfalls um eine scheinbare Nicht-Statistik.

(b) Keine Einwände sehe ich zunächst dagegen begründet, dass § 62 a BeamtVG in Satz 1 ausschließlich eine Übermittlung durch die personalverwaltende Stelle an eine Bundesstelle vorsieht: Damit wird zum Ausdruck gebracht, dass nach der Vervollständigung durch den Arzt, als Hilfskraft der personalverwaltenden Stelle (siehe oben unter 2), erst wieder die Bundes-Stelle die „personenbezogenen" Daten, also den Erhebungsbogen-Inhalt, zur Kenntnis nimmt, dass mithin der Umschlag mit dem Erhebungsbogen auf dem Weg zu der Bundes-Stelle nicht geöffnet wird, insbesondere auch nicht im landesweit die Unterlagen sammelnden Ministerium.

(c) Problematisch ist jedoch, dass Datenempfänger das BMI sein soll. Dort müssten dann nämlich zumindest die in § 26 Abs. 1 BStatG vorgesehenen organisatorischen Maßnahmen der Abschottung von den anderen Bereichen gewährleistet werden. Das hat deswegen hier in besonderer Weise zu geschehen, weil anders als bei gewöhnlichen Statistiken im Verwaltungsvollzug keine stufenweise Aggregierung auf dem Wege von der unteren zur obersten Behörde stattfindet, sondern eine unmittelbare Übermittlung der personenbezogenen Daten - „Einzelangaben" - an die mit der Auswertung der Daten betraute Stelle. Meiner Meinung nach gilt das in § 26 Abs. 1 BStatG ausgesprochene Gebot aus verfassungsrechtlichen Gründen, nämlich der Sicherung der (materiellen) Zweckbindung, auch in dem Falle, dass die Regelung, dass ein Bundesministerium Aufgaben der Statistik wahrnimmt (vgl. BVerfGE 65,1 ff., unter C II a. E., S. 51 unten, und IV 1, S. 61) und dabei Einzelangaben zu verarbeiten hat, durch ein Gesetz und nicht lediglich durch Regierungsbeschluss getroffen wird.

Es war vom Bund, auch vom BfD, nicht zu erfahren, ob im BMI eine solche besondere Statistikstelle eingerichtet wird (die man sich sparen könnte, wenn man den im Statistischen Bundesamt vorhandenen Sachverstand dafür eingesetzt, also die Erhebungsbögen dorthin übermitteln und dort auswerten ließe).

(d) Die Angaben, die der neue § 62 a BeamtVG zum Datensatz - statistikrechtlich gesprochen zum Erhebungsprogramm - macht, sind, was Satz 1 Nr. 2 der Vor-

schrift betrifft, zweifellos verfassungswidrig: Die Formulierung, es würden *die erforderlichen Daten zur Person und letzten Beschäftigung des Betroffenen, die zur statistischen Auswertung erforderlich seien*, erhoben, genügt nach heutigen verfassungsrechtlichen Maßstäben nicht mehr. Bei Statistikgesetzen ist es seit langem aus guten verfassungsrechtlichen Gründen Standard, dass sämtliche Merkmale, aus denen sich das Erhebungsprogramm zusammensetzt, aufgelistet werden. Das ergibt sich im Übrigen auch aus § 26 Abs. 2 BStatG im Wege des Umkehrschlusses! Diese Anforderungen gelten auch dann, wenn - wie hier - die Statistik, die geregelt ist, eine Statistik im Verwaltungsvollzug ist (Beispiel: Hochschulstatistikgesetz).

Weder die Existenz der vom BMI bisher gestalteten Vordrucke noch der Bezug auf den Versorgungsbericht, also auf den eingangs genannten Art. 17 BeamtVGÄndG, reichen aus, um, wie die Entwurfsverfasser anscheinend annehmen, mittels des Tatbestandsmerkmals „Erforderlichkeit“ (dessen doppeltes Vorkommen schon die Unsicherheit der Gesetzesverfasser erkennen lässt) das Erhebungsprogramm gesetzlich in der gebotenen Weise bestimmt sein zu lassen.

Erst recht fehlt es damit an der erforderlichen Normenklarheit: Der Umfang des Eingriffs in das Grundrecht auf informationelle Selbstbestimmung ergibt sich gerade nicht „klar und für den Bürger erkennbar“ (vgl. BVerfGE 65,1,44) aus dem Gesetzestext.

An den Anforderungen, die an Bestimmtheit und Normenklarheit zu stellen sind, änderte sich selbstverständlich nichts, wenn man, anders als hier, die Datensammlung nicht als Statistik im Rechtssinne einordnete.

(e) Die festgestellte Unbestimmtheit wird in Satz 2 der Vorschrift, der ein Ersatz-Datenbeschaffungs-Verfahren vorsieht, noch ergänzt: Zwar weitet die Vorschrift das Erhebungsprogramm, jedenfalls bei verfassungskonformer Auslegung, nicht über Satz 1 hinaus aus. Aber es soll eine in verschiedener anderer Hinsicht ausufernde Verarbeitung personenbezogener Daten erlaubt werden:
- Die Daten sollen bei jedermann erhoben werden dürfen, der über sie verfügt. „Stelle“ im Sinne der allgemeinen datenschutzrechtlichen Terminologie ist nämlich bekanntermaßen jedermann (vgl. § 16 Abs. 1 BDSG, § 15 SächsDSG). Das erweckt den Eindruck, dass der Gesetzgeber nicht weiß, welche Fälle er konkret erfassen will.
- Wer erheben dürfen soll, bleibt unbestimmt. Es ist nicht klar, dass die Erlaubnis nur für die nach Satz 1 übermittelnde Stelle gelten soll. Sollte dies der Fall sein, ginge die Erhebung nach Satz 2 der Übermittlung nach Satz 1 gegebenenfalls voraus.
- Wie die auskunftsfähige Stelle gefunden werden soll, bleibt unklar. Sollen bei der Such-Anfrage personenbezogene Daten übermittelt werden dürfen?
- Vor allem aber enthält Satz 2 im Unterschied zu Satz 1 bezeichnenderweise nicht eine Übermittlungserlaubnis, sondern eine Erhebungserlaubnis. Damit ist jedoch gerade im Anwendungsbereich des Arztgeheimnisses, in welchen er-

klärtermaßen die Standardfälle des Tatbestandes des Satzes 2 fallen sollen, noch in keiner Weise entschieden, dass die betreffende „Stelle“, bei der angefragt wird, auch übermitteln dürfte. Soll die Statistik insoweit, also partiell, einwilligungsabhängig, d. h. lediglich auf freiwilliger Grundlage durchgeführt werden?

- Möglicherweise sind Fälle gemeint, in denen der die Dienstunfähigkeit bescheinigende Fachmann ausnahmsweise nicht Bediensteter des betreffenden Dienstherrn ist (etwa psychiatrischer Spezialgutachter), zugleich aber ein besonderes Berufsgeheimnis zu wahren hat. Falls dem so sein sollte, hätte man eine die Tatbestände von Satz 1 und 2 zusammenfassende Formulierung schaffen müssen, welche denjenigen, der eine Dienstunfähigkeit eines Beamten bescheinigt, verpflichtet, den - im Gesetz bestimmten - Datensatz an die zuständige (siehe oben unter c) Bundes-Stelle zu übermitteln.
  Man hätte damit auch für den Amtsarzt eine gegenüber § 7 Abs. 1 SächsStatG, also der Erlaubnis von Statistiken im Verwaltungsvollzug, offenkundigere Offenbarungsbefugnis beschaffen.
  So, wie er Gesetz geworden ist, ist Satz 2 des § 62 a BeamtVG offensichtlich gesetzestechnisch und verfassungsrechtlich missglückt.

Der BfD hat mich - im Unterschied zu einigen Landesbeauftragten für den Datenschutz - mit der nicht schlüssigen Begründung, es handele sich nicht um Statistik im Rechtssinne, bei meinen Einwendungen gegen § 62 a BeamtVG nicht unterstützt.

Dass das SMF dann erklärt hat, es werde die in § 62 a BeamtVG ausgesprochene Verpflichtung zur Datenübermittlung an das BMI erfüllen, kann ich angesichts dessen angemessenerweise nicht im Sinne des § 26 SächsDSG beanstanden. In solchen Fällen bin ich darauf beschränkt, warnend auf die Rechtswidrigkeit der Verfahrensweise hinzuweisen.

5.7.3 Dürfen nach sächsischem Recht amtliche Statistiken mittels rechnergestützter telefonischer Befragung durchgeführt werden?

Ein Verkehrsverbund - der Rechtsform nach ein Zweckverband - hatte das Angebot eines Marktforschungsunternehmens eingeholt, für ihn eine „Potential- und Akzeptanzuntersuchung“ für den ÖPNV im Verbandsgebiet durchzuführen.

Das Neue an dieser Erhebung war, dass die Auskunftserteilenden lediglich *fernmündlich* befragt werden sollten, und außerdem *rechnergestützt*, d. h. so, dass der Interviewer die Daten unmittelbar (im Rahmen des Telefongesprächs) eingeben sollte.
Daraus ergab sich die Frage, inwieweit es einer besonderen, ausdrücklichen gesetzlichen Erlaubnis für Erhebungen bedarf, welche die eine oder andere dieser beiden Eigenschaften haben dürfen.

Was die *Fernmündlichkeit* der Befragung betrifft, so spricht manches dafür, dass die Regelung des § 17 Abs. 4 Satz 1 SächsStatG (= § 15 Abs. 4 BStatG), wonach *bei*

Einsatz von Erhebungsbeauftragten die in den Erhebungsvordrucken enthaltenen Fragen mündlich oder schriftlich beantwortet werden können, einen Umkehrschluss begründet; denn die telefonische - „fernmündliche“ - Beantwortung ist nicht vorgesehen. Wichtiger als diese an den Gesetzeswortlaut anknüpfende Überlegung dürften verfassungsrechtliche Erwägungen sein:
Die fernmündliche Befragung ist in tatsächlicher Hinsicht mit sonst nicht bestehenden Unsicherheiten verbunden. Denn der zu Befragende hat weniger Möglichkeiten zum Nachdenken, zum Nachfragen bei anderen Haushaltsangehörigen oder gar zum Nachsehen in seinen Unterlagen. Außerdem kann er sich der amtlichen Identität des Befragers nicht versichern, jedenfalls dann nicht, wenn dieser ihn anruft (was aus Kostengründen der Normalfall sein dürfte). Daraus lassen sich vier Regeln ableiten:
(A) Im Interesse der Gewinnung zutreffender Daten und somit der Geeignetheit und damit Verfassungsgemäßheit einer Statistik und im Interesse einer Übermittlungssicherheit für den zu Befragenden darf die telefonische Befragungsform niemals obligatorisch sein.
(B) Die telefonische Befragung ist nur erlaubt, wenn sie in dem die Durchführung der Statistik anordnenden formellen Gesetz vorgesehen ist (wegen der Wesentlichkeit dieser Erhebungsmethode; bei Statistiken ohne Auskunftspflicht zusätzlich Übereilungsgefahr bei der Entscheidung für Auskunftserteilung).
(C) Es muss (durch gesetzliches Gebot) gewährleistet sein, dass der zu Befragende vor seiner telefonischen Befragung schriftlich darauf hingewiesen wird, dass er sich auf die fernmündliche Form der Befragung nicht einzulassen braucht.
(Nur auf diese Weise wird das bisherige Schutzniveau aufrechterhalten: Die Möglichkeit ruhiger Überlegung der Entscheidung, ob man sich ausschließlich schriftlich befragen lassen will, lässt sich nur auf diese Weise wahren. Die Regel folgt aus [A] und [B], wenn die Freiwilligkeit gesichert sein soll. Als Forderung findet sie sich im 14. TB des BfD, BT-Drs. 12/4805 vom 27. April 1993 auf S. 129.)
(D) Bei gemischt obligatorisch-freiwilligen Erhebungen (wie dem Mikrozensus) darf die telefonische Befragung nicht vorgesehen werden (weil die erforderliche Bedenkzeit für die Entscheidung beim Übergang von der Pflichtantwort zur freiwilligen Beantwortung nicht gewährleistet ist; notwendiger Übereilungsschutz).
Sind diese Regeln richtig, müssen sie auch für Kommunalstatistiken gelten - mit der Folge, dass es nicht ausreicht, dass die Erlaubnis zur telefonischen Befragung lediglich durch Selbst-Ermächtigung in der Satzung ausgesprochen wird.

Das bedeutet übrigens zugleich: §§ 8 f. SächsStatG und die gesamten sonstigen unzweifelhaft für Kommunalstatistiken geltenden Regelungen des Sächsischen Statistikgesetzes sind keine Beschränkungen der in § 4 SächsGemO eingeräumten Befugnis zur Rechtsetzung durch Satzung. (Genau aus diesem Grunde hat die Gemeinde nicht mangels eines gesetzlichen Verbotes telefonischer statistischer Befragungen die Befugnis, sich selbst durch Satzung zum Einsatz dieses Mittels zu ermächtigen.)

Ein weiterer Sachgrund kommt hinzu: Erfahrungsgemäß werden amtliche Statistiken vom Kommunen mit wesentlicher höherer Wahrscheinlichkeit teilprivatisiert durchgeführt als vom Staat (vgl. 4/5.7.3 und 5/5.7.5). Die Unsicherheit der befragten Personen, ob der Frager, mit dem sie telefoniert - und der sich dann natürlich auch

mit der Nennung des Namens des Unternehmens melden muss, welches die Befragung im offengelegten Auftrag der Kommune durchführt und für welches er tätig ist -, auch wirklich in Durchführung einer (amtlichen) Kommunalstatistik handelt, ist daher noch größer als es schon bei staatlichen Statistiken der Fall ist. Deswegen bedarf die Zulassung fernmündlicher statistischer Befragungen für Kommunalstatistiken noch mehr einer Entscheidung des formellen Gesetzgebers als dies im Falle der staatlichen (amtlichen) Statistik der Fall ist.

Dagegen lässt sich auch nicht mit Erfolg einwenden, dass die Bundesregierung in der Begründung ihres Entwurfes zu § 11 a BStatG (der seit einigen Jahren rechnergestützte Erhebungsverfahren für Bundesstatistiken erlaubt) erklärt hat, die Vorschrift stelle klar, „dass Erhebung [...] auch [...] durch [...] Telefon und Interviews, bei denen die Antworten der Befragten direkt von den die Erhebung durchführenden Statistischen Ämtern der Länder oder des Bundes in einen Computer eingegeben werden", durchgeführt werden dürfen (BR-Drs. 653/95 vom 13. Mai 1995, S. 30). Nicht nur, dass gerade diesen Teil der seinerzeit gegebenen Begründung die Sächsische Staatsregierung in ihre Begründung zu § 13 a SächsStatG, als diese Vorschrift 1999 eingefügt wurde, nicht übernommen hat, bei im Übrigen wortgenauer Übernahme: Vor allem hat der Innenausschuss des Bundestages in seiner Beschlussempfehlung zum oben bereits zitierten 14. TB des BfD (BT-Drs. 13/1663, zitiert nach dem Abdruck in RDV 1995, S. 184 f.) überzeugend darauf hingewiesen, dass die telefonische Durchführung der Erhebung gegenüber ihrer Rechnergestütztheit ein zusätzliches Maß an Grundrechtseingriff aufweist.

Gilt nun diese Notwendigkeit einer besonderen ausdrücklichen Erlaubnis durch formelles Gesetz in gleicher Weise auch für die *Rechnergestütztheit* der Durchführung einer statistischen Erhebung?
Die Tatsache, dass - auf Drängen des BfD - eine entsprechende ausdrückliche Erlaubnis in Gestalt des § 11 a in das BStatG eingeführt worden ist, spricht eher *für* eine solche Notwendigkeit. Zwar hat die Bundesregierung in der Begründung des Gesetzentwurfes die Einführung als bloße Klarstellung bezeichnet, und diesem Vorgehen ist dann insoweit wörtlich auch der sächsische Gesetzgeber im Jahre 1999 bei der Einführung des § 13 a SächsStatG gefolgt. Dieser Meinung war aber vorher schon der Innenausschuss des Deutschen Bundestages in seiner schon genannten Beschlussempfehlung zum 14. TB des BfD a.a.O. mit ausführlicher und überzeugender Begründung entgegengetreten.

Für Kommunalstatistiken wie im vorliegenden Fall kann diese Frage offengelassen werden. § 13 a SächsStatG gehört zusammen mit einigen anderen Vorschriften - §§ 10 f., 13 Abs. 4 Satz 1, 19, 22 Abs. 1 (vgl. § 22 Abs. 2, § 19 Abs. 9!) - zu einer Gruppe von Vorschriften, deren Geltung ersichtlich auf Landesstatistiken beschränkt ist.

Weder das SMI noch das Statistische Landesamt haben Einwände gegen meine Rechtsauffassung erhoben. Man hat mir mitgeteilt, dass die Materialien zum Gesetzgebungsverfahren zu § 13 a SächsStatG keine Anhaltspunkte dafür enthielten, inwieweit sich die Beteiligten Gedanken darüber gemacht haben, warum sie in der Vorschrift nicht neben den Landesstatistiken auch die Kommunalstatistiken erwähnt haben.

Dem Zweckverband musste ich mitteilen, dass die von ihm geplante rechnergestützte telefonische Befragung in der Form einer amtlichen Statistik unzulässig wäre (und telefonische Befragungen sogar für amtliche Landesstatistiken nach geltendem Recht unzulässig wären).
Die beiden Ausweichmöglichkeiten, die ich dem Zweckverband erläutert habe, waren: Entweder konnte er die Erhebung vollständig privatisiert durch das besagte Unternehmen durchführen lassen, also so, dass weder im Einladungsschreiben noch in einem sonstigen Zusammenhang die Auftragserteilung durch den Zweckverband - der nun einmal ein Träger öffentlicher Gewalt ist - in Erscheinung trat, oder aber so, dass als Auftraggeber der Befragung ausschließlich und gemeinschaftlich die im Verbandsgebiet tätigen Verkehrsunternehmen auftraten - ein pfiffiger Vorschlag, den der Zweckverband selbst gemacht hatte. In beiden Fällen wäre der Zweckverband von sämtlichen Vorgaben des Sächsischen Statistikgesetzes frei, brauchte also insbesondere weder das Statistische Landesamt noch den Sächsischen Datenschutzbeauftragten zu beteiligen und brauchte auch keine Satzung. Deswegen entzieht es sich auch legitimerweise meiner Kenntnis, ob der Zweckverband von einer dieser beiden Möglichkeiten Gebrauch gemacht hat.

5.7.4 Erhebung des Alters der Teilnehmer an Volkshochschulkursen

Volkshochschulen sind, auch wenn es auf den ersten Blick verblüffen mag, (kommunale) öffentliche Stellen, mit der Folge, dass gemäß seinem § 2 Abs. 1 das SächsDSG auf sie anwendbar ist.
Ich hatte aufgrund einer Eingabe zur prüfen, ob die Volkshochschule einer sächsischen Großstadt zu Recht auf ihrem Anmeldeformular, auf dem unter anderem die Kurs-Nummer, Name, Anschrift und Bankverbindung anzugeben waren, mit der Bemerkung „Bitte ankreuzen“ und „Für statistische Zwecke“ die Angabe verlangte, zu welcher von sechs vorgesehenen Altersgruppen (z. B. bis 18 Jahre, 19 - 25 Jahre, über 65 Jahre) der sich anmeldende Kursteilnehmer gehöre.
Von dieser Datenerhebung - auf freiwilliger Grundlage - geht nun natürlich die Welt wahrlich nicht unter. Aber: Auch gegenüber Volkshochschulen muss ich darauf dringen, dass bei der Verarbeitung personenbezogener Daten durch sächsische öffentliche Stellen die Gesetze eingehalten werden.

Die Rechtslage war und ist eindeutig: Für die Erhebung des Merkmals „Altersgruppenzugehörigkeit“ durch die Volkshochschule fehlte es an der erforderlichen Rechtsgrundlage.

Auf § 7 Abs. 1 SächsStatG, also die gesetzliche Erlaubnis sog. Statistiken im Verwaltungsvollzug, konnte die Erhebung nicht gestützt werden. Dazu hätten die Daten, wie es das Gesetz ausdrückt, im *Geschäftsgang* der Volkshochschule als öffentlicher Stelle anfallen müssen. Geschäftsgang in diesem Sinne ist die Durchführung von Verwaltungsvorgängen mit Außenwirkung für Einzelfälle - eben der sog. Verwaltungsvollzug. Das bedeutete hier, dass die Volkshochschule die Angabe über die Altersgruppenzugehörigkeit eines Kursteilnehmers benötigte, um den Kursteilnahmevertrag anzubahnen oder durchzuführen. Gerade das aber, so betonte der Deutsche

Volkshochschul-Verband e. V., der neben dem Sächsischen Volkshochschulverband e. V. mir gegenüber auf den Plan gerufen worden war, sei nicht der Fall.

Der Einwand der Volkshochschule und ihrer Verbände, die Kenntnis der Altersgruppenzugehörigkeit bisheriger Kurse sei nützlich für die Erfüllung der Aufgabe, das künftige Kursangebot zu gestalten, geht fehl: Die Ausgestaltung des künftigen Angebotes ist gerade keine Frage des Verwaltungsvollzuges, sondern eine Planungsaufgabe. Das ist etwas völlig anderes als die Abwicklung des Teilnehmer-Verhältnisses: Anmeldung, Gebühreneinzug, vielleicht Ausstellung einer Teilnehmerbescheinigung, Gestellung der Lehrkraft und der Räumlichkeiten in ordnungsgemäßer Weise. Dafür ist allenfalls die Frage der Volljährigkeit von Bedeutung, ansonsten ist das Alter der Teilnehmer insoweit unerheblich.

Mit ein wenig mehr Erfolg hätte sich die Volkshochschule darauf berufen können, dass die Kenntnis der Altersgruppenzusammensetzung der Teilnehmer eines bestimmten Kurses für die konkrete Unterrichtsgestaltung wichtig sei. Insoweit handelt es sich nämlich noch um Verwaltungsvollzug in einem hier möglicherweise maßgeblichen weiten Sinn (unmittelbare oder über die bloße Gestellung mittelbare Erbringung einer Dienstleistung eines Trägers öffentlicher Gewalt gegenüber einem genau begrenzten Personenkreis). Allerdings wäre die praktische Bedeutung sehr gering: Die Alterszusammensetzung seines Kurses überblickt der Dozent zu Beginn der ersten Unterrichtsstunde buchstäblich auf den ersten Blick. Ab dann kann er - falls es nötig und möglich sein sollte - seinen Unterricht entsprechend gestalten. Offenbar geht es darum in der Praxis eben gar nicht.

Mit noch ein wenig mehr Erfolg hätte sich die Volkshochschule darauf berufen können, dass manche Kurse nur mit einer homogenen Alterszugehörigkeit der Kursteilnehmer sinnvoll durchgeführt werden könnten - sodass die Zulassung zu dem Kurs von bestimmten Altersgegebenheiten abhängig gemacht werde. Nur: Letzteres hat die Volkshochschule gerade ausdrücklich als Erhebungszweck ausgeschlossen, von ersterem war nie die Rede. Man hat sich ausschließlich auf die Planung des zukünftigen Kursangebotes und auf Statistik überhaupt als Erhebungszweck gestützt und damit in keiner Weise erkennbar gemacht, dass man nicht eine Primärstatistik durchführen, sondern durch Verwaltungsvollzug angefallende personenbezogene Daten im Wege der Sekundärstatistik zu statistischen Zwecken auswerten wolle, wie es § 7 Abs. 1 SächsStatG voraussetzt.

Es handelt sich demnach bei der Erhebung des Merkmals „Altersgruppenzugehörigkeit“ rechtlich von vornherein um - amtliche - Statistik.
Eine solche bedarf nach dem SächsStatG - wie nach vielen, aber nicht allen allgemeinen Statistikgesetzen in Deutschland - auch dann einer Rechtsvorschrift als Grundlage, wenn die Erhebung ohne Auskunftspflicht, also mit voller Freiwilligkeit der Beantwortung, durchgeführt wird.
Dass der Deutsche Volkshochschulverband e. V. bundesweit ein mit allen Landesverbänden abgestimmten Erhebungsbogen verwendet, ersetzt keine Rechtsgrundlage und begründet insbesondere auch keine rechtliche Verbindlichkeit für den einzelnen kommunalen Volkshochschul-Träger.

5.7.5 Statistikrechtliche Meldepflichten im Falle der Veräußerung land- bzw. forstwirtschaftlicher Flächen

Durch eine Anfrage aus Fachkreisen erfuhr ich, dass die BVVG (Bodenverwertungs- und -verwaltungs GmbH), die für Rechnung des Bundes ehemals volkseigene land- und forstwirtschaftlich genutzte Flächen veräußert, sich aus datenschutzrechtlichen Gründen gehindert gesehen habe, dem StaLA im Falle entsprechender Vertragsabschlüsse Namen und Anschriften Beteiligter zu nennen, falls der Notar nicht in den Vertrag eine dahingehende Ermächtigung durch die Vertragsparteien aufgenommen hatte.
Von dieser Voraussetzung war die betreffende Datenübermittlung an das StaLA bzw. die Erhebung durch diese von Rechts wegen jedoch keineswegs abhängig; das StaLA hatte aber auch keinen Fehler gemacht, wenn es es für sinnvoll erklärt hatte, dass es die Meldung statt von den Vertragsparteien vom beurkunden Notar erhielt; dies ergibt sich im Einzelnen aus folgendem:

Bei der Veräußerung land- oder forstwirtschaftlich genutzter Flächen entsteht - auch wenn die BVVG Veräußerer ist - gegenüber dem StaLA dann, wenn der Erwerber nicht der bisherige Pächter ist, also im Falle des Bewirtschafterwechsels, im Rahmen der sog. Bodennutzungshaupterhebung nach dem Agrarstatistikgesetz, sofern der Sitz des übernehmenden Betriebes im Freistaat Sachsen liegt, eine statistikrechtliche Meldepflicht im Umfange des folgenden Datensatzes:
- Abgebender Betrieb:
  Vor- und Familienname sowie Anschrift des Betriebsinhabers, ersatzweise des veräußernden Eigentümers
- Übernehmender Betrieb:
  Vor- und Familienname sowie Anschrift des Betriebsinhabers, ersatzweise des Erwerbers
- Flächengröße.

Der Umfang des Datensatzes ergibt sich aus § 8 Abs. 1 Nr. 2, § 92 Abs. 1 Nr. 3 AgrStatG. Die Pflicht, diese sog. Veränderungsmeldung an das StaLA zu erstatten, trifft beide Vertragsteile, genauer gesagt „Inhaber oder Leiter“ des abgebenden und des übernehmenden Betriebes und Unternehmens. Die BVVG ist als Veräußerer nicht unbedingt ‘Inhaber oder Leiter des abgebenden Betriebes’, denn die Flächen sind in der Regel verpachtet, aber sie ist - so sieht es auch der für die BVVG zuständige Bundesdatenschutzbeauftragte - im Sinne der genannten Vorschrift *abgebendes Unternehmen.* Daher trifft die BVVG auch unmittelbar, nicht etwa nur aufgrund einer Übernahme der Erfüllung der Pflicht des bisherigen Verpächters oder des Erwerbers, die genannte Meldepflicht.
Die Auskunftspflicht gemäß § 93 Abs. 2 Nr. 1, 1. Fall AgrStatG erfasst jeweils auch die Angaben zum Partner des Betriebswechsels, also zum Vertragspartner, mithin nicht nur die Angaben zur eigen Person bzw. zum eigenen Betrieb.

Keine Einwände bestehen datenschutzrechtlich dagegen, wenn die Vertragsparteien den beurkundenden Notar damit beauftragen, die statistikrechtliche Meldepflicht für sie zu erfüllen. Zwar erhält das Statistische Landesamt auf diese Weise ein zusätzliches Datum, nämlich die Angabe, welcher Notar den Veräußerungsvertrag beurkun-

det hat. Solange die Behörde es jedoch nicht darauf anlegt, dieses zusätzliche Datum zu bekommen, fehlt es am zielgerichteten Beschaffen dieses Datums und darum (vgl. Auernhammer, Rdnr. 26 zu § 3 BDSG) am Erheben dieses Datums. (Zu dieser Erhebung wäre das Statistische Landesamt mangels Nennung dieses Merkmals im Agrarstatistikgesetz nicht befugt). Die von der BVVG vertretene Auffassung, das Statistische Landesamt habe sogar Abschriften des vollständigen Vertrages verlangt, erwies sich als Missverständnis.

5.8 Archivwesen; Altdaten

5.8.1 Zum Verhältnis zwischen archivrechtlicher Anbietungspflicht und Löschungspflichten

Am Beispiel von Vorschriften, welche die Entfernung von Unterlagen aus Personalakten von Beamten sowie die Vernichtung (Löschung) dieser Unterlagen anordnen, ist unter den Datenschutzbeauftragten des Bundes und der Länder die Frage erörtert worden, wie sich solche - namentlich auch Disziplinarvorgänge betreffenden - Vorschriften zu den archivrechtlichen Anbietungspflichten verhalten.

Im Ergebnis hat sich herausgestellt, dass es in Bund und Ländern sehr unterschiedliche Regelungen gibt.

Aus dem Sächsischen Archivgesetz lässt sich zu der Frage nichts entnehmen, ob das Archivgesetz oder die das Löschungsgebot enthaltenden Vorschriften den Vorrang genießen.

Demgegenüber lässt das Hamburgische Archivgesetz ausdrücklich die Anbietungspflicht gegenüber den Löschungspflichten - nicht nur gegenüber denjenigen des Dienst- und Arbeitsrechtes - zurücktreten (§ 3 Abs. 2 Satz 2 HmbArchivG).

Andere Länderarchivgesetze schreiben ausdrücklich vor, dass dem zuständigen Archiv auch diejenigen nicht mehr zur Aufgabenerfüllung benötigten, personenbezogene Daten enthaltenden Unterlagen anzubieten sind, die nach anderen Rechtsvorschriften des Landesrechts vernichtet werden müssten (d. h. deren personenbezogene Daten gelöscht werden müssten). So ist es nach § 4 Abs. 2 Nr. 1 BbgArchivG. § 8 Abs. 2 Nr. 1 SaarlArchivG erfasst sogar auch die bundesrechtlichen Löschungsgebote.

Das ist unter Datenschutzgesichtspunkten verfassungsrechtlich unbedenklich, wenn die anliefernde Stelle nicht wieder auf das Archivgut zurückgreifen und es im Zusammenhang mit der ursprünglichen Aufgabenerfüllung weiter verwenden darf, wenn also das Archivrecht zusätzlich vorsieht, dass solche Unterlagen bzw. Daten von Behörden, insbesondere auch von der Stelle, die sie abgegeben hat, nicht vor Ablauf der dem Persönlichkeitsrechtsschutz dienenden archivrechtlichen Schutzfristen genutzt werden dürfen. (Das Argument, das aus der Fürsorgepflicht des Dienstherrn gegenüber dem Bediensteten folgende Gebot, den Bediensteten von seiner Belastung durch überholte Vorwürfe zu befreien, werde verletzt, ist daher dann ohne Grundlage.)

Eine solche Regelung spricht auch Sachsen in § 10 Abs. 3 SächsArchivG aus. Es heißt dort:

> (3) Die in Absatz 1 festgelegten Schutzfristen gelten auch bei der Benutzung durch öffentliche Stellen. Für die abgebenden öffentlichen Stellen gelten die Schutzfristen des Absatzes 1 nur für Unterlagen, die bei ihnen aufgrund besonderer Vorschriften hätten gesperrt, gelöscht oder vernichtet werden müssen.

Damit wird in Satz 2 mittelbar ausgesprochen, was die zuletzt genannten Vorschriften ausdrücklich bestimmen. Denn Satz 2 setzt ja voraus, dass die Anbietungspflicht auch in denjenigen Fällen besteht, in denen das die Löschung vorschreibende besondere Gesetz im Unterschied zu den allgemeinen Datenschutzgesetzen nicht selbst ausdrücklich die Löschungspflicht gegenüber der Anbietungspflicht zurücktreten lässt, wie das etwa § 20 Abs. 8 BDSG (durch das Fehlen der Verweisung auf § 2 Abs. 7 BArchG) und § 19 Abs. 3 SächsDSG tun.

Eine solche ausdrückliche Zurücktretens-Regelung enthält jetzt auch § 489 Abs. 9 StPO in der Fassung des StVÄG 1999 (entspricht § 490 in der Entwurfsfassung). Möglicherweise soll allerdings mit der Formulierung „*besondere* archivrechtliche Regelung“ gerade zur Voraussetzung gemacht werden, dass das Archivrecht die Anbietungspflicht ausdrücklich auch für den Fall ansonsten bestehender Löschungspflichten vorsieht; die amtliche Begründung (BR-DS. 65/99 vom 5.2.1999) äußert sich jedoch (auf Seite 73) weniger anspruchsvoll, wenn sie zusammenfassend folgert, *Absatz 9 stelle somit klar, dass § 490 keine archivrechtlichen Regelungen vorgehende Rechtsvorschrift über die Vernichtung von Unterlagen sei.*

Mit Regelungen, welche der archivrechtlichen Anbietungspflicht den Vorrang gegenüber Löschungspflichten einräumen, also im Grunde mit jeder Erlaubnis der Archivierung von Unterlagen mit personenbezogenen Daten, ist aus verfassungsrechtlichen Gründen allerdings vorausgesetzt, dass der in der fortgesetzten Speicherung im Archiv liegende Grundrechtseingriff durch ein Allgemeininteresse gerechtfertigt wird, welches von Verfassungs wegen grundsätzlich den nötigen Rang, das nötige Gewicht, gegenüber dem Grundrecht auf informationelle Selbstbestimmung hat, in das eingegriffen wird. Die durch das Archivgut verkörperten Erinnerungs- und Erkenntnismöglichkeiten für spätere Generationen müssen daher Verfassungsrang haben. Dieser ist vermutlich aus der Wissenschaftsfreiheit, in Sachsen wohl zusätzlich auch aus der Bestimmung herzuleiten, dass der Freistaat „der Kultur verpflichtet“ ist (Art. 1 SächsVerf).

Einen demgegenüber anderen Weg scheint der Gesetzgeber in § 4 Abs. 1 BArchG eingeschlagen zu haben: Während § 2 Abs. 7 BArchG das Archivrecht, namentlich die Anbietungspflicht, gegenüber dem allgemeinen datenschutzrechtlichen Löschungsgebot zurücktreten lässt, welch letzteres jedoch dann gemäß § 20 Abs. 8 BDSG wiederum, wie oben angesprochen, hinter der Anbietungspflicht zurücktritt (vgl. am klarsten Bergmann/Möhrle/Herb Rdnr. 102 zu § 20 BDSG), sollen demgegenüber anscheinend solche Löschungsgebote endgültig der Anbietungspflicht vorgehen, die als Rechtsansprüche des Betroffenen statt als Pflichten der Behörde ausgestaltet sind. Diese gesetzliche Unterscheidung leuchtet kaum ein: Vom bloßen Wort-

laut her sind auch die speziellen Regelungen des Disziplinarrechtes (z. B. § 119 Abs. 1 Satz 1 BDO, § 112 Abs. 2 SächsDO) oder des § 45 Abs. 1 und 2 BZRG, aber auch die Löschungsvorschriften in § 489 Abs. 2 und 4 StPO (in der Fassung des StVÄG 1999) sowie in § 29 StVG als Löschungspflichten der Behörde, nicht als Ansprüche des Betroffenen formuliert. Und es dürfte, umgekehrt, nicht angehen, dem Betroffenen, dessen Daten nach einem allgemeinen Datenschutzgesetz zu löschen wären, einen dahingehenden Anspruch gegen den Rechtsträger der speichernden Stelle, also ein subjektives öffentliches Recht (wie es ja auch im Falle des Auskunftsrechtes besteht), zu versagen.

Vermutlich ist die Fragestellung allerdings kaum von praktischer Bedeutung, weil die Archivare an Eintragungen im Verkehrszentralregister, im Bundeszentralregister oder an gewöhnlichen Disziplinarverfahren nicht interessiert sind. Anders könnte es sich allerdings mit der Archivwürdigkeit der Personalakten prominenter Beamter verhalten: Unterlagen über beauftragte oder sogar durchgeführte Disziplinarverfahren gegen leitende Beamte oder z. B. angeblich disziplinarrechtliche - Ermittlungen im Bundeskanzleramt wegen möglicher Aktenunterdrückung können im Einzelfall durchaus von bleibendem Interesse sein.

Eine pragmatische Lösung wäre also vielleicht ein auf Disziplinarverfahren bezogener genereller Verzicht der Archivare auf die Erfüllung der Anbietungspflicht, von dem Personalvorgänge leitender Beamten oder bestimmter prominenter Dienststellen i. V. m. bestimmten Arten von Dienstvergehen (nämlich den stärker amtsausübungsbezogenen) ausgenommen wären.

Ich habe die sächsische Staatsregierung - zuständig ist das SMI, sowohl für das Archivwesen als auch das öffentliche Dienstrecht - gebeten, zu meiner Rechtsauffassung Stellung zu nehmen und gegebenenfalls Vorschläge für eine praktische, ebenso arbeits- wie datenverarbeitungssparsame Handhabung zu unterbreiten. Bis jetzt steht eine Antwort noch aus. Ich werte das als grundsätzliche Zustimmung. Wird nichts archiviert, ist das kein Datenschutzverstoß, sondern nur ein Problem der Archivverwaltung.

5.8.2 Daten über DDR-Kinderkrippen-Kinder nunmehr dort, wo sie von Gesetzes wegen hingehören

Immer noch geht es immer wieder einmal um den ordnungsgemäßen Verbleib von DDR-Altdaten. Manchmal ist es nicht leicht, denjenigen zu finden, der die Last, die Unterlagen ordnungsgemäß aufzubewahren und auch die Dritten zustehenden Auskünfte zu erteilen, zu übernehmen hat. Und es ist zu entscheiden, inwieweit die Unterlagen zu vernichten sind.

Ein spektakulärer Fall war Folgender:

In einer öffentlichen Veranstaltung, in der über gesteigerte Gewaltbereitschaft Jugendlicher als mögliche Spätfolge des vergesellschafteten Aufziehens von Kleinst- und Kleinkindern in der DDR diskutiert wurde, berief sich, wie mir durch eine

Presseveröffentlichung bekannt wurde, ein ehemaliger leitender Mitarbeiter des DDR-Instituts für Hygiene des Kinder- und Jugendalters, das in Leipzig eine Untersuchungsstelle für Kinder-Krippen unterhalten hat, auf die 10.000 Berichte über Krippen-Kinder, die er bei sich zu Hause - in der Leipziger Gegend - aufbewahre, mittels deren er forsche und die aus Untersuchungen des Verhaltens von Kindern und Erziehern eben durch das genannte Institut angefallen waren.

Diese Berichte - rund 25.000 Blatt - hatte der Betreffende im Zusammenhang mit der Auflösung des Institutes gegen Zahlung eines zweistelligen DM-Betrages ausgehändigt bekommen, und er hatte sie nicht gemäß § 35 Abs. 2 SächsDSG gemeldet.

Im Hinblick auf die Strafvorschriften des § 35 Abs. 5 Nr. 1 bzw. 2 SächsDSG habe ich dann bei der zuständigen Staatsanwaltschaft Leipzig Strafanzeige gestellt. Im Zuge des Ermittlungsverfahren beschlagnahmten Staatsanwaltschaft und Polizei die Unterlagen - ein halbes Dutzend große Umzugskartons voll.

Als ich zur Stellungnahme aufgefordert wurde, habe ich mir die beschlagnahmten Unterlagen zusammen mit den Ermittlungsakten auf der Grundlage von § 24 SächsDSG übersenden lassen und mich davon überzeugt, dass die Angaben in den Unterlagen personenbezogen waren (Namen oder PKZ) und, wie das bei Untersuchungen von Psychologen auch nicht anders sein kann, im starken Maße die Persönlichkeit der Kinder kennzeichneten, aber auch recht persönliche Informationen über deren Eltern enthielten. Hinzu kamen Unterlagen mit Personalaktenqualität, die sich auf Beschäftigte des Instituts bezogen (z. B. auch zur politischen Einstellung).

Es war klar, dass die Unterlagen dem zuständigen Archiv angeboten werden mussten. Die Daten betrafen zu dreiviertel Kinderkrippen außerhalb des heutigen Freistaates Sachsen. Das genannte Institut war eine zentrale Einrichtung der DDR mit Stammsitz in Berlin-Ost. Daher war gemäß § 2 Abs. 8 BArchG das Bundesarchiv für die Entscheidung über eine Archivierung zuständig. Diesem habe ich die beschlagnahmten Unterlagen unmittelbar angeboten. Im Einvernehmen mit dem Archivreferat des SMI hat das Bundesarchiv dann den überwiegenden Teil der Unterlagen, weil ihnen bleibender Wert zuzumessen sei, archiviert.

Der ehemalige Inhaber der Unterlagen hat der Übergabe an das Bundesarchiv zugestimmt und von diesem - natürlich nur nach Maßgabe der dem Persönlichkeitsrechtsschutz dienenden archivrechtlichen Regeln - erleichterte Nutzungsbedingungen zugesichert bekommen.

Das strafrechtliche Ermittlungsverfahren ist dann mit Zustimmung des Gerichtes gemäß § 153 Abs. 1 StPO, also wegen geringer Schuld, eingestellt worden. Weil der Beschuldigte im Schriftwechsel mit etlichen Stellen des Bundes und auch des Freistaates sowie mit dem sogenannten Deutschen Jugendinstitut auf den Datenbestand und dessen Auswertung durch ihn hingewiesen hat, war der Tatbestand der Verheimlichung gemäß § 35 Abs. 5 Nr. 1 SächsDSG nicht erfüllt. Vielleicht auch deswegen hat im Hinblick auf die Unterlassung der Meldung die Staatsanwaltschaft wegen geringer Schuld das öffentliche Interesse an der Verfolgung verneint. Dagegen habe

ich keine Einwände erhoben. Aber immerhin: Ohne § 35 SächsDSG hätte man es kaum geschafft, die Unterlagen dorthin zu bringen, wo sie hingehören, wenn man sie nicht überhaupt vernichtet, nämlich in ein staatliches Archiv.

5.8.3 Psychiatrische Unterlagen in falschen Händen: Strafrechtliches Nachspiel im Hinblick auf § 35 SächsDSG

In dem Fall von 6/5.8.1 habe ich, wie berichtet, mich seinerzeit auch mit einer Strafanzeige an die Staatsanwaltschaft gewandt. Diese hat Anklage wegen Verstoßes gegen § 35 Abs. 5 Nr. 1 SächsDSG (und wegen Diebstahls) erhoben, im November 2000 ist es zur mündlichen Verhandlung gekommen. Auch in diesem Falle (vgl. vorstehend 5.8.2) hat das Gericht keine Strafe verhängt. Aber es hat das Verfahren nur nach § 153 a Abs. 2 StPO eingestellt: Der Angeklagte hat DM 5.000,00 zahlen müssen. Es dürfe, gerade auch für die Petentin, dem Rechtsfrieden gedient haben, dass der Arzt nicht ungeschoren davongekommen ist.

5.8.4 Auskünfte aus Archiven als Ersatz für Melderegisterauskünfte?

Das Archiv einer sächsischen Universität bat mich um Rat wegen mehrerer Anfragen, in denen nach Daten, vor allem Anschriften, von Personen gefragt werde, die als Ausländer, vor allem aus Afrika, dem Nahen Osten und Kuba, hier studiert oder geforscht haben. Die Fragen würden vor allem von Frauen gestellt, welche ihren Kindern durch Angabe einer Anschrift im Ausland etwas über deren (angebliche) Abstammung mitteilen wollten, oder durch solche (angeblichen) Kinder eines bestimmten Ausländers selbst.

Es gibt keine Rechtsvorschrift, die es dem Universitätsarchiv erlaubt, die seinerzeit angegebene Heimatanschrift oder ähnliche Daten solchen Interessenten zur Verfügung zu stellen.
Maßgeblich ist das SächsArchivG (§ 14). Die dem Persönlichkeitsrecht-Schutz dienenden Schutzfristen sind in diesen Fällen noch nicht abgelaufen. Denn ist unbekannt, ob der Betroffene verstorben ist, dauert die Schutzfrist 100 Jahre ab seiner Geburt; diese Vorschrift gilt natürlich auch für DDR-Altdaten, um die es sich hier im Wesentlichen handelt - § 10 Abs. 2 Satz 2 SächsArchivG e contrario.
Auch wenn die Betroffenen an der Universität angestellt waren, ändert das nichts: Ihre damals angegebene Heimatanschrift oder ähnliche private Umstände gehören nicht zur Amts-Ausübung im Sinne von § 10 Abs. 2 Satz 3 SächsArchivG.
Ein Auskunfts- oder Einsichts-Anspruch nach § 6 Abs. 1 bzw. 3 SächsArchivG scheidet aus. Er besteht nur für die auf die eigene Person, d. h. die eigenen persönlichen oder sachlichen Verhältnisse (§ 3 Abs. 1 SächsDSG) bezogenen Angaben. Die seinerzeit angegebene Heimatanschrift eines (angeblichen) ehemaligen Partners oder Erzeugers des Antragstellers (Auskunftsbegehrenden) gehört nicht mehr zu den zu *dessen Person* gespeicherten Daten. Zwar wäre die Eigenschaft als Elternteil ein sog. Datum mit Doppelbezug, das Aussagen sowohl über seine persönlichen Verhältnisse als auch des Kindes trifft; für die seinerzeit angegebene Heimatanschrift eines Vaters

gilt dies jedoch nur noch in einem Maße, das so schwach ist, dass es für den Auskunftsanspruch nicht mehr ausreicht. Für die Staatsbürgerschaft oder Volkszugehörigkeit könnte anderes gelten. Nur fehlt es dann vermutlich immer noch an der Gewissheit über die Vaterschaft. Ohne solche Gewissheit steht nicht mit der nötigen Sicherheit fest, dass es sich um ein Datum auch des (der) Auskunftsbegehrenden handelt. Entsprechende Nachweise werden aber nicht vorgelegt.

Über die Universitätsarchive kommen die Betreffenden somit nicht an die gewünschten Daten. Es bleibt jedoch der Weg über eine Melderegisterauskunft. Gemäß § 5 Abs. 1 Nr. 12 SächsMG speichert die Meldebehörde gegenwärtige, frühere und künftige Anschriften. Nach § 32 Abs. 1 Nr. 4 SächsMG darf die Meldebehörde Auskunft über Anschriften einzelner bestimmter Einwohner erteilen. Diese Befugnis der Meldebehörde ist an keine weiteren Voraussetzungen gebunden. Eine Auskunft über frühere Anschriften des Betroffenen darf die Meldebehörde gemäß § 32 Abs. 2 Nr. 5 SächsMG allerdings nur dann erteilen, wenn der Antragsteller ein berechtigtes Interesse glaubhaft macht; das sollte ihm wohl gelingen.

Man kann das Ergebnis verallgemeinern: Wenn jemand mit der Behauptung, mit einem Dritten etwas zu tun zu haben, von einer öffentlichen Stelle dessen Anschrift haben möchte, dann sind die Meldebehörden zuständig und ist Melderecht maßgeblich. Archivierte Verwaltungsunterlagen sind dafür nicht zu nutzen. Die Anfragenden sollten daher an die Meldebehörden verwiesen werden.

5.8.5 Zugang zu Wirtschaftsdaten aus der DDR-Statistik

Ein Petent arbeitet an einer Darstellung der Geschichte eines DDR-Kombinates. Zu diesem Zweck hatte er vom StaLA sog. Leistungskennziffern dieses Kombinates aus den Sechziger Jahren haben wollen, weil die Bestände in den Archiven insoweit eine Lücke aufwiesen. Das StaLA hat unter Berufung auf *datenschutzrechliche Gründe* abgelehnt - zu unrecht. Datenschutzrechtlich steht nämlich einer Übermittlung von Einzelangaben aus der DDR-Statistik, die sich auf Kombinate, Betriebe, Genossenschaften u. ä. Einrichtungen der DDR-Wirtschaft beziehen, durch das StaLA an Private, insbesondere auch zu deren Forschungs- und sonstigen Darstellungs-Zwekken, nichts entgegen. Die Gründe, die ich dem StaLA dargelegt habe, sind folgende:

(1) Es ist kein Geheimhaltungsgebot (Übermittlungs-Verbot) ersichtlich, welches für solche Daten bestünde. Denn es gibt keine fortgeltende DDR-Statistik-Geheimnis-Vorschrift. Auch ist das geltende Statistikrecht, namentlich §§ 18 f. SächsStatG, auf Statistiken, die auf der Grundlage von DDR-Recht durchgeführt worden sind, nicht anwendbar. Schließlich könnten auch nach einer förmlichen Archivierung solche DDR-Geheimhaltungsvorschriften nicht im Rahmen des § 5 Abs. 7, 2. Halbs. SächsArchivG fortgelten.

(2) Auch ein etwaiger Bezug der Daten auf bestimmte (bestimmbare, § 3 Abs. 1 SächsDSG) natürliche Personen, nämlich diejenigen, die seinerzeit in den betreffenden Einrichtungen der DDR-Staatswirtschaft tätig gewesen sind, änderte daran nichts. Es gäbe dann zwei Möglichkeiten:

(2.1) Entweder ist es noch Aufgabe des StaLA, personenbezogene Daten aus der DDR-Statistik aufzubewahren. In diesem Falle - den ich für äußerst fraglich halte - wäre die vom Petenten gewünschte Datenübermittlung nach § 15 Abs. 1 Nr. 1 i. V. m. § 12 Abs. 2 Nr. 4 SächsDSG erlaubt. Es handelt sich vorliegend um ein wissenschaftliches Interesse, an welches keine größeren Anforderungen zu stellen sind, weil das Interesse der Betroffenen - des genannten Personenkreises der leitenden „Kader" - aus nachfolgend dargelegten Gründen insoweit keinen Schutz verdient.

(2.2) Wenn hingegen, was meiner Auffassung nach der Fall ist, die Aufbewahrung personenbezogener DDR-Daten nicht zu den gesetzlich vorgesehenen Aufgaben des StaLA gehört, ergibt sich die Übermittlungs-Erlaubnis aus § 15 Abs. 1 Nr. 2 SächsDSG. Denn der betreffende Personenkreis hat kein schutzwürdiges Interesse am Unterbleiben der Übermittlung. Dabei bedarf es der Anhörung und gegebenenfalls Unterrichtung der betreffenden Personen, die § 15 Abs. 3, 1. Halbs. vorschreibt, gemäß dem 2. Halbsatz nicht, weil sie zu einem das Grundrecht auf informationelle Selbstbestimmung im Verhältnis zur Übermittlung als solcher unverhältnismäßig belastenden Ausmaß an Verarbeitung personenbezogener Daten führen müssten: Die Statistikverwaltung müsste erst ermitteln, welche Personen seinerzeit verantwortlich in der betreffenden Einrichtung der DDR-Wirtschaft tätig gewesen sind und diesen unter Verwendung von Melderegister-Daten 'nachspüren'. Der Grundrechtseingriff wäre demnach wesentlich schwerwiegender als die bloße Übermittlung; denn es handelt sich ausschließlich um Amtsträger-Daten, für die im Ergebnis Grundrechtsschutz (Datenschutz) nicht stattfindet: Dies ergibt sich aus dem Verfassungsrecht, welches seinen Niederschlag in statistikrechtlichen und archivrechtlichen Vorschriften gefunden hat. So ergibt sich aus § 15 FPStatG, dass für Betriebe und Unternehmen, an denen Bund, Länder oder kommunale Körperschaften mehr als 50 v. H. des Nennkapitals oder Stimmrechtes halten, *die statistischen Ergebnisse* auf der Ebene der Erhebungseinheit veröffentlicht werden dürfen (i. V. m. § 2 Abs. 3 FPStatG; vgl. zu der Thematik 8/5.7.1), und in § 10 Abs. 2 Satz 3, 2. Halbs. i. V. m. § 4 Abs. 2 Satz 2 SächsArchivG ist geregelt, dass *Mitarbeiter der ehemaligen staatlichen oder wirtschaftsleitenden Organe, der Kombinate, Betriebe, Genossenschaften und Einrichtungen aus der Zeit zwischen dem 8. Mai 1945 und dem 2. Oktober 1990* als Amtsträger, soweit es um die Ausübung ihrer Ämter geht, nicht in den Genuss der persönlichkeitsschützenden archivrechtlichen Schutzfristen (§ 10 Abs. 1 Satz 3 und 4 SächsArchivG) kommen.

Das SMI habe ich in dessen Eigenschaft als oberste Aufsichtsbehörde für das staatliche Archivwesen (§ 3 Abs. 2 Satz 1 SächsArchivG) darauf hingewiesen, dass nach einer förmlichen Archivierung derartiger Unterlagen (vgl. § 5 Abs. 2 SächsArchivG) die Rechtslage klarer, zumindest einfacher wäre.

Das StaLA hat meinen Ausführungen nicht widersprochen und dem Petenten die gewünschten Daten zukommen lassen.

5.9 Polizei

5.9.1 Gesetz zum Schutz der Bevölkerung vor gefährlichen Hunden

Wäre ich an dem Entwurf des am 1. September 2000 in Kraft getretenen Gesetzes beteiligt worden, hätten nachstehende datenschutzrechtlichen Mängel rechtzeitig verhindert werden können:

1. Nach § 7 Abs. 1 GefHundG hat der bisherge Halter eines Pitbull-Terriers, American-Staffordshire-Terriers oder Bullterriers bei dessen Veräußerung den Namen und die Anschrift des neuen Halters anzugeben. Die mit dieser Bestimmung einhergehende Datenerhebung bei Dritten (der bisherige Hundehalter ist gegenüber dem Erwerber Dritter) halte ich grundsätzlich gemäß § 11 Abs. 4 Nr. 1 SächsDSG für zulässig, jedoch nur, soweit sich der neue Hundehalter innerhalb der Grenzen des Freistaates Sachsen aufhält. Bei einer „Migration“ des Hundes nach außerhalb endet die Zuständigkeit sächsischer Behörden mit der Folge, dass die Daten des neuen Hundehalters nicht erhoben werden dürfen und zur Aufgabenerfüllung auch in keiner denkbaren Weise erforderlich sind (gegen eine nichtpersonenbezogene Frage nach dem Verbleib des Hundes ist nichts einzuwenden). Trotzdem werden Verstöße gegen § 7 Abs. 1 GefHundG gemäß § 12 Abs. 1 Nr. 10 GefHundG als Ordnungswidrigkeit mit Geldbuße geahndet und begründen zudem die Unzuverlässigkeit nach § 9 Abs. 2 Nr. 4 GefHundG.

   Im Übrigen macht die problematische Datenerhebung - auch bei Abgabe des Hundes innerhalb Sachsens - nur dann Sinn, wenn entsprechende Kontrollmitteilungen an die nunmehr zuständige Behörde erfolgen würden, für die es jedoch ersichtlich keine Rechtsgrundlage gibt (auf Art. 33 SächsVerf sowie auf das Urteil des Bundesverfassungsgerichts vom 15. Dezember 1983 - BVerfGE 65, 44 bis 46 sei hingewiesen).

   Es ist hier wie so oft: Viel Lärm, viel Populismus, wenig Effektivität.

2. Wer einen gefährlichen Hund halten will, muss u. a. persönlich zuverlässig sein. § 9 GefHundG enthält einen Katalog von Voraussetzungen, die die Unzuverlässigkeit begründen. Dies sind insbesondere einschlägige Vorstrafen, aber auch Trunk- oder Rauschmittelsucht, Arzneimittelmissbrauch oder die Tatsache, dass jemand wegen einer psychischen Krankheit oder einer geistigen oder seelischen Behinderung nach § 1896 BGB betreut wird. Es stellt sich die Frage, woher die Informationen stammen und aufgrund welcher Rechtsgrundlagen die Datenerhebung bzw. -übermittlung erfolgt. Entsprechende Befugnisse zur Datenerhebung und Verpflichtungen zur Datenübermittlung vermochte ich jedenfalls nicht zu erkennen.

3. Nach § 7 Abs. 2 GefHundG hat die für die Erhebung der Hundesteuer zuständige Stelle der Gemeinde der zuständigen Kreispolizeibehörde die Aufgabe einer Hundehaltung sowie Daten über den Verbleib des (gefährlichen) Hundes (einschließlich Namen und Anschriften des neuen Halters) mitzuteilen.

Diese Bestimmung würde nur dann Sinn machen, wenn bei der Veranlagungsbehörde die Hunderasse bzw. das Merkmal „gefährlicher Hund“ gespeichert wäre, was nach den Hundesteuersatzungen jedoch regelmäßig nicht der Fall ist. Außerdem erhebt bei weitem nicht jede Gemeinde Hundesteuer.

Allerdings sind die Gemeinden nach § 10 GefHundG verpflichtet, für gefährliche Hunde Abgaben nach Maßgabe des kommunalen Satzungsrechts zu erheben. Gemeinden, die bisher aus gutem Grund keine Hundesteuer erhoben haben und auch weiterhin keine Hundesteuer erheben möchten, sind jetzt zum Erlass einer Hundesteuersatzung - nur für gefährliche Hunde? - verpflichtet, obgleich nicht bekannt ist, ob sich im Gemeindegebiet überhaupt ein gefährlicher Hund befindet (Satzung auf Vorrat?). Eine Mitteilungspflicht der Kreispolizeibehörde an die für die Erhebung der Hundesteuer zuständige Stelle ist jedenfalls im GefHundG nicht vorgesehen, so dass in der Gesamtschau die §§ 7 Abs. 2, 10 GefHundG wenig Sinn machen.

Im Übrigen halte ich die Regelung in § 10 GefHundG schon deshalb für bedenklich, weil die Verpflichtung der Gemeinden, für gefährliche Hunde Steuern zu erheben, nicht in erster Linie der Erzielung von Einnahmen dient, sondern im Hinblick auf § 7 Abs. 2 GefHundG der polizeilichen Gefahrenabwehr (zum Begriff „Steuern“ siehe § 3 Abs. 1 AO).

Dies alles habe ich dem SMI in der Hoffnung auf eine baldige Änderung des Gesetzes mitgeteilt.

5.9.2 Polizeiliche Datenverarbeitung im Zusammenhang mit Aufenthaltsverboten

Das Sächsische Polizeigesetz erlaubt in § 21 Abs. 2 der Polizei, einer Person bis zu drei Monaten zu untersagen, sich in einem Gemeindeteil oder -Gebietsteil aufzuhalten, wenn Tatsachen die Annahme rechtfertigen, dass die Person dort eine Straftat begehen oder zu ihrer Begehung beitragen wird (Negativprognose).
Damit die Anwendung dieser Vorschrift landeseinheitlich praktiziert wird, hatte das SMI „Anwendungshinweise zum Erlass von Aufenthaltsverboten“ erlassen. Die auf meine Initiative hin vorgenommenen Modifizierungen der Anwendungshinweise (vgl. 8/5.9.1) sehen vor, dass die Polizei spätestens drei Monate nach Ablauf des Aufenthaltsverbotes in jedem Einzelfall über die Löschung der gespeicherten personenbezogen Daten entscheiden muss (Relevanzprüfung). Daten ohne erkennbaren Gefahrenabwehrhintergrund oder mögliche Strafrechtsrelevanz sind umgehend zu löschen. Dies gilt gleichermaßen für die Speicherung von personenbezogenen Daten in Akten wie für die automatisierte Speicherung. Um diese Relevanzprüfung auch bei automatisierter Datenspeicherung nach drei Monaten vornehmen zu können, enthalten die Anwendungshinweise die Vorgabe, dass sich die Datenverarbeitung nach der Errichtungsanordnung des Landeskriminalamtes für die Dateien „Polizeiliches Auskunftssystem Sachsen“ (PASS) zu richten hat.

Diese verbindlichen Vorgaben wurden jedoch durch die sächsische Polizei nicht konsequent eingehalten, wie meine Kontrolle beim Polizeirevier Leipzig ergab. So

musste ich feststellen, dass Entscheidungen über die Löschung der personenbezogenen Daten nicht dokumentiert und die einschlägigen Daten aus programmtechnischen Gründen nicht in PASS, sondern in der Datei Vorkommnisbericht (DVB) gespeichert waren. In DVB werden Daten jedoch erst nach zwei Jahren einer Relevanzprüfung unterzogen, während nur PASS technisch sicherstellen kann, dass spätestens drei Monate nach Erlass des Aufenthaltsverbots eine Relevanzprüfung erfolgen kann. Schließlich enthielten die im Polizeirevier aufbewahrten Akten erkennnungsdienstliche Unterlagen (Lichtbilder der Betroffenen aus PASS), deren weitere Aufbewahrung nach Ablauf des Aufenthaltsverbotes gegen das Vernichtungsgebot des § 20 Abs. 3 SächsPolG verstieß.

Nur weil die beim Kontrollbesuch anwesenden Vertreter des SMI mir zusagten, diese Fehler umgehend abzustellen, konnte ich von einer Beanstandung absehen.

Inzwischen hat mir das SMI versichert, dass

1. spätestens drei Monate nach dem Erlass eines Aufenthaltsverbotes einzelfallbezogen zu prüfen ist, ob die Speicherung personenbezogener Daten in diesem Zusammenhang noch erforderlich ist bzw. die Daten zu löschen sind.
2. bei der automatisierten Datenspeicherung in DVB sicherzustellen, dass das Datenschutzniveau im Vergleich mit einer Speicherung in PASS identisch ist (Relevanzprüfung nach drei Monaten).
3. nicht erforderliche in den Akten befindliche erkennungsdienstliche Unterlagen zu vernichten.

Ich werde wie im Vorjahr kontrollieren, ob diese aufsichtlichen Anweisungen befolgt werden.

5.9.3 BGS-Zugriff auf das polizeiliche Auskunftssystem Sachsen (PASS)

Wegen der zuvor erweiterten Aufgabenstellung des BGS hatte im Jahr 1999 das BMI mit dem SMI ein „Sicherheitskooperationssystem“ zwischen BGS und der sächsischen Polizei schriftlich vereinbart. Danach sollten unter anderem personenbezogene Daten „systematisch“ übermittelt werden dürfen. Ein „Datenzugriff auf die jeweilige Polizei- bzw. BGS-Dateien sowie der Datenaustausch“ sollte „soweit, als dies zur jeweiligen Aufgabenerfüllung erforderlich ist und für Zwecke erfolgt, für die Daten erhoben oder gespeichert worden sind“, zulässig sein. Im Übrigen enthielt die Vereinbarung weitgefasste Regeln: So sollten „erforderliche Ergänzungen und Einzelfallregelungen ... nach regionalen Erfordernissen vorgenommen werden dürfen, ohne dass vorher feststand, um was es gehen sollte.

Für eine solche Kooperation, die bestimmte Dienststellen des BGS - hier die im Freistaat Sachsen gelegenen BGS-Ämter Chemnitz und Pirna - sowie sächsische Polizeidienststellen automatisiert im Online-Verfahren auf die im PASS gespeicherten Daten zugreifen lässt, sah das SMI die Vorschrift des § 48 Abs. 2 SächsPolG als ausreichende gesetzliche Grundlage an. Nach dieser Vorschrift darf das SMI zur Erfüllung vollzugspolizeilicher Aufgaben unter anderem mit dem Bund einen Daten-

verbund vereinbaren, der eine automatisierte Datenübermittlung zwischen Polizeidienststellen ermöglicht.

Die Auffassung des SMI vermochte ich nicht uneingeschränkt zu teilen. Denn der allgemein formulierte Text der Vereinbarung konnte datenschutzrechtlich lediglich die Möglichkeit eröffnen, punktuelle und nach konventionellen Muster ablaufende Datenübermittlungen vorzunehmen; Übermittlungen im automatisierten Abrufverfahren, die nach sächsischem Recht besondere Zulässigkeitskriterien erfüllen müssen, wären aber von der Vereinbarung ersichtlich nicht erfasst worden. Ferner war zu bedenken, dass die PASS-Errichtungsanordnung keine Befugniszuweisung enthält, derzufolge „erforderliche Ergänzungen und Einzelfallregelungen ... nach regionalen Erfordernissen“ vereinbart werden können: Eine Zusammenarbeit mit dem BGS ist in der Errichtungsanordnung nämlich nicht geregelt.

Das SMI hat daraufhin eine ergänzende Vereinbarung mit dem BMI entworfen, die meine datenschutzrechtlichen Bedenken weitgehend berücksichtigt. Die Vereinbarung macht nunmehr deutlich, welche BGS-Dienststellen zu welchen Zwecken in welchem Umfang auf PASS zugreifen dürfen. Damit genügen die Datenübermittlungen im automatisierten Verfahren auch dem besonderen landesrechtlichen Zulässigkeitanforderungen nach §§ 48 Abs. 2, 35 SächsPolG i. V. m. § 13 SächsDSG. Außerdem wurde der BGS in der aktualisierten Version der PASS-Errichtungsanordnung in den Aufgaben- und Adressatenkreis der Datei aufgenommen, die - als ausdrücklicher Bestandteil der noch abzuschließenden Vereinbarung - insoweit auch für den Bund gilt.

Über den Fortgang der Angelegenheit werde ich weiter unterrichten.

5.9.4 Fehler bei erkennungsdienstlicher Behandlung durch die Polizei

Aufgrund der Eingabe eines Petenten erhielt ich Kenntnis von der Verfügung eines sächsischen Polizeireviers, worin der Petent aufgefordert wurde, sich einer erkennungsdienstlichen (ED-)Behandlung nach § 81 b 2. Alternative StPO zu unterziehen. Danach dürfen u. a. Lichtbilder und Fingerabdrücke des Beschuldigten auch gegen seinen Willen aufgenommen werden, wenn es für Zwecke des Erkennungsdienstes notwendig ist. Diese Maßnahme dient nicht der Überführung des Beschuldigten in einem bestimmten Strafverfahren (§ 81 b 1. Alt. StPO), sondern der vorsorglichen Bereitstellung von Hilfsmitteln für die Aufklärung späterer Straftaten. Die Maßnahme ist notwendig, wenn Anhaltspunkte dafür vorliegen, dass der Beschuldigte in ähnlicher oder anderer Weise erneut straffällig werden könnte und die erkennungsdienstlichen Unterlagen zur Förderung der dann zu führenden Ermittlungen geeignet erscheinen.

Im vorliegenden Fall hatte der Polizeibeamte die ED-Behandlung mit einem bestimmten gegen den Petenten eingeleiteten Ermittlungsverfahren begründet. Aufgrund eines staatsanwaltschaftlichen Bescheides war das der polizeilichen Verfügung zugrunde liegende Ermittlungsverfahren jedoch bereits zuvor mangels hinreichenden Tatverdachts (§ 170 Abs. 2 StPO) eingestellt worden. Damit stand fest, dass der von

der Polizei angegebene Grund für die erkennungsdienstliche Behandlung nicht mehr vorlag. Die Aufforderung zum Erscheinen zur erkennungsdienstlichen Behandlung war somit im vorliegenden Fall rechtswidrig. Vom Polizeirevier wurde die Unzulässigkeit der Verfügung auch sofort erkannt.

Ich habe den Vorfall trotzdem zum Anlass genommen, das SMI dringend zu ersuchen, die ihm zu Gebote stehenden aufsichtsrechtlichen Maßnahmen zu ergreifen, um jeglichen unvorsichtigen Umgang mit erkennungsdienstlichen Maßnahmen, die tief in das Persönlichkeitsrecht eingreifen, zu unterbinden. Daraufhin wurden sämtliche Leiter der Polizeidirektionen zur Rechtslage ausführlich belehrt.

5.9.5 Auskunfts- und Löschungsersuchen abgelehnter Asylbewerber zu ihren im INPOL und SIS gespeicherten Daten

Immer häufiger erhielt ich zuständigkeitshalber über den BfD die Gesuche abgelehnter Asylbewerber, insbesondere algerischer Nationalität, um Auskunft und Löschung ihrer Ausschreibung zur Einreiseverweigerung bzw. ihrer Personenfahndung im Schengener Information System (SIS). Diese Petenten hatten ihr Ersuchen zunächst an die in Frankreich für die Kontrolle des Datenbestandes des Schengener Informationssystems zuständige Datenschutzbehörde „Commission Nationale de l'Informatique et des Libertés (CNIL)" gerichtet, welche die Ersuchen sodann an den BfD weitergegeben hatte.

Im Rahmen meiner datenschutzrechtlichen Bewertung der Eingaben habe ich Folgendes festgestellt: Die Zentrale Ausländerbehörde für Sachsen, das Regierungspräsidium Chemnitz, hatte vor Jahren bei abgelehnten und abgeschobenen sowie bei abgelehnten und nicht abgeschobenen („untergetauchten") Asylbewerbern gem. Art. 96 Abs. 1 und Abs. 3 SDÜ (Schengener Durchführungsübereinkommen) die entsprechenden Eintragungen im SIS bzw. INPOL zur Einreisesperre und für die Durchsetzung von Erstattungsansprüchen für die Kosten Ihrer Abschiebung veranlasst.
Nach § 8 Abs. 2 AuslG darf ein Ausländer, der ausgewiesen oder abgeschoben worden ist, nicht erneut ins Bundesgebiet einreisen und sich darin aufhalten. Auf Antrag wird dies in der Regel befristet, z. B. nach Begleichung der Abschiebekosten.

Nach Art. 112 Abs. 1 SDÜ ist jedoch die zuständige Ausländerbehörde auch verpflichtet, in jedem Einzelfall anhand der Schengen-Kriterien zu prüfen, ob jeweils nach Ablauf einer dreijährigen Speicherungsfrist die bestehende SIS-Speicherung weiterhin aufrechterhalten oder gelöscht werden muss. Eine Löschung der SIS-Speicherung kann nicht von der Begleichung der Abschiebekosten abhängig gemacht werden. Unabhängig von einer Löschung der internationalen SIS-Speicherung kann jedoch die nationale Ausschreibung zur Einreiseverweigerung weiterhin bestehen bleiben.

Diese Einzelfallprüfungen nach Art. 112 Abs. 1 SDÜ durch die zentrale Ausländerbehörde waren nach dreijähriger Speicherung jedoch offensichtlich nicht umfassend

erfolgt. Für die nachträgliche Prüfungen der vielen laufenden Vorgänge stand bei der Behörde nicht das benötigte Personal zur Verfügung. Nach intensiver Diskussion mit der zentralen Ausländerbehörde hat diese in enger Abstimmung mit dem Bundesverwaltungsamt, dem Ausländerzentralregister, dem LKA Sachsen und dem SMI die generelle Löschung aller im INPOL und SIS von ihr ausgelösten Personenfahndungen, wenn sie vor dem 26. April 1994 eingetragen waren, veranlasst. Dabei wurden über 16.000 bedenkliche Eintragungen gelöscht. Zugleich sind dem LKA Listen übergeben worden, die eine Prüfung und Überarbeitung der Ausschreibungen zwischen dem 27. April 1994 und dem 31. Juli 2000 gemäß Art. 96 SDÜ ermöglichen.

Mit der generellen Löschung und Überarbeitung der Ausschreibungen ist nunmehr gewährleistet, dass die Fahndungsausschreibungen der zentralen Ausländerbehörde im SIS „Schengen-konform“ sind. Damit wurde den internationalen Anforderungen an das Grundrecht auf informationelle Selbstbestimmung hinsichtlich der Speicherung personenbezogener Daten von vielen abgelehnten Asylbewerbern entsprochen.

5.9.6 Speicherung von Wiederholungsfällen bei Verstößen im ruhenden Verkehr

Kontrollen in drei kommunalen Bußgeldstellen haben ergeben, dass in den dort geführten automatisierten Dateien entgegen einem Erlass des SMI vom 22.5.1995 (vgl. 4./5.9.7) und ungeachtet meiner früheren Hinweise (vgl. 5./5.9.15) weiter Daten über so genannte Mehrfachtäter im ruhenden Verkehr gespeichert werden. Eine Rechtsgrundlage hierfür ist nicht ersichtlich, die Speicherung erledigter Park- und Halteverstöße in örtlichen Dateien deshalb ein klarer Verstoß gegen Gesetz und Recht.

In den kontrollierten Bußgeldstellen blieben Angaben zum Fahrzeughalter (Name, Vorname, Anschrift, Geburtsdatum, amtliches Kennzeichen des Fahrzeugs, Tatort, Datum und Uhrzeit des Verkehrsverstoßes, Beweismittel, Höhe der festgesetzten und Höhe des bezahlten Verwarnungsgeldes oder der Geldbuße) auch dann gespeichert, wenn das Verwarnungsgeld oder die Geldbuße bezahlt worden war. Der zuständige Sachbearbeiter erhielt bei jeder Tat wegen der alphabetisch geordneten Namen der Betroffenen so stets Kenntnis von deren Vortaten.

Falschparken ist eine geringfügige Ordnungswidrigkeit nach §§ 24 StVG, 12 StVO. Sie kann verfolgt und mit einem Verwarnungsgeld, § 27 StVG, §§ 56, 58 Abs. 2 OWiG, oder einer Geldbuße geahndet werden. Solange das festgesetzte Verwarnungsgeld oder die Geldbuße noch nicht eingegangen sind, dürfen die Daten des Täters zum Zwecke der Verfolgung und Ahndung in der Bußgeldstelle gespeichert werden. Danach ist die Kenntnis der erhobenen Daten zur Erfüllung der Aufgaben der Bußgeldstelle nicht mehr erforderlich und damit unzulässig, § 12 Abs. 1 Nr. 1 SächsDSG.

Insbesondere hat der Gesetzgeber den Bußgeldstellen keine Registeraufgaben zugewiesen. Eine solche Aufgabe erfüllt ausschließlich das beim Kraftfahrt-Bundesamt

(„Flensburg“) geführte Verkehrszentralregister nach §§ 28 bis 30c StVG. Die dort genannten Voraussetzungen sind, so hat das Bundesverwaltungsgericht entschieden, abschließend (BVerwGE 51, 359 [367 ff.]), und können nicht entsprechend auf die Bußgeldstellen angewandt werden.

Denn im Bereich von Bagatellverfahren können Wiederholungen allenfalls dann Berücksichtigung finden, wenn sie ohne besondere Nachforschungen bekannt sind oder sich von selbst im Verfahren ergeben. Auch ein behördeninterner Aktenplan, der Aufbewahrungsfristen von drei bis zehn Jahren für die dem einzelnen Verfahren zu Grunde liegende Akte vorsieht, oder der Hinweis auf die Möglichkeit eines Wiederaufnahmeverfahrens, § 85 OWiG, vermögen die Speicherung nicht zu rechtfertigen: Die Akte ermöglicht keine Übersicht über Vortaten; die sehr seltene Wiederaufnahme stützt sich auf die Akte, nicht auf eine automatisierte Datei.

Die Bußgeldstellen müssen deshalb durch geeignete technisch-organisatorische Maßnahmen dafür sorgen, dass Daten erledigter Park- und Halteverstöße unverzüglich gelöscht werden. Vorhandene Datenbestände sind zu bereinigen. Bei künftigen Kontrollen werde ich darauf besonders achten.

5.9.7 Bundesmodellprojekt „Frühintervention bei erstauffälligen Drogenkonsumenten“

Zusammen mit SMS und SMI konnte ich ein zunächst heikel erscheinendes Verfahren zur Beratung jugendlicher Drogenkonsumenten durch einen privaten Hilfsverein datenschutzgerecht gestalten:

Durch das als „Modellprojekt“ vom Bundesgesundheitsministerium finanzierte Verfahren sollen demnächst bundesweit 14- bis 25-Jährige, die der Polizei erstmals durch Drogenkonsum auffallen, besser über die Wirkung illegaler Drogen informiert und bereits in diesem frühen Stadium zu einer dauerhaften Verhaltensänderung motiviert werden. Dies soll in Informations- und Beratungskursen regional tätiger privater Vereine geschehen. Die Teilnahme an den Kursen soll den Jugendlichen bescheinigt werden und die Chance auf das nach § 31a BtMG unter bestimmten weiteren Voraussetzungen mögliche Absehen von der weiteren Verfolgung der Straftat erhöhen. In Sachsen soll ein Leipziger Verein diese Aufgaben im Raum Leipzig, Torgau und Grimma erfüllen.

Aus datenschutzrechtlicher Sicht lautete danach die Grundfrage: Wie sollte der Verein von den jugendlichen Drogenkonsumenten erfahren? In der mir zunächst vorgelegten Konzeption war von einer „enge(n) und verlässliche(n) Zusammenarbeit“ zwischen den beteiligten Vereinen und „der Polizei, der Staatsanwaltschaft, dem Gericht sowie dem Jugendamt bzw. der Bewährungshilfe“, ohne die eine „Zuführung“ des Drogenkonsumenten zu den Kursen nicht gelingen könne, die Rede. Auch die weitere Darstellung des Projekts konnte nicht anders verstanden werden, als dass Polizei und Staatsanwaltschaften die im Ermittlungsverfahren erhobenen Daten der Betroffenen (z. B. Name, Vorname, Geburtsdatum, Wohnanschrift, Angaben zum Tatzeitpunkt und –ort, Art und Menge des Betäubungsmittels, etc.) an den Verein

übermitteln sollten. Das wäre datenschutzrechtlich nicht ohne die Einwilligung der Betroffenen zulässig gewesen:

Denn als Rechtsgrundlage für die Übermittlung der genannten Daten von der Polizei oder einer Staatsanwaltschaft an den Leipziger Verein war ein spezielles Gesetz nicht ersichtlich. Auch § 15 SächsDSG als Auffangvorschrift schied wegen der mit einer Übermittlung verbundenen Zweckänderung bzw. wegen der Schutzwürdigkeit des Interesses des Betroffenen am Unterbleiben der Übermittlung als Rechtsgrundlage aus. Einzig die schriftliche Einwilligung der Betroffenen nach § 4 Abs. 1 SächsDSG hätte die Übermittlung rechtfertigen können. Dabei hätte die Polizei in jedem Einzelfall die Frage der Einwilligungsfähigkeit genau prüfen müssen, weil zwar schon 14-Jährige in der Regel über die erforderliche Einwilligungsfähigkeit verfügen, es jedoch bei Drogenkonsumenten dieses Alters nicht ganz fern liegt, zu prüfen, ob bei Hinzutreten weiterer, typischer Umstände, etwa einer psychischen oder geistigen Reifeverzögerung, die erforderliche Einwilligungsfähigkeit im Zeitpunkt der Erklärung fehlt.

Aufgrund dieser rechtlichen und tatsächlichen Schwierigkeiten änderten SMI und SMS auf meine Initiative hin ihre konzeptionellen Vorstellungen dergestalt, dass nunmehr auf die Übermittlung personenbezogener Daten von der Polizei oder Staatsanwaltschaften an den Hilfsverein gänzlich verzichtet wird. Die Polizei unterrichtet den Betroffenen künftig lediglich in allgemeiner Form über das Angebot des Vereins und händigt ihm zur Erläuterung ein – datenschutzrechtlich unbedenkliches – Faltblatt des Vereins aus. Ob und ggf. wann der Betroffene daraufhin tatsächlich einen Kurs des Vereins besucht und eine ihm erteilte Bescheinigung über seine Teilnahme am Kurs (selbst) zu seiner Ermittlungsakte gibt, bleibt ihm überlassen. Zu einer „Meldung“ des jugendlichen Erstkonsumenten an den Verein, das heißt zu einer Übermittlung personenbezogener Daten, kommt es jedenfalls nicht mehr. Damit hatte sich auch die Frage erledigt, unter welchen Voraussetzungen hier von einer wirksamen Einwilligung der Jugendlichen ausgegangen werden konnte.

Wir werden abwarten, ob dieses spontan zu wählende Angebot ausreicht und sich diejenigen, die der Beratung am meisten bedürfen, beim Verein melden. Ich bin auch bereit, über andere Anstöße und Hinweise, gelegentlich auch über „gelinde Nachhilfe“ nachzudenken. Das Anliegen des Vereins sollte jedenfalls unterstützt werden und konkrete Wirkung entfalten.

5.9.8 Landesweiter Wettbewerb „Qualität der Polizeiarbeit“

Mit dem landesweiten Wettbewerb „Qualität der Polizeiarbeit“ will das SMI „Bürgernähe und Bürgerfreundlichkeit“ in den Sächsischen Polizeirevieren fördern.

Bei den konzeptionellen Vorarbeiten, in die ich frühzeitig eingebunden wurde, musste das Problem gelöst werden, inwieweit die aus einer Befragung betroffener Bürger bestehende Aktion ohne personenbezogene Datenverarbeitung durchgeführt werden konnte. In intensiven Beratungen mit dem SMI habe ich ein zufriedenstellendes Ergebnis erzielt:

Die personenbezogenen Daten der auf dem Postweg befragten Bürger dürfen keiner weiteren Verwendung für Zwecke des Polizeivollzugsdienstes zugänglich gemacht werden.

Weil wegen der den Befragten eingeräumten Möglichkeit, Angaben in einem Freitextfeld zu machen, nicht ausgeschlossen werden kann, dass auch Daten erhoben werden, die eine Identifizierung von einzelnen Polizeibediensteten ermöglichen, wird das SMI sicherstellen, dass bei der Auswertung der Befragungsunterlagen die in § 31 SächsDSG normierten datenschutzrechtlichen Garantien für die Verarbeitung von Beschäftigtendaten eingehalten werden, also keinesfalls irgendwelche einzelne Personalmaßnahmen gegen Beamte ergriffen werden.

5.10 Verfassungsschutz

5.10.1 Gesetzgebungsvorhaben im Bereich des Sächsischen Verfassungsschutzes

Im Berichtszeitraum unterbreitete mir das SMI seine Pläne, das Sächsische Verfassungsschutzgesetz in zwei Regelungsbereichen zu ändern. In beiden Fällen führte meine datenschutzrechtliche Kritik dazu, die Gesetzgebungsvorhaben (einstweilen) nicht weiter zu verfolgen:

- Mit dem ersten Gesetzgebungsvorhaben wollte das SMI sicherstellen, dass in jedem Einbürgerungsverfahren bei der Verfassungsschutzbehörde vorliegende, verfahrensverwertbare Erkenntnisse zu dem jeweiligen Einbürgerungsbewerber Berücksichtigung finden; es wurde also die Praxis der „Regelanfrage“ der Einbürgerungsbehörden beim Verfassungsschutz angestrebt. Dies stellte eine Erweiterung des geltenden Aufgabenkatalogs des Sächsischen Landesamtes für Verfassungsschutz dar, der bislang nur eine einzelfallbezogene Anfrage beim Verfassungsschutz vorsieht.
  Mit der Befugniserweiterung stellte sich die Frage, ob ein solches flächendeckendes Abfrageverfahren von den für die Einbürgerungsbehörde maßgeblichen bundesrechtlichen Vorschriften gedeckt ist. Hierzu habe ich Folgendes ausgeführt:

  § 86 Nr. 2 AuslG ist der Maßstab, an dem sich die Einbürgerungsbehörde zu orientieren hat. Danach müssen „tatsächliche Anhaltspunkte“ für die Annahme vorliegen, dass - vereinfacht formuliert - Einbürgerungsbewerber relevante Kriterien im Sinne verfassungsfeindlicher und auf den Ausländerextremismus bezogene Bestrebungen erfüllen. Der für die Einbürgerung allein zuständige Normadressat sind die Einbürgerungsbehörden. (Dies beachtete im Übrigen auch der Gesetzentwurf, der die einschlägige Neuregelung die Hilfestellung des Landesamtes für Verfassungsschutz für die Einbürgerungsbehörden nach wie vor unter „Mitwirkungsaufgaben“ des § 2 Abs. 2 SächsVSG aufführte.)

  Somit steht fest, dass *bei den Einbürgerungsbehörden* tatsächliche Anhaltspunkte in dem oben beschriebenen Sinne vorliegen müssen. Erst wenn dies der Fall ist, dürfen bei den einschlägigen Behörden (LfV, Polizei) Verifikationsinformationen

abgerufen werden. Dieser Rechtslage entspricht das Sächsische Verfassungsschutzgesetz in seiner geltenden Fassung, in dem es als Bedingung für eine Beteiligung des Verfassungsschutzes den einschlägigen „Verdacht“ fordert.

Die Novellierung des Ausländergesetzes (des Bundes) hat an dieser Rechtslage - entgegen der entsprechenden Andeutung in der Begründung des Gesetzentwurfs nichts geändert: Denn hätte der Bundesgesetzgeber gewollt, dass eine obligatorische Beteiligung des Verfassungsschutzes im Einbürgerungsverfahren erfolgt, müsste dies aus dem Wortlaut des Ausländergesetzes - zumindest aber aus dessen Begründung - hervorgehen. Dies ist jedoch nicht der Fall.

Damit wird klar, dass der kompetenzielle Rahmen der für die Einbürgerung zuständigen Behörde durch die Novelle des Ausländergesetzes nicht erweitert worden ist.

Die geplante gesetzliche Regelanfrage hätte ferner gegen das verfassungsmäßige Gebot der Verhältnismäßigkeit verstoßen, weil sie eine Abstufung der Voraussetzungen (Differenzierung nach geographischer Herkunft der Einbürgerungsbewerber) vorsieht. Gerade aber in diesem Zusammenhang konkretisiert die amtliche Begründung zu § 86 AuslG den Prüfmaßstab, in dem sie den exemplarischen Hintergrund „PKK“ und „radikale Islamisten“ nennt. Somit wird deutlich, dass nicht in jedem Fall - etwa wie bei einer Regelanfrage - einschlägige Verdachtsmomente vorliegen können. Damit ließ bereits die bundesrechtliche Gesetzessituation das Novellierungsvorhaben nicht zu. Darüber hinaus habe ich das SMI vor der Gefahr gewarnt, dass anlässlich von Anfragen der Einbürgerungsbehörden Ermittlungen wie bei Sicherheitsüberprüfungen angestellt und entsprechende Datensammlungen auf Zeit beim LfV angelegt werden.

Keinesfalls wäre es zulässig, die Tatsache eines Einbürgerungsantrages zum Anlass zu nehmen, Tätigkeiten des LfV zu initiieren.
Im Übrigen wird meine Rechtsauffassung durch die vom Bundeskabinett beschlossene Allgemeine Verwaltungsvorschrift zum Ausländergesetz bestätigt, wonach eine Datenerhebung beim Verfassungsschutz nur erforderlich ist, wenn es konkrete Zweifel an Angaben des Betroffenen gibt, die zudem durch Tatsachen begründet sein müssen.

- Das zweite Novellierungsvorhaben zum Sächsischen Verfassungsschutzgesetz enthielt eine Erweiterung der Aufgaben um die „Beobachtung der Organisierten Kriminalität“. Diesen Entwurf habe ich aufgrund der folgenden Erwägungen abgelehnt: Mit der beabsichtigten Aufgabenerweiterung würde eine vom Bisherigen abweichende andere institutionelle Qualität von Verfassungsschutz geschaffen; sozusagen eine Polizei ohne Polizeibefugnisse, die nicht an das strafprozessual normierte Legalitätsprinzip und auch nicht durchgängig an den verfassungsrechtlichen Verhältnismäßigkeitsgrundsatz gebunden wäre.

  Die beabsichtigte Aufgabenerweiterung verstieße ferner gegen den - gerade im Freistaat Sachsen explizit (in Art. 83 Abs. 3) normierten - Verfassungsgrundsatz der Trennung von Verfassungsschutz und Polizei, der sich nicht nur historisch aus

dem „Frankfurter Polizeibrief“, sondern unmittelbar aus dem Rechtsstaatsprinzip ableitet. Denn unsere verfassungsgemäße Ordnung gebietet es, eine durchgängige Verwaltungskontrolle und gerichtlichen Individualrechtsschutz zu gewährleisten. Nur durch eine organisatorisch-institutionelle und eine aufgabenmäßige Trennung zwischen Verfassungsschutz und Polizei können diese Verfassungsgarantien aufrechterhalten werden.

Die Erweiterung der Aufgaben des Landesamtes für Verfassungsschutz auf die Beobachtung von Bestrebungen und Tätigkeiten der Organisierten Kriminalität ist auch nicht notwendig. Die vom SMI behauptete Lücke bei der Bekämpfung der Organisierten Kriminalität besteht nicht. Gemäß der schon 1995 in Kraft getretenen „Gemeinsamen Verwaltungsvorschrift des Sächsischen Staatsministeriums der Justiz und des Sächsischen Staatsministeriums des Innern über die Zusammenarbeit von Staatsanwaltschaft und Polizeivollzugsdienst bei der Bekämpfung der Organisierten Kriminalität“ (VwV-BekämpfungOK) gibt es den Begriff der sog. „Initiativermittlungen“. Danach sind im Bereich der Organisierten Kriminalität auch unterhalb der Schwelle des Anfangsverdachts (§ 152 Abs. 2 StPO) Ermittlungen möglich. Begründet wird dies damit, dass Strafanzeigen in diesem Bereich häufig nicht erstattet werden; dies u. a. deswegen, weil Zeugen Angst hätten. Die VwV-BekämpfungOK führt dazu aus, dass bei „Initiativermittlungen“ keine gesetzliche Verfolgungspflicht besteht, die Strafverfolgungsbehörde sich mithin von Opportunitätserwägungen leiten lassen kann. Diese „Initiativermittlungen“ sind zwar aus strafprozessualer und dogmatischer Sicht mehr als problematisch, weil sie die Schwelle zur Einleitung eines staatsanwaltschaftlichen Ermittlungsverfahrens absenken und die bewährte Abgrenzung Gefahrenabwehr/ Strafverfolgung mit den sich daran anschließenden Verantwortlichkeiten verschieben - sie umfassen aber notwendigerweise bereits die vom Entwurf in Aussicht genommenen, den Verfassungsschutz zu übertragenden Beobachtungsaufgaben hinsichtlich der Organisierten Kriminalität.
Auch die vom Entwurf vorgesehene Anlehnung der Definition des Begriffs der Organisierten Kriminalität an die Formulierung in der Anlage E zu den Richtlinien für das Straf- und Bußgeldverfahren ist in diesem Umfang unzulässig. Nicht alles, was Organisierte Kriminalität im Sinne der vorgenannten Richtlinie ausmacht, richtet sich gegen Staat und Verfassung.

Dies ist aber Voraussetzung, um dem Gebot der Trennung von Verfassungsschutz und Polizei gerecht zu werden. Dieses ergibt sich bereits unmittelbar aus dem Rechtsstaatsprinzip (Grundsatz der durchgängigen Verwaltungskontrolle und des individuellen Rechtsschutzes durch Gerichte), darüber hinaus aus Art. 83 Abs. 3 Satz 1 SächsVerf: Danach ist die Polizei eine Institution mit Eingriffs- und Zwangsbefugnissen zur Gefahrenabwehr und zur Störungsbeseitigung, der Verfassungsschutz hingegen eine Institution zur bloßen Gefahrenaufklärung oder Gefahrenerforschung.

Schließlich definiert Art. 73 Nr. 10 lit. b GG den Verfassungsschutz als Schutz der freiheitlichen demokratischen Grundordnung, des Bestandes und der Sicherheit des Bundes oder eines Landes.

Zwar kann auch die gemäß der offiziellen Definition von „Gewinn- oder Machtstreben bestimmte planmäßige Begehung von Straftaten, die einzeln oder in ihrer Gesamtheit von erheblicher Bedeutung für die Rechtsordnung sind, durch mehr als zwei Beteiligte, die auf längere oder unbestimmte Zeit arbeitsteilig tätig werden, unter Verwendung gewerblicher oder geschäftsähnlicher Strukturen oder unter Anwendung von Gewalt oder durch entsprechende Drohungen“ als Auslösung der Sicherheit der Bürger die Staatssicherheit mittelbar gefährden, wenn der Staat und seine Organe als handlungsunfähig erscheinen. Dies ist jedoch mittelbare Folge jeder Kriminalität. Bei diesen Straftaten handelt es sich um keine neuen Phänomene: Schon immer gab es Straftaten, die im größeren Stil nur arbeitsteilig begangen werden konnten; sie haben im Rahmen der Organisierten Kriminalität lediglich eine andere Quantität.

Für die Konturierung des Verfassungsschutzes, der nicht für alles zuständig sein kann, was den Staat mittelbar gefährdet, muss daher ausschlaggebend sein, dass Aspekte der Sicherheit von Bund und Ländern in Rede stehen und - als Folge - eine Gefährdung von Staat und Gesellschaft zu besorgen ist. Deshalb kommt die Tätigkeit des Verfassungsschutzes nur in solchen Fällen in Betracht, in denen eine organisierte kriminelle Einflussnahme auf Politik, Verwaltung und Justiz anzunehmen ist.

Ich gehe davon aus, dass die vorgenannten Gesetzgebungsvorhaben eingestellt werden.

5.10.2 Mängel der Aktenführung beim LfV

Im Berichtszeitraum habe ich aus Anlass von Eingaben mehrere Kontrollen im Landesamt für Verfassungsschutz durchgeführt. Dabei traten insoweit Mängel zutage, als Sachbearbeitungsvermerke sich auf Akteninhalte bezogen, die zum Zeitpunkt meiner Kontrolle der Akte nicht zu entnehmen waren. Ich habe von einer förmlichen Beanstandung abgesehen, weil die Amtsleitung die Defizite der Aktenführung sofort einräumte und entsprechende geeignete Maßnahmen zur Mängelbeseitigung einleitete. Gleichwohl werde ich angesichts der zu verbessernden Aktenführung noch im Jahr 2001 eine Querschnittsprüfung im Landesamt für Verfassungsschutz durchführen.

5.11 Landessystemkonzept / Landesnetz

Sächsische Fördermitteldatenbankverordnung

In den Berichtszeitraum fällt der Erlass der auf § 1 Abs. 3 des Gesetzes über Fördermitteldatenbanken im Freistaat Sachsen (SächsFöDaG) basierenden Verordnung durch die Staatsregierung, in der im Einzelnen die in der landeseinheitlichen Fördermitteldatenbank verarbeiteten personenbezogenen Daten sowie die Fristen für die Trennung der Daten von den Vorhaben aufgeführt sind. In Zusammenarbeit mit dem zuständigen Referat der Staatskanzlei und der Koordinierungs- und Beratungsstelle für Informationstechnologie sind die für die Verarbeitung notwendigen Datenkategorien klar abgegrenzt und übersichtlich beschrieben worden, so dass sowohl für

Anwender wie auch für Betroffene die Datenverarbeitung übersichtlich und vorhersehbar ist. Die Entscheidung, diese Datenkategorien nicht detailliert im Gesetz, sondern in einer Verordnung aufzuführen, um so eine größere Flexibilität zu gewährleisten, hat sich als sehr sinnvoll erwiesen. Bereits kurze Zeit nach dem Erlass der Verordnung stellte sich aufgrund neuer Anforderungen der EU die Frage einer Überarbeitung. Ich bin in diesen – wohl ständig fortdauernden – Prozess gut eingebunden und kann meine Vorstellungen in die gemeinsame Willensbildung einbringen.

5.12 Ausländerwesen

Das Standesamt als Informant der Polizei?

Der Ausländerbeauftragte einer Kreisverwaltung teilte mir mit, ein zur Abschiebung ausgeschriebener türkischer Staatsangehöriger sei im Standesamt festgenommen und in Abschiebegewahrsam gebracht worden. Er habe sich gemeinsam mit seiner Verlobten, einer deutschen Staatsangehörigen vor dem Zimmer der Standesbeamtin aufgehalten, um bei ihr „das Aufgebot“ zu bestellen.

Daraufhin habe ich sofort bei der Polizeiführung nachgefragt und zunächst ausweichende und sachlich falsche Informationen erhalten, mit denen ich mich aber nicht zufrieden geben konnte. Folgender Sachverhalt stellte sich heraus:
Die Polizei handelt in Amtshilfe für die Ausländerbehörde, wenn es darum geht, einen Abschiebehaftbefehl zu vollstrecken. Zu diesem Zweck hatte die Polizei sich - wohl wissend, dass der Ausländer eine Deutsche heiraten wolle - an die Leiterin des Standesamtes gewandt und sie gebeten unverzüglich Mitteilung zu geben, wenn der Ausländer (mit seiner Verlobten) im Standesamt auftaucht. Die Standesbeamtin ist diesem Wunsch der Polizei nachgekommen und hat den Ausländer „verpfiffen“, obwohl sie wusste, dass die ernsthafte Absicht bestand zu heiraten und dass damit der Abschiebegrund entfallen würde.

Diese Formen der „informationellen Zusammenarbeit“ und der Datenübermittlung stellten sich somit als rechtswidrig heraus. Das SMI hat sich meiner Auffassung angeschlossen und unverzüglich dafür gesorgt, dass der Ausländer aus der Haft entlassen wurde und heiraten konnte.

5.13 Wahlrecht

Gewinnung geeigneter Wahlhelfer für die sächsische Kommunalwahl am 10. Juni 2001

Eine Vielzahl von Eingaben - z. B. auch beim Landesamt für Statistik - veranlasste mich, das SMI um Lösung der folgenden Problematik zu bitten:

Wahlhelfer können sich die Gemeinden auch aus dem Kreis derjenigen aussuchen, die in irgendeiner Behörde beschäftigt sind. Zu diesem Zweck bitten viele Bürgermei-

ster die Leiter der Behörden, von denen sie annehmen, dass dort Gemeindebürger beschäftigt sind, um Benennung geeigneter Wahlhelfer.

§ 10 Abs. 2 KomWG verpflichtet die Behördenleiter dann zu entsprechenden Namensnennungen an die Bürgermeister. Adressaten dieser Bestimmungen sind demnach die Behördenleiter, nicht aber die Betroffenen selbst, deren Daten zunächst erhoben und anschließend übermittelt werden sollen. Die Datenauswahl (Erhebung) sowie die daran anschließende Datenübermittlung erfolgt regelmäßig ohne Kenntnis der Betroffenen. Ob dadurch deren schutzwürdige Interessen beeinträchtigt werden können, bleibt ungeprüft. Der damit verbundene Eingriff in das Recht auf informationelle Selbstbestimmung steht im Widerspruch zu den vom Bundesverfassungsgericht geprägten und normativ wirkenden Grundsätzen. Die Bediensteten können nämlich nicht mit hinreichender Sicherheit überschauen, welche sie betreffenden Informationen wann und bei welcher Gelegenheit durch wen erhoben und weitergegeben werden. Mit dem Recht auf informationelle Selbstbestimmung ist aber eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der der Bürger nicht mehr wissen kann, wer was wann und bei welcher Gelegenheit über ihn weiß (BVerfGE 65, 43).

Schon die Auswahl eines „geeigneten" möglichen Wahlhelfers durch den Behördenleiter ist nicht möglich. Soll etwa der Behördenleiter erfahren, ob und welche Gründe es gibt, dass sein Mitarbeiter ungeeignet ist (z. B. weil er selbst oder seine Frau kandidiert, weil er im Wohnort „verschrien" ist, weil er am Wahltag aus privaten Gründen verhindert ist etc.)?

Selbstverständlich ist das Grundrecht auf informationelle Selbstbestimmung nicht schrankenlos gewährleistet. Soll der Einzelne aber eine Einschränkung hinnehmen, bedarf es einer (verfassungsmäßigen) gesetzlichen Grundlage, aus der sich die Voraussetzungen und der Umfang der Beschränkung klar und für den Betroffenen erkennbar ergeben und die damit den rechtsstaatlichen Geboten der Normenklarheit und der Verhältnismäßigkeit entspricht (BVerfGE 65, 44). Daran mangelt es ersichtlich bei § 10 Abs. 2 KomWG (dto. § 8 Abs. 6 SächsWahlG). Ich halte eine Änderung der Bestimmungen in den Wahlgesetzen, die die Datenübermittlung an die Bürgermeister regeln, im Lichte vorstehender Grundsätze für unerlässlich und habe deshalb eine entsprechende Gesetzesinitiative durch das SMI angeregt.

Da dies vor der bevorstehenden Kommunalwahl nicht mehr zu realisieren sein wird, habe ich außerdem vorgeschlagen, die sächsischen Behörden zu einer dem Recht auf informationelle Selbstbestimmung entsprechenden Verfahrensweise (etwa durch Übersendung von 7/5.13.2) anzuhalten. Die Behörden könnten beispielsweise über das Sächsische Amtsblatt und über die Mitteilungsblätter des Sächsischen Landkreistages und des Sächsischen Städte- und Gemeindetages zuverlässiger und früher erreicht werden, als durch diesen Beitrag.

5.14 Sonstiges

In diesem Jahr nicht belegt.

6 Finanzen

6.1 Erhebung von personenbezogenen Daten Dritter nach den Hundesteuersatzungen

Sächsische Gemeinden, die Hundesteuer erheben, haben in aller Regel eine Hundesteuersatzung, die der vom SSG im „Sachsenlandkurier“ 8/96 veröffentlichten Mustersatzung entspricht. U. a. hat danach der bisherige Hundehalter bei Veräußerung oder Verschenkung eines Hundes Namen und Anschrift des neuen Hundehalters anzugeben. Die verwendeten *Abmelde*formulare sehen regelmäßig eine diesbezügliche Datenerhebung vor. In manchen Fällen wird auch ohne eine entsprechende Satzungsbestimmung darüberhinaus in *Anmelde*formularen nach dem bisherigen Besitzer und dessen Anschrift gefragt.

Abgesehen davon, dass bei Veräußerung eines Hundes *nach* außerhalb die Zuständigkeit der bisherigen Gemeinde endet und dass bei Zuwanderung eines Hundes *von* außerhalb eine Zuständigkeit der Gemeinde bezüglich des (auswärtigen) bisherigen Hundehalters nicht gegeben ist, ließe § 11 Abs. 4 Nr. 1 SächsDSG solche Datenerhebungen bei Dritten nur zu, wenn ein (formelles) Gesetz oder eine Rechtsverordnung dies vorsieht oder zwingend voraussetzt. *Eine Regelung per Satzung scheidet demnach aus*, sich die Datenverarbeitung auch nicht ansatzweise aus einem Gesetz ergibt.

Die Hundesteuersatzungen regeln lediglich, dass und aus welchem Anlass ein Hund an- bzw. abzumelden ist, nicht jedoch mit welchen personenbezogenen Daten dies zu erfolgen hat (Gebot der Normenklarheit). Auch die Mustersatzung des SSG enthält keine entsprechende Norm.

In einem Gespräch mit dem SMI und dem SSG im November 2000 wurde mir Abhilfe zugesagt.

Die Gemeinden sollten bis dahin auf die Datenerhebung sowie auf evtl. vorgesehene Bußgelder wegen unterlassener Mitteilung des neuen Hundehalters verzichten.

6.2 Flächendeckende Hundebestandsaufnahme

Der SSG veröffentlichte in einem Mitgliederrundschreiben auf Bitte des SMI die Stellungnahme der Staatsregierung zu 8/6.6, in der die Beauftragung von Privatunternehmen mit der Hundebestandsaufnahme im Wege der Auftragsdatenverarbeitung nach § 7 SächsDSG für zulässig erachtet wird.

Bereits im April 2000 hatte ich nochmals deutlich gemacht, dass es sich bei der Feststellung der Hundehalter (Erhebung der Besteuerungsgrundlage) um eine hoheitsrechtliche Tätigkeit im Bereich des Abgabenrechts handelt. Die §§ 85, 86, 88 bis 94 AO, die eindeutig das Über- und Unterordnungsverhältnis zwischen Obrigkeit und Steuerpflichtigen dokumentieren, sprechen unwiderleglich für diese Auffassung. § 3 Abs. 1 Nr. 3 SächsKAG erklärt diese Verfahrensvorschriften der AO mit der Folge für anwendbar, dass diese den Bestimmungen des SächsDSG als leges

speciales vorgehen. Die Erhebung von Besteuerungsgrundlagen nach Abgabenrecht ist eine hoheitsrechtliche Aufgabe und daher nicht gleichzusetzen mit Datenerhebungen i. S. v. § 3 Abs. 2 Nr. 1 SächsDSG. Die Übertragung hoheitsrechtlicher Aufgaben auf Private ist nur im Wege der Beleihung auf gesetzlicher Grundlage möglich.

Es ist deshalb fehlerhaft anzunehmen, dass die Übertragung einer hoheitsrechtlichen Aufgabe auf Privatunternehmen im Wege der Auftragsdatenverarbeitung gemäß § 7 SächsDSG zulässig sei. Da Datenverarbeitung für sich gesehen *keine Aufgabe* der Verwaltung, sondern lediglich ein (technisches) Hilfsmittel zur Erledigung der öffentlichen Aufgabe darstellt, kann § 7 SächsDSG keine Aufgabe der Verwaltung originär konstituieren.

Bei einer persönlichen Erörterung des Problems mit dem zuständigen Abteilungsleiter im SMI im Juni 2000 bestand ausdrücklich insoweit Einigkeit, ein Eindruck, der sich in den darauffolgenden Wochen und Monaten noch verstärkte, weil keine Gegenargumente mehr vorgetragen wurden.

Um so mehr hat mich die Veröffentlichung der Stellungnahme der Staatsregierung zu 8/6.6 in den SSG-Mitteilungen überrascht, die geeignet ist, die sächsischen Gemeinden zur (rechtswidrigen) Beauftragung privater Unternehmen mit der flächendeckenden Hundebestandsaufnahme zu verleiten.

Um evtl. Beanstandungen betroffener Gemeinden gemäß § 26 SächsDSG zu vermeiden, habe ich dem SMI ein nochmaliges Überdenken der Rechtssituation angeraten und um Richtigstellung in den SSG-Mitteilungen gebeten. Hierzu war man zwar nicht bereit, jedoch konnte in einer gemeinsamen Erörterung beim SMI Überlegungen in Gang gesetzt werden, die auf ein Umdenken in Sachen *„Erhebung von Besteuerungsgrundlagen als hoheitsrechtliche Aufgabe, die nicht im Wege der Auftragsdatenverarbeitung gemäß § 7 SächsDSG auf Private übertragen werden kann“* hoffen lassen.

6.3 Anerkennung von Werbungskosten für Auslandstudienreisen - Anforderung von Teilnehmerlisten und Versand von Kontrollmitteilungen

Eine als „endlose Geschichte“ anmutende Kontroverse mit dem SMF hat ein einvernehmliches Ende gefunden.

So soll als Ergebnis einer Erörterung eine OFD-Verfügung über die steuerliche Behandlung von Auslandsstudienreisen so modifiziert werden, dass unter Berücksichtigung des Grundsatzes der gleichmäßigen Besteuerung dem Recht auf informationelle Selbstbestimmung gleichermaßen Rechnung getragen wird.

Es soll deutlich herausgestellt werden, dass die Anforderung einer Liste über die Mitreisenden immer dann entfällt, wenn sich der homogene Teilnehmerkreis bereits aus den vom Steuerpflichtigen vorgelegten Unterlagen eindeutig ergibt.

In den Fällen, in denen eine Teilnehmerliste zur Feststellung des homogenen Teilnehmerkreises unabdingbar ist, führt das veranlagende Finanzamt stichprobenweise eine Prüfung der Berufsangaben durch Anfragen bei den für die weiteren Reiseteilnehmer zuständigen Finanzämtern durch .

Nach der Entscheidung über die Anerkennung/Nichtanerkennung der Werbungskosten legt das Finanzamt den Vorgang, einschließlich der Teilnehmerliste der OFD mit Bericht vor. Da nicht auszuschließen ist, dass auch andere Finanzämter (der Mitreisenden) die Teilnehmerliste der OFD vorlegen, sollen dort die Mehrexemplare unverzüglich gelöscht/vernichtet werden.
Ein Exemplar verbleibt sodann bei der OFD für einen noch festzulegenden Zeitraum (Bestandskraft, Verjährung?).

Vorteil: Die Teilnehmerlisten befinden sich nicht mehr (wie bisher) in verschiedenen Finanzämtern in den Steuerakten, sondern nur noch als Einzelexemplar bei der OFD.

„Kontrollmitteilungen“, die aus Gründen der gleichmäßigen Besteuerung an die für die Mitreisenden zuständigen Finanzämter geschickt werden, müssen personenbezogen sein, weil bei der von mir bisher angeregten allgemeinen Information die Gefahr besteht, dass sie „untergehen“. Dagegen findet ein entsprechender Hinweis in der Steuerakte der Mitreisenden bei einem Antrag auf Anerkennung von Werbungskosten für die Auslandsstudienreise Beachtung.

Im Hinblick auf den Grundsatz der gleichmäßigen Besteuerung sind meine bisher vorgetragenen Bedenken ausgeräumt. Ich habe das SMF um Übersendung der modifizierten OFD-Verfügung gebeten.

6.4 Kündigung eines städtischen Bediensteten wegen Steuerhinterziehung

Ein städtischer Bediensteter legte beim Finanzamt offensichtlich gefälschte Belege mit der Behauptung vor, er hätte Dienstreisen, Dienstgänge und Fachliteratur aus eigener Tasche zu bezahlen und dienstliche Akten zu Hause zu bearbeiten.

Das Finanzamt erkannte die geltend gemachten Werbungskosten nicht an. In seinem Einspruchsverfahren und bei verschiedener Anhörungen bestand der Bedienstete nachhaltig auf Anerkennung der Werbungskosten für Dienstreisen, Dienstgänge, Fachliteratur und häusliches Arbeitszimmer mit der Folge, dass das Finanzamt die Beschäftigungsbehörde zur Sachverhaltsaufklärung einschaltete.

Dies führte zur Kündigung des Bediensteten.

Der an Kündigungsverfahren zu beteiligende Personalrat vermutete einen Verstoß des Finanzamtes gegen das Steuergeheimnis (§ 30 AO) und bat mich um Stellungnahme.

Ich verwies auf § 93 Abs. 1 Satz 3 AO, wonach andere Personen (dazu zählen auch juristische Personen - § 93 Abs. 1 Satz 2 AO) zur Auskunft angehalten werden sollen

(„sollen“ bedeutet in der Regel „müssen“), wenn u. a. die Sachaufklärung durch den Beteiligten *keinen Erfolg verspricht.* Diese Voraussetzungen liegen vor, wenn nach den Umständen des Falles oder nach den Erfahrungen mit dem Beteiligten eine Sachaufklärung durch ihn nicht zu erwarten ist. Ob die Sachaufklärung durch den Beteiligten zum Ziele führt oder Erfolg verspricht oder ob dies nicht zutrifft, ist eine Frage der (vorweggenommen) Beweiswürdigung. Diese Würdigung ist Sache des Finanzamtes, nicht Sache des Auskunftspflichtigen (vgl. Tipke/Kruse Rdnr. 4a zu § 93 Abs. 1 Satz 3 AO).

Auch wies ich auf das Schreiben des BMF vom 10. Mai 2000, Az.: IV A 4-S 0130-19/00 hin, in dem geregelt ist, unter welchen Voraussetzungen steuerrechtlich geschützte Daten (§ 30 AO) an die für dienstrechtliche/arbeitsrechtliche Maßnahmen zuständigen Stellen mitgeteilt werden dürfen. Eine Mitteilung darf danach u. a. dann erfolgen, wenn der Bedienstete eine erhebliche kriminelle Energie an den Tag gelegt hat, etwa bei der Fälschung von Belegen (das BMF-Schreiben ist in der Zeitschrift „Der Betrieb“ DB 22/00, S. 1103 abgedruckt).
Die Vorgehensweise des Finanzamtes war korrekt.

6.5 Versand eines Grundsteuer-Änderungsbescheids an den Wohnungsverwalter. Wurde hier das Steuergeheimnis verletzt?

In einer Eingabe hatte ich mich mit folgendem Sachverhalt zu befassen:

Ein Petent besitzt eine Eigentumswohnung, die vermietet ist. Das Stadtsteueramt sandte den Grundsteuer-Änderungsbescheid nicht an ihn, sondern wie schon in den Vorjahren an die Hausverwaltungsgesellschaft (Verwalter) in der Annahme, sie sei Zustellungsvertreter. Eine *ausdrückliche* Vollmacht, die den Verwalter zum Empfang von Grundsteuerbescheiden ermächtigt hätte, hatte der Petent nicht erteilt. In den Akten des Stadtsteueramtes befand sich jedoch die Kopie des Verwaltervertrages, der von allen Eigentümern unterzeichnet worden war. Darin hieß es: „Der Verwalter ist berechtigt ... Willenserklärungen und Zustellungen entgegenzunehmen, soweit sie an alle Wohnungseigentümer in dieser Eigenschaft gerichtet sind.“ In dieser Formulierung sah das Stadtsteueramt eine umfassende Vollmacht zu Gunsten des Verwalters, zumal dieser entsprechend auftrat, z. B. den Schriftverkehr und Verhandlungen führte und die Grundsteuer für den Petenten und die anderen Eigentümer überwies. Hinzu kam, dass der Petent die zuvor in gleicher Weise adressierten Grundsteuerbescheide niemals moniert hatte.

Die Zustellung des letzten Grundsteuer-Änderungsbescheids betrachtete der Petent nunmehr als unbefugte Offenbarung seiner vom Steuergeheimnis gemäß § 30 AO geschützten Daten.

Aus meiner Sicht bietet dieser Sachverhalt keine Anhaltspunkte für einen Datenschutzverstoß, und zwar aus folgenden Gründen.

Gemäß § 122 Abs. 1 AO kann ein Verwaltungsakt auch gegenüber einem Bevollmächtigten bekanntgegeben werden. Besteht eine *allgemeine* Vertretungsvollmacht i. S. v. § 80 Abs. 1 AO, so ist der Bevollmächtigte auch zum Empfang und zur Kenntnisnahme von Steuerbescheiden berechtigt. Nur wenn keine allgemeine Vollmacht vorliegt, ist eine besondere Vollmacht für die Zustellung erforderlich (Tipke-Kruse, Kommentar zur Abgabenordnung, § 122 AO, Tz. 43).

Offenbar ist das Stadtsteueramt aufgrund des Auftretens des Verwalters, der seine Vollmacht mit dem Verwaltervertrages belegte, eines fehlerhaften Verständnisses des Vertragstextes sowie des Duldungsverhaltens des Petenten von einer solchen allgemeinen Vertretungsvollmacht des Verwalters ausgegangen und hat ihm deshalb den Bescheid gemäß § 122 Abs. 5 AO zugestellt. Das ergab sich aus einem Schreiben des Stadtsteueramtes an den Petenten. Darin hieß es: „Bereits an Ihren Verwalter bekanntgegebene Steuerbescheide wurden bisher von Ihnen nicht beanstandet. Sollte zwischenzeitlich eine Änderung zu der von Ihnen erteilten Verwaltervollmacht eingetreten sein, bitten wir um Ihre Mitteilung."

Im Regelfall geht die Zustellung eines Steuerbescheids an einen zum Empfang nicht Berechtigten mit der Verletzung des Steuergeheimnisses einher. Ob hier für den Verwalter eine Anscheinsvollmacht, vielleicht auch eine Duldungsvollmacht vorlag und ob die dazu für das Zivilrecht entwickelten Grundsätze auch für das Steuerrecht gelten, habe ich dahinstehen lassen. Selbst wenn man davon ausgeht, dass keine ausreichende Vollmacht vorlag, erscheint eine Verletzung des Steuergeheimnisses zweifelhaft; denn Voraussetzung dafür ist die unbefugte *Offenbarung* von Verhältnissen eines anderen.

Das Offenbaren von Verhältnisses bedeutet jedoch, dass jemandem Verhältnisse mitgeteilt werden, die diesem noch nicht bekannt sind (Tipke-Kruse, Kommentar zur Abgabenordnung, § 30, Tz. 31). Dem Verwalter waren jedoch die „Grundsteuerverhältnisse" des Petenten sehr wohl bekannt: das Eigentum an der Wohnung, der Grundsteuer-Messbetrag und die für ihn auf sein Grundsteuerkonto überwiesenen Beträge. Der auf Beschluss des Stadtrats geänderte Hebesatz gehört meiner Auffassung nach weder zu den „Verhältnissen des Steuerpflichtigen", noch ist er durch den Steuerbescheid „offenbart" worden.

In der Gesamtschau war für mich kein Datenschutzverstoß zu erkennen, der den Petenten in seinem Persönlichkeitsrecht verletzt hätte. Dem Stadtsteueramt habe ich - zur Vermeidung von Ärger - empfohlen, als Adressaten künftig stets den Steuerpflichtigen zu benennen, wenn dieser keine eindeutige und schriftliche Zustellungsvollmacht erteilt hat.

6.6 Die Ausstellung von Lohnsteuerkarten für Kinder und das Jugendarbeitsschutzgesetz

§ 52 JArbSchG lautet: „Über die Ausstellung von Lohnsteuerkarten an Kinder im Sinne von Abs. 1 und 3 ist die Aufsichtsbehörde durch die ausstellende Behörde zu unterrichten."

Ein Gewerbeaufsichtsamt forderte die Meldebehörden in seinem Zuständigkeitsbereich auf, bei der Ausstellung von Lohnsteuerkarten für Kinder den Arbeitgeber zu erfragen und diesen im Rahmen der Mitteilung nach § 52 JArbSchG anzugeben. Dem Vernehmen nach sollen die Meldebehörden der Aufforderung gefolgt sein - bis auf eine. Die hatte Zweifel an der Rechtmäßigkeit der Datenerhebung und trug das Problem an mich heran.

Auch aus meiner Sicht gab es weder für die Datenerhebung (Ermittlung des Arbeitgebers) noch die Datenübermittlung (Mitteilung des ermittelten Arbeitgebers) eine Rechtsgrundlage, und zwar aus folgenden Gründen:

Im Zuge der Ausstellung von Lohnsteuerkarten handeln die Gemeinden gemäß § 39 Abs. 6 EStG als Landesfinanzbehörden. Da die Meldebehörden insoweit Steuerrecht vollziehen, haben sie die einschlägigen steuerrechtlichen Vorschriften zu beachten. Diese regeln in §§ 39 ff EStG sowie in R 108 bis R 110 LStR das Verfahren.

Gemäß R 108 Abs. 2 LStR hat die Gemeinde „die Lohnsteuerkarten auf Grund ihrer melderechtlichen Unterlagen, z. B. Melderegister oder Einwohnermeldekartei, auszustellen“. § 5 SächsMG zählt die Daten abschließend auf, die von der Meldebehörde im Melderegister gespeichert werden dürfen; der Arbeitgeber des Betroffenen gehört *nicht* dazu. Nichts anderes ergibt sich aus § 6 SächsMG für die Datenerhebung. Auch das Jugendarbeitsschutzgesetz sieht spezialgesetzlich weder die Erhebung von Arbeitgeberdaten vor noch deren Übermittlung, soweit sie der Meldebehörde (z. B. aus einem Gespräch) bekannt sind. § 52 JArbSchG bestimmt lediglich, dass die Aufsichtsbehörde (Gewerbeaufsichtsamt) über die Ausstellung von Lohnsteuerkarten an Kinder zu unterrichten ist. Die in den einschlägigen Kommentaren zum Jugendarbeitsschutzgesetz vertretene Auffassung, ein ggf. bekannter Arbeitgeber sei mitzuteilen, ist für mich nicht nachvollziehbar.

Ich habe bei der Oberfinanzdirektion Chemnitz angeregt, in dem jährlich von ihr herausgegebenen „Merkblatt für die Gemeinden über die Ausstellung und Übermittlung der Lohnsteuerkarten“ die den Gewerbeaufsichtsämtern zu übermittelnden Daten (Name, Anschrift, Geburtsdatum) im Einzelnen aufzuführen. Mir wurde zugesagt, das Merkblatt für das Jahr 2001 entsprechend zu ergänzen.

7 Kultus

7.1 Datenschutz in der Schule

7.1.1 Kopfnoten und verbale Einschätzungen auf Zeugnissen

Seit 1. August 1999 wird im Verordnungswege vorgeschrieben, Betragen, Fleiß, Mitarbeit und Ordnung mit den Noten 1 bis 5 zu bewerten (Kopfnoten). Außerdem ist diese Bewertung durch „verbale Einschätzungen“ zu ergänzen und zu präzisieren.

Verschiedene Schulleiter hielten diese Regelung für rechtswidrig und baten mich um datenschutzrechtliche Prüfung. Schließlich würden die in Frage stehenden Kopfnoten

und verbalen Einschätzungen das Persönlichkeitsrecht der betroffenen Schüler nicht unerheblich berühren, z. B. wenn die Zeugnisse bei Lehrstellenbewerbungen von den Ausbildungsbetrieben verlangt werden.

Da ich im Schulgesetz keine ausreichende Verordnungsermächtigung - zumindest für die verbalen Einschätzungen - sah, erörterte ich das Problem ausführlich mit dem SMK, ohne dass die Angelegenheit bislang abgeschlossen werden konnte.

Das SMK vertritt die Ansicht, durch § 62 Abs. 1 und Abs. 2 Nr. 10 SchulG ermächtigt zu sein, durch Rechtsverordnung Einzelheiten der Schulverhältnisse, so auch die Kopfnoten und verbalen Einschätzungen in Zeugnissen regeln zu dürfen und beruft sich auf umfangreiche Rechtsprechung und Verfahrensweisen in anderen Bundesländern.

Im Hinblick auf die umfangreiche Rechtsprechung des Bundesverfassungsgerichts zum Bestimmtheitsgebot des Art. 80 Abs. 1 Satz 2 GG bin ich - unter Zurückstellung ursprünglicher Zweifel - der Auffassung des SMK gefolgt, dass § 62 Abs. 2 Nr. 10 SchulG für die Kopfnoten selbst als ausreichende Verordnungsermächtigung angesehen werden kann, weil sich Inhalt, Zweck und Ausmaß aus dem Schulgesetz in der Gesamtschau ermitteln lassen (vgl. BVerfGE 19, 361; 42, 200).

Dies gilt jedoch nicht für die verbalen Einschätzungen.

Das Bundesverfassungsgericht stellt neben den oben zitierten Entscheidungen nämlich auch fest, dass die Bestimmtheit der Ermächtigungsnorm der Grundrechtsrelevanz der Regelung entsprechen muss, zu der ermächtigt wird. Greift die Regelung erheblich in die Rechtsstellung des Betroffenen ein, so müssen höhere Anforderungen an den Bestimmtheitsgrad der Ermächtigung gestellt werden, als wenn es sich um einen Regelungsbereich handelt, der die Grundrechtsausübung weniger tangiert (BVerfGE 41, 266; 58, 278; 62, 210).

Es liegt auf der Hand, dass verbale Einschätzungen in das Persönlichkeitsrecht der Schüler erheblich tiefer eingreifen können als herkömmliche, an Leistungen orientierte Schulnoten. Freitextfelder bieten dem Lehrer die Möglichkeit, Persönlichkeitsbewertungen, Charakterbilder, Hinweise zur Verhaltensstruktur, Haltungsbeschreibungen zur sozialen Kompetenz und ähnliche Analysen verbal frei abzugeben, die der Obrigkeit - und der Lehrer verkörpert sie - ohne klare, vorhersehbare Rechtsgrundlagen in einer freien Gesellschaft nicht zustehen. Der Appell des SMK und der Regionalschulämter an die Lehrer, von negativen Formulierungen abzusehen, ändert daran nichts. Jedes Votum zur Persönlichkeit ist an klare, spätestens vor Gericht eindeutig beweisbare und rechtlich bestimmte Voraussetzungen geknüpft. Was wäre von einer Bewertung zu halten wie „wirkt glatt“, „spricht schnell“, „argumentiert gelöst“, „hat viele Ideen“, „Saisonarbeiter“, „Matthias bewährt sich in der Klassengemeinschaft, gibt aber zu schnell auf“.

Die besondere Eingriffstiefe solcher verbalen Einschätzungen wird insbesondere bei Schulwechseln oder Lehrstellenbewerbungen deutlich. Es ist bereits üblich, dass der

Lehrmeister sich nicht nur das „cleane“Abgangszeugnis, sondern auch frühere Zeugnisse vorlegen lässt.

Deshalb ist dem verfassungsrechtlichen Bestimmtheitsgebot in besonderem Maße Rechnung zu tragen. Wegen des beispielhaften Charakters der Aufzählung in § 62 Abs. 2 SchulG dürfen keine Regelungen über verbale Einschätzungen - am Bestimmtheitsgebot vorbei - getroffen werden.

Ähnliche Verfahrensweisen in Baden-Württemberg und Rheinland-Pfalz sind nicht vorbildlich, denn auch dort dürften die entsprechenden Regelungen dem verfassungsrechtlichen Bestimmtheitsgebot nicht gerecht werden. Diesbezüglich habe ich meine Datenschutzkollegen in beiden Bundesländern informiert.

Da es ersichtlich an einer Verordnungsermächtigung mangelt, die Art. 75 Abs. 1 Satz 2 SächsVerf entspricht, halte ich die Regelungen über verbale Einschätzungen in den sächsischen Schulordnungen für rechtswidrig.

Entweder wird in den Schulordnungen künftig auf verbale Einschätzungen verzichtet - im Elterngespräch sollten diese Bewertungen abgegeben und erörtert werden, aber nicht auf dem Dokument „Zeugnis“, das für unbeteiligte Dritte bestimmt ist; ich könnte mir auch einen Elternbrief vorstellen, der die freie Bewertung von Verhalten und Leistung enthält - oder es wird dafür (im Schulgesetz) eine Rechtsgrundlage geschaffen, die dem Bestimmtheitsgebot entspricht. Das dürfte nicht leicht fallen.

Das SMK hält jedoch nach wie vor aus „*schulfachlicher*“ Sicht eine Beibehaltung der verbalen Untersetzungen der Kopfnoten, allerdings mit Ausnahme der Abschlusszeugnisse, für „*sinnvoll*“ und vermochte „angesichts der in anderen Bundesländern bestehenden Regelungen“ meinen *rechtlichen* Einwänden gegen diese Verfahrensweise nicht in allen Punkten zu folgen (dem „Sinnvoll Erachten aus schulfachlicher Sicht“ wird demnach vor „rechtlichen Erfordernissen“ der Vorzug gegeben).

Da der Staatsminister für Kultus mir versichert hat, sich dafür einzusetzen, dass im Zuge der Novellierung des Schulgesetzes meinen Hinweisen baldmöglichst Rechnung getragen wird, verzichte ich einstweilen auf *rechtliche* Überzeugungsarbeit.

7.1.2 Viele Fragen bei der Schulfähigkeitsuntersuchung offen

Schulpflichtig gewordene Kinder werden vor der Einschulung einer Schulfähigkeitsuntersuchung unterzogen. Diese besteht aus zwei Teilen: einer ärztlichen Untersuchung durch den Kinder- und Jugendärztlichen Dienst der Gesundheitsämter und einem unabhängig davon durchgeführten pädagogischen Test durch einen Lehrer der künftigen Grundschule. Das Ergebnis der ärztlichen Untersuchung wird dem Grundschulleiter mitgeteilt (Bedenken / keine Bedenken gegen die Einschulung). Diese Mitteilung und der pädagogische Test bilden die Grundlagen für die Entscheidung des Schulleiters, ob das Kind in die erste Klasse aufgenommen wird.

In einer Eingabe hat mir ein Petent Einzelheiten über die Schulfähigkeitsuntersuchung seines Kindes mitgeteilt. Er kritisierte zum einen den Fragebogen zur Anamnese des Kindes im Vorfeld der ärztlichen Untersuchung. Zwar enthalte er einen Hinweis auf die Freiwilligkeit der Angaben, gleichwohl hätte das Gesundheitsamt auf der Beantwortung der Fragen bestanden. Zum anderen kritisierte er den in der Schule durchgeführten „pädagogischen" Test. Hierbei hätte es sich um einen veritablen psychometrischen Schulreifetest gehandelt, der nicht von einer qualifizierten Fachkraft, sondern „fröhlich und unbekümmert" von einer Lehrerin durchgeführt worden sei. Ein Laie sei jedoch mit den Grundlagen der Testtheorie nicht vertraut und regelmäßig nicht in der Lage, aus den erhobenen Daten die richtigen Schlüsse zu ziehen. Als Fachmann könne er dies beurteilen.

Die Eingabe war für mich Anlass, mich eingehender mit der Gesamtproblematik zu befassen, und zwar mit folgendem Ergebnis:

1. *Rechtsgrundlagen*

   Aus meiner Sicht reichen §§ 27 Abs. 4 Satz 2 und 59 Abs. 5 SchulG als Rechtsgrundlagen für die derzeit durchgeführten ärztlichen und pädagogischen Schulfähigkeitsuntersuchungen nicht aus. Auch ermächtigt § 62 Abs. 2 Nr. 11 SchulG m. E. nicht zum Erlass einer Rechtsverordnung, die diese Untersuchungen regelt. Folglich wären § 3 Abs. 1 der Schulgesundheitspflegeverordnung (ärztliche Schulaufnahmeuntersuchung) und § 4 Abs. 3 der Schulordnung Grundschulen (Pflicht zur ärztlichen Schulaufnahmeuntersuchung) rechtswidrig.

   Meine Rechtsauffassung habe ich dem SMS und SMK dargelegt. Wie mir mitgeteilt wurde, werde derzeit ein Gesetzentwurf erarbeitet zur Änderung des Gesetzes über den öffentlichen Gesundheitsdienst, des Schulgesetzes sowie des Gesetzes zur Förderung von Kindern in Kindertageseinrichtungen. Auch die Folgeänderungen in der Schulgesundheitspflegeverordnung des SMK seien in Vorbereitung.

2. *Pädagogische Tests durch Lehrkräfte*

   Dieser, weder durch Rechtsverordnungen noch Verwaltungsvorschriften konkretisierte Bereich hat dem Vernehmen nach inzwischen zu einem „Wildwuchs" geführt. Deshalb wurde vom SMK eine Arbeitsgruppe eingerichtet, welche die Notwendigkeit solcher Tests erörtern und ggf. Vorgaben erarbeiten soll. Mir wurde zugesagt, mich zu gegebener Zeit zu beteiligen.

3. *Inhalt Anamnesebogen für die ärztliche Untersuchung*

   Ich habe die Erforderlichkeit der mit dem Anamnesebogen erhobenen Daten in Frage gestellt, z. B. über die Erkrankungen der Mutter während der Schwangerschaft, über Geburtsverlauf, Geburtsgewicht, kindliche Entwicklung (Wann hat es die erste Zähne bekommen, wann hat es sprechen, wann laufen gelernt?), sämtliche Kinderkrankheiten, gesundheitliche Besonderheiten, den behandelnden Arzt, verabreichte Medikamente usw.

   Das SMS wird ein Gutachten in Auftrag geben, in dem die Erforderlichkeit / Nicht-Erforderlichkeit jedes einzelnen Merkmals geprüft und begründet wird.

Auch soll die Frage untersucht werden, ob der Anamnesebogen vom untersuchenden Arzt generell oder nur dann zu verlangen ist, wenn begründete Zweifel an der Schulfähigkeit des Kindes bestehen.

4. *Statistik*
   Gegen die von den Gesundheitsämtern im Rahmen der Schulfähigkeitsuntersuchungen erstellte Statistik bestehen keine datenschutzrechtlichen Bedenken, weil sie im Sinne des Sächsischen Statistikgesetzes die Merkmale einer Statistik im Verwaltungsvollzug erfüllt.

Ich hoffe, die Angelegenheit ist auf einem guten Weg.

7.1.3 Datenerhebung bei Schülern durch Privatunternehmen im Rahmen von Schulveranstaltungen

Im Dezember des letzten Jahres hat die Volksbank Dresden für Schulen eine Informationsveranstaltung zum Euro durchgeführt. Im Zuge der Veranstaltung wurden die Schüler zur Teilnahme an einem Quiz aufgefordert und gebeten, Namen und Anschrift anzugeben, obwohl die Gewinne an Ort und Stelle verteilt wurden. Wie sich zeigen sollte, war das Quiz lediglich ein Vorwand für die Erhebung von Anschriftendaten; denn kurze Zeit später wurden sie für Zwecke der Kundenwerbung genutzt. Da hieß es in den Schreiben an die Schüler: „Komm einfach mit Deinen Eltern in die Volksbank Dresden und schon kannst Du ganz selbstständig Geldgeschenke einzahlen oder Taschengeld abheben. [...] Hast Du schon einmal daran gedacht, Dir später etwas ganz Tolles zu kaufen, ein Auto zum Beispiel. Du weißt nur nicht, wie Du Dir das leisten kannst?! Dann komm zu uns - wir reden darüber und planen ganz genau, wie Du das schaffen kannst!“

Mit Recht empörte Eltern wandten sich in einer Eingabe an mich, u. a. weil sie vermuteten, die Schule hätte der Volksbank Listen mit den Namen und Anschriften der Schüler übermittelt. Dies hat sich - wie in allen vergleichbaren Fällen bisher - *nicht* bestätigt. Stets war es so, dass die Schüler die Daten selbst angegeben haben.

Immer wieder verbinden Privatunternehmen Schülerveranstaltungen mit einfachen geschäftlichen Interessen. Dabei bedienen sie sich der unterschiedlichsten Methoden, um an Adressdaten zu gelangen. So werden Schüler z. B. anlässlich von Betriebsbesichtigungen aufgefordert, sich zum Nachweis von Betriebsausgaben für einen Imbiss in eine Anwesenheitsliste einzutragen, oder man animiert sie zur Teilnahme an einem Wettbewerb, Preisausschreiben oder wie hier einem Quiz. Auch wird den Schülern vorgegaukelt, man benötige Namen und Anschriften, um ihnen versprochene Klassenfotos, Poster, Informationsmaterial zu Bewerbungen („Wie bewerbe ich mich erfolgreich?“) o. Ä. zusenden zu können. Das geschäftliche Interesse hinter solchen Datenerhebungen durchschauen auch die beteiligten Lehrkräfte nicht immer.

Ich habe beim SMK angeregt, die Schulleiter auf derartige Praktiken von Privatunternehmen - vorzugsweise Sparkassen, Banken, Versicherungen, Krankenkassen - aufmerksam zu machen, damit die Schüler bereits vor der jeweiligen Veranstaltung über

die wirklichen Absichten der Unternehmen informiert werden können oder damit die Verantwortlichen bereits im Vorfeld mit den Veranstaltern vereinbaren, auf personenbezogene Schülerdaten zu verzichten.

7.1.4 Diese Datenerhebung zur Bewilligung der Fördermittel für eine Volkshochschule ging zu weit

Nach der „Richtlinie des SMK zur Förderung der Weiterbildung“ vom 20. Februar 1997 erhält eine Weiterbildungseinrichtung nur dann Fördermittel, wenn sie als förderungswürdig anerkannt ist. Der Antrag zum Anerkennungsverfahren ist vorgeschrieben und verlangt zur Personalausstattung *zahlenmäßige* Angaben; im Antragsformular für die jährlichen Fördermittel ist die ausgeübte Tätigkeit und die Qualifikation des *hauptberuflich-pädagogischen* Personals in pseudonymisierter Form anzugeben. Gegen die Richtlinie und die vorgeschriebenen Formblätter ist datenschutzrechtlich nichts einzuwenden.

Bei einer als förderungswürdig anerkannten Volkshochschule, die u. a. Kreativkurse für Behinderte (Malen, Fotografie, Tanz, Heimatkunde, Kochen) von Honorardozenten *nebenberuflich* durchführen lässt, fragte die Bewilligungsbehörde abweichend von der Förderrichtlinie nach den Qualifikationen, einschlägigen Berufserfahrungen und die hauptberuflichen Tätigkeiten dieser Honorardozenten. Darüber hinaus stellte sie über die behinderten Kursteilnehmer u. a. folgende Fragen:

- Welche Ausbildung haben die geistig behinderten bzw. mehrfach schwerbehinderten Teilnehmer?
- Welche Lernziele lassen sich bei dem Grad/Art der Behinderung erreichen?

Die Volkshochschule berief sich auf den Datenschutz und beantwortete die Fragen zu den Dozenten durch eine nicht personenbezogene Auflistung der Berufe und Vorbildungen, aber die Fragen zu den Behinderten überhaupt nicht. Das SMK bat mich um Prüfung, ob die Datenerhebung über die Behinderten rechtmäßig sei. Dies habe ich verneint, weil es keine Rechtsgrundlage für eine solche Datenerhebung bei Dritten gibt, weder spezialgesetzlich, z. B. in der Sächsischen Haushaltsordnung, noch nach § 11 Abs. 4 SächsDSG.

Hinzu kommt, dass eine Volkshochschule die von der Bewilligungsbehörde verlangten Daten weder erheben noch speichern dürfte, da sie zu ihrer Aufgabenerfüllung nicht erforderlich sind (§ 11 Abs. 1 SächsDSG). Salopp könnte man sagen: Kreativkurse an einer Volkshochschule kann im Nebenberuf - oder auch ohne Beruf - grundsätzlich jeder einschlägig begabte Laie durchführen (z. B. Hobbyköchinnen im Kochen, Sonntagsmaler im Zeichnen, Rentnerinnen in Volkstanz, Autoverkäufer in Heimatkunde). Für eine solche nebenberufliche Lehrtätigkeit ist weder eine einschlägige Qualifikation noch eine einschlägige hauptberufliche Tätigkeit notwendig. Ebensowenig ist die Vorbildung eines Teilnehmers zur Belegung eines Kreativkurses von Bedeutung, noch schon gar nicht darf die Teilnahme von Art und Grad der Behinderung anhängig gemacht werden.

Andererseits ist das Anliegen des SMK verständlich: Denn die Fördermittel sollen nur für wirklich qualifizierte Lehrende und Lernende ausgereicht werden.

Deshalb bleibe ich mit dem SMK in konstruktiven Verhandlungen.

7.1.5 Einrichtung von E-Mail Adressen für Schüler

Ein Schulleiter fragte mich, ob es datenschutzrechtliche Bedenken gegen die Einrichtung von E-Mail-Adressen für Schüler gibt.

Die wichtigste Voraussetzung für die Zulässigkeit der Verarbeitung von personenbezogenen Daten ist, dass sie zur gesetzlichen Aufgabenerfüllung der öffentlichen Stelle, in diesem Fall der Schule, erforderlich ist. Davon bin ich ausgegangen; denn die angestrebte Kommunikationsform zwischen Schülern, Lehren und Dritten über das Internet dürfte dem in § 1 SchulG definierten Erziehungs- und Bildungsauftrag dienen. Also habe ich mich wie folgt geäußert:

Die Einrichtung der E-Mail-Adressen und die sich daran anschließende Nutzung sind notwendigerweise mit Datenverarbeitungsvorgängen im Sinne von § 3 SächsDSG verbunden, insbesondere mit dem Erheben, Speichern, Übermitteln und Löschen von Schülerdaten. Da das Schulgesetz und die dazu ergangenen Rechtsverordnungen den Umgang mit moderner Kommunikationstechnik nicht bereichsspezifisch regeln und kein Schüler verpflichtet ist, sich eine E-Mail-Adresse „verpassen zu lassen“, darf sie nur mit dessen Einwilligung eingerichtet werden (§ 4 Abs. 1 Nr. 2 SächsDSG).

Eine datenschutzgerchte Einwilligung erfordert die Aufklärung des Betroffenen über den Verwendungszweck seiner Daten und die Freiwilligkeit, außerdem ist ein Hinweis auf etwaige Folgen bei Verweigerung der Einwilligung notwendig. Aus der Verweigerung der Einwilligung dürfen dem Schüler jedoch keine Nachteile entstehen (z. B. Ausschluss von Lehrinhalten oder organisatorischen Informationen über den Schulbetrieb). Im vorliegenden Fall halte ich es sogar für unabdingbar, die Betroffenen auch über die „Gefahren des Internets“ und über die von der Schule getroffenen Gegenmaßnahmen aufzuklären.

Bei minderjährigen Schülern stellt sich die Frage, ob sie ohne einen Sorgeberechtigten einwilligen dürfen. Die datenschutzrechtliche Einwilligung ist nicht von der bürgerlich-rechtlichen Geschäftsfähigkeit, sondern von der Einsichtsfähigkeit abhängig. Da diese ab dem 15. Lebensjahr angenommen wird, ist bei jüngeren Schülern deshalb eine gemeinsame Einwilligungserklärung mit einem Sorgeberechtigten erforderlich.

Das SMK habe ich gebeten, alle Schulen entsprechend zu informieren.

7.1.6 Fragen zum Klassentreffen

Ich unterstütze die Organisation von Klassentreffen, so gut ich kann. In 7/7.4 habe ich mich zur geschäftsmäßigen Organisation von Klassentreffen geäußert. Welche Unter-

lagen aber dürfen ehemalige Schüler einsehen, welche Daten darf ihnen die Schule mitteilen, wenn sie selbst ein Klassentreffen organisieren wollen? Zu diesem Thema erreichen mich immer wieder Anfragen. Zum Beispiel:

Darf die Schule noch vorhandene Klassenbücher den Ehemaligen zum Zweck der gemeinsamen Erinnerung am Tag des Klassentreffens herausgeben?

Nein: Bei der Einsichtnahme in die Klassenbücher würde ein ehemaliger Schüler nicht nur Kenntnis von den eigenen Daten, sondern - gewollt oder ungewollt - auch Kenntnis von den Daten seiner Mitschüler erhalten. Eine Übermittlung dieser personenbezogenen Daten durch die Schule an private Dritte ist nur unter den Voraussetzungen von § 15 SächsDSG zulässig. Diese Vorschrift erlaubt die Übermittlung nur, wenn

- sie zur Erfüllung der Aufgaben der übermittelnden Stelle erforderlich ist *und* für Zwecke erfolgt, für die eine Nutzung nach § 12 Abs. 1 bis 4 SächsDSG zulässig wäre, oder
- der Empfänger ein berechtigtes Interesse an der Kenntnis der Daten glaubhaft darlegt *und* der Betroffene kein schutzwürdiges Interesse am Unterbleiben der Übermittlung hat. Zur Feststellung des schutzwürdigen Interesses wäre der Betroffene gemäß § 15 Abs. 3 SächsDSG vor der Übermittlung zu hören.

Nach der 1. Alternative kommt eine Übermittlung schon deshalb nicht in Betracht, weil es für die Aufgabenerfüllung der Schule nicht erforderlich ist, Erinnerungen ehemaliger Schüler aufzufrischen.

Nach der 2. Alternative müsste die Schule - das Klassentreffen als berechtigtes Interesse unterstellt (s. u.) - sämtliche in den Klassen- oder Gruppenbüchern genannten Schüler anschreiben (und zuvor die aktuellen Anschriften sowie ggf. Namensänderungen nach Eheschließung feststellen), um ein evtl. bestehendes schutzwürdiges, der Datenübermittlung entgegenstehendes Interesse zu erkunden. Dazu ist die Schule nicht verpflichtet. Wenn ein Schulleiter also ein diesbezügliches Anliegen ehemaliger Schüler „aus Datenschutzgründen“, sozusagen mit einer Kurzformel, ablehnt, so hat das seine Richtigkeit.

Ein anderes Beispiel:

Darf die Schule einem ehemaligen Schüler eine Liste mit den Namen und Adressen seiner früheren Mitschüler aushändigen?

Ja: Derartige Auskünfte sind gemäß § 15 Abs. 1 Nr. 1 i. V. m. §§ 12 Abs. 2 Nr 1 und 11 Abs. 4 Nr. 8 SächsDSG zulässig; denn zum Auftrag der Schule gehört es auch, die Organisation von Klassentreffen zu unterstützen. Wir leben in Sachsen in einem Kulturstaat. Aufgabe der Schule ist deshalb nicht nur die bloße Wissensvermittlung, sondern auch die Pflege der Tradition und des Zusammengehörigkeitsgefühls ehemaliger Schüler und Lehrer. Ich halte es deshalb für sachgerecht und mit den Aufgaben und Befugnissen einer staatlichen Schule vereinbar, wenn sie einem ehemaligen

Schüler die Adressen seiner damaligen Mitschüler überlässt. Allerdings darf der Empfänger die Adressdaten nur zu dem Zweck nutzen, zu dem er sie von der Schule erhalten hat (§ 15 Abs. 4 SächsDSG).

7.1.7 Überprüfung der Angaben in einer Entschuldigung wegen Krankheit durch den Schulleiter

In einer Eingabe wurde ich gefragt, ob ein Schulleiter den in einer Entschuldigung als Fehlgrund angegebenen Arztbesuch durch Rückfrage bei dem (vermutlich) behandelnden Arzt überprüfen dürfe. Dies habe ich aus folgenden Gründen verneint:

§ 2 Abs. 3 SBO ist eindeutig. Danach hat *der Entschuldigungspflichtige* bei einer Krankheitsdauer von mehr als fünf Tagen oder bei auffällig häufigen oder langen Erkrankungen, wenn es der Schulleiter verlangt und begründet, ein ärztliches Zeugnis beizubringen. Eine andere Form der Datenerhebung, z. B. durch Nachforschungen bei Dritten (hier dem Arzt), ist nicht vorgesehen und damit rechtswidrig.

Vor dem Hintergrund, dass es offenbar immer wieder Ärzte gibt, die unter Missachtung ihrer ärztlichen Schweigepflicht den Schulen Auskunft erteilen anstatt sie zu verweigern, habe ich das SMK gebeten, die Schulleiter auf die Rechtslage hinzuweisen. Dies ist geschehen.

7.2 Kirchlicher Datenschutz

Die Direktion der Evangelischen Brüder-Unität Herrnhut hat am 19. September 1995 beschlossen, das „Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland (DSG-EKD)“ vom 12. November 1993 (ABl. EKD 1994 S. A 15) für ihren deutschen Bereich zu übernehmen. Sie hat den entsprechenden Synodenbeschluss, die Ausführungsbestimmungen sowie ein Merkblatt zum Datenschutz mit einer dazugehörigen Verpflichtungserklärung vorgelegt. Nach Prüfung der vorgelegten Unterlagen habe ich mein Einvernehmen mit der Feststellung erklärt, dass im Bereich der Evangelischen Brüder-Unität ausreichende Datenschutzregelungen gemäß § 14 SächsDSG gelten bzw. Maßnahmen gemäß § 30 Abs. 3 SächsMG getroffen sind.

Darüber hinaus habe ich das SMK darauf hingewiesen, dass auch für die Kirchen Novellierungsbedarf aufgrund der EG-Richtlinie besteht. Ich werde das Gespräch mit den Kirchen und dem SMK suchen, um uns über eine Verfahrensweise für die Zwischenzeit bis zur Umsetzung im kirchlichen Bereich zu verständigen.

8 Justiz

8.1 Staatsminister übermittelt personenbezogene Daten aus einem Ermittlungsverfahren an Privatperson

Aufgrund eines schwerwiegenden Datenschutzverstoßes musste ich gegenüber dem - inzwischen nicht mehr im Amt befindlichen - Staatsminister der Justiz eine Beanstandung aussprechen: Der Staatsminister hatte ausweislich eines von ihm gefertigten Aktenvermerks einen Bericht der Staatsanwaltschaft und dessen Auswertung im eigenen Hause angefordert und Informationen daraus weitergegeben, um einen örtlich involvierten, ihm politisch nahestehenden Landtagsabgeordneten über ein Ermittlungsverfahren zu unterrichten.

Über den Fall habe ich gesondert berichtet.

Veranlasst durch meine Beanstandung kündigte das SMJus an, die datenschutzrechtlichen Belange in der Berichtspraxis durch eine Neufassung der einschlägigen Regelung im Organisationsstatut der Staatsanwaltschaften und durch eine datenschutzrechtlich einwandfreie Verfahrensweise bei der Beantwortung von Anfragen und Petitionen künftig sicherzustellen. Bereits in meinem 8. Tätigkeitsbericht (Seite 85) hatte ich die notwendigen grundlegenden Änderungen des Berichtswesens der Staatsanwaltschaften angemahnt (8/8.3). So hat die Aufdeckung des Datenschutzverstoßes des Staatsministers eine durchaus positive Wirkung gezeitigt: Künftig wird es nicht mehr möglich sein - wie im vorliegenden Fall -, dass direkte Weisungen an nachgeordnete Beamte (unter Umgehung des Staatssekretärs) und die Anforderung von Berichten unter Verschweigung der wirklichen Motivation (politische Unterrichtung anstelle von Dienstaufsicht) erfolgen. Damit wird durch klare Verfahrensregeln ein zweckwidriger, von persönlicher, parteilicher oder taktischer Motivation getragener Umgang mit personenbezogenen Daten jedenfalls erheblich erschwert, wenn nicht verhindert.

Infolge der Schwere des datenschutzrechtlichen Verstoßes des Staatsministers habe ich die Beanstandung gegenüber dem SMJus auch in Form einer Pressemitteilung veröffentlicht. Wegen dieser Veröffentlichung ist ein strafrechtliches Ermittlungsverfahren gegen mich eingeleitet worden, das zur Anklage geführt hat, über die das Gericht noch nicht entschieden hat.

8.2 Überwachung des Schriftverkehrs, den Gefangene mit dem Sächsischen Datenschutzbeauftragten führen

Im Berichtszeitraum haben sich eine Reihe von Gefangenen aus Justizvollzugsanstalten des Freistaates bei mir über die Behandlung ihrer Post durch das Anstaltspersonal beschwert. Mehrere dieser Beschwerden waren begründet. Die Behandlung des Schriftwechsels der Gefangenen entsprach nicht den Vorschriften des

Strafvollzugsgesetzes, das das Briefgeheimnis nach Art. 10 GG mit bestimmten Einschränkungen hinsichtlich Ausmaß und Zweck einer Überwachung, auch für Untersuchungs-, Straf- oder andere Gefangene garantiert.
So hatte sich zum Beispiel ein Gefangener bei mir telefonisch darüber beschwert, dass ihm ein an mich adressierter und verschlossener Brief zweimal mit der Begründung wieder ausgehändigt worden sei, er habe ihn den JVA-Bediensteten zur Kontrolle *offen* zu übergeben.

Das Verhalten des JVA-Personals war rechtswidrig: Zwar schreibt § 29 Abs. 3 StVollzG vor, dass der Gefangenen-Schriftwechsel grundsätzlich (nur!) „aus Gründen der Behandlung oder der Sicherheit oder Ordnung der Anstalt“ überwacht, das heißt einer Text- und Inhaltskontrolle unterzogen, werden darf. Nicht überwacht werden darf dagegen der Schriftwechsel des Gefangenen mit seinem Verteidiger, an und von den Landtagen, dem Deutschen Bundestag, dem Europäischen Parlament, den Europäischen Gerichtshof für Menschenrechte, die Europäische Kommission für Menschenrechte, den Europäischen Ausschuss zur Verhütung von Folter und unmenschlicher oder erniedrigender Behandlung oder Strafe und die Datenschutzbeauftragten des Bundes und der Länder, § 29 Abs. 1, 2 StVollzG. Mithin dürfen Gefangene Schreiben an mich und von mir verschlossen abgeben und verschlossen erhalten. Letzteres stelle ich durch jeweils ein Begleitschreiben, dessen Text mit dem SMJus abgestimmt ist, sicher (vgl. 4/8.2.5).

Der Leiter der betroffenen JVA hat den Sachverhalt eingeräumt und den Vorfall zum Anlass genommen, alle Bediensteten über die Rechtslage zu belehren. Den betreffenden Brief hat er passieren lassen.

Eine Reihe von Beschwerden, zum Teil mit schwerwiegenden Vorwürfen über angeblich mangelnde Verschwiegenheit des Anstaltspersonals über den Inhalt der von ihnen dienstlich zur Kenntnis genommenen Schreiben der Gefangenen, sind derzeit noch nicht abschließend bearbeitet. Ich werde den gesamten Bereich künftig noch intensiver beobachten müssen.

8.3 Datenübermittlung von Strafvollzugsbehörden an Finanzbehörden

Das SMJus informierte mich darüber, dass das BMJ mit einer erneuten Änderung des § 180 Abs. 5 StVollzG plane, den Strafvollzugsbehörden zur ermöglichen, den Finanzbehörden über die Tatsache der Haft und den Entlassungszeitpunkt eines steuerpflichtigen Gefangenen hinaus weitere Auskünfte zu erteilen. Aus der Sicht der hinter dem Gesetzentwurf stehenden Bundesländer und des Bundes sei diese Gesetzänderung erforderlich, weil sich aufgrund einer 1998 erfolgten Änderung von § 180 Abs. 5 StVollzG „die Strafvollzugsbehörden einiger Länder offenbar gehindert“ sehen, derartige weitere Auskünfte zu erteilen.

Diese Sicht wurde durch das SMJus allerdings nicht geteilt. Es war vielmehr der Auffassung, dass die Übermittlung weiterer personenbezogener Daten bereits nach

geltendem Recht zulässig sei, da sie zur Abwehr erheblicher Nachteile für das Gemeinwohl erforderlich sei.

Dem habe ich Folgendes entgegengehalten: Angesichts der Tatsache, dass der Anteil der steuerpflichtigen Strafgefangenen an der steuerpflichtigen Gesamtbevölkerung des Freistaates Sachsen im Promillebereich liegt, ist die Annahme einer erheblichen Gefahr für das Gemeinwohl durch die Beschränkung der Datenübermittlung an Finanzbehörden auf die Tatsache der Haft und den Entlassungszeitpunkt eines steuerpflichtigen Gefangenen eher fernliegend. Vorbehaltlich der in Aussicht genommenen Änderung des § 180 Abs. 5 StVollzG wäre die Übermittlung weiterer personenbezogener Daten daher unzulässig.

Mit dieser Auffassung konnte ich das SMJus überzeugen. Es wies daher die sächsischen Justizvollzugsanstalten an, von der Erteilung weiterer als von § 180 Abs. 5 StVollzG vorgesehene Auskünfte abzusehen, solange eine entsprechende gesetzliche Ermächtigung nicht vorliegt.

8.4 Dürfen Daten aus der Bewährungshilfe an ein Kreiswehrersatzamt weitergegeben werden?

Ein Kreiswehrersatzamt bat einen Landgerichtspräsidenten, einen Bewährungshelfer anzuweisen, Auskünfte über das Bewährungsverhalten eines unter Bewährungsaufsicht stehenden Verurteilten zu erteilen. Die Angaben würden zur Entscheidung im Musterungs- und Einberufungsverfahren, insbesondere über einen möglichen Ausschluss oder eine Zurückstellung des Wehrpflichtigen, benötigt.

Das SMJus als Landesjustizverwaltung bat mich deshalb zu prüfen, ob die Auskunftserteilung in analoger Anwendung der Vorschriften des Soldatengesetzes (§ 62) und des Zivildienstgesetzes (§ 45) jeweils i. V. m. § 125 c des Beamtenrechtsrahmengesetzes (BRRG) zulässig wäre.

Bei meiner datenschutzrechtlichen Bewertung ließ ich mich von folgenden Erwägungen leiten: Angaben zum Bewährungsverhalten des Verurteilten greifen besonders tief in dessen Grundrecht auf informationelle Selbstbestimmung ein, so dass für die Verarbeitung dieser Angaben eine bereichsspezifische Übermittlungsregelung unabdingbar ist. Nach dem hierfür vom Bundesverfassungsgericht in seinem Volkszählungsurteil entwickelten Grundsätzen verbietet sich erst recht ein Rückgriff auf die Anwendung nicht-bereichsspezifischer Vorschriften im Wege etwa der „Rechtsanalogie“, (ein häufig unter schwachen Juristen beliebter Begriff).
Darüber hinaus sind weitere Gesichtspunkte zu beachten: Durch das Justizmitteilungsgesetz hat der Gesetzgeber den Vorgaben des Bundesverfassungsgerichts entsprochen und die bislang überwiegend in Verwaltungsvorschriften des Bundes und der Länder geregelten Mitteilungspflichten der Gerichte und Staatsanwaltschaften an andere öffentliche Stellen auf die erforderlichen gesetzlichen Grundlagen gestellt. Mit der Ergänzung von Soldatengesetz und Zivildienstgesetz durch Art. 17 und 18 JuMiG hat der Gesetzgeber ausdrücklich nur Mitteilungen geregelt, die Strafsachen

gegen bereits im Dienst befindliche Soldaten und Zivildienstleistende betreffen; für die erst zur Einberufung anstehenden Soldaten bzw. Zivildienstleistenden hat er hierauf bewusst verzichtet, so dass schon die für eine Analogie notwendige „planwidrige Regelungslücke“ nicht erkennbar ist.

Schließlich wäre die in Aussicht genommene Datenübermittlung auch wegen des gewünschten Datenumfangs unzulässig. So verpflichtet § 125 c Abs. 1 BRRG unter anderem das Gericht in Bezug auf Strafverfahren gegen Beamte bei Erhebung der öffentlichen Klage dem zuständigen Dienstherrn die in Nummern 1 - 3 aufgeführten Urkunden zu übermitteln und Hinweise über ein eventuell eingelegtes Rechtsmittel oder den Erlass und den Vollzug eines Haft- bzw. Unterbringungsbefehls zu geben, um dienstrechtliche Maßnahmen sicherzustellen; nach Abs. 3 kommen hierfür auch Entscheidungen über Verfahrenseinstellungen in Betracht. Die vom Kreiswehrersatzamt begehrte Auskunft über das Bewährungsverhalten eines Verurteilten wird von diesen Mitteilungspflichten ersichtlich *nicht* erfasst, so dass sich auch insoweit jegliche „Analogie“ verbietet. Die erbetenen Angaben besitzen - im Gegensatz zu den vorgenannten Mitteilungen - einen qualitativ anderen Informationsgehalt und sind auch keine „sonstigen Tatsachen, die in einem Strafverfahren bekannt werden“, so dass auch § 125 c Abs. 4 BRRG nicht anwendbar ist. Im Übrigen habe ich gravierende Bedenken, ob die Kenntnis der gewünschten Daten im vorliegenden Fall für wehrdienstliche Maßnahmen erforderlich gewesen wäre.

Aus diesen Gründen habe ich dem SMJus mitgeteilt, dass die vom Kreiswehrersatzamt gewünschte Auskunftserteilung unzulässig wäre.

8.5 Pfändung von Patientenunterlagen in einem Insolvenzverfahren

Ein niedergelassener Arzt, dem es bei der Erweiterung seiner Praxis finanziell übel ergangen war, und der deshalb ein Insolvenzverfahren beantragen musste, benachrichtigte mich telefonisch, dass der Gerichtsvollzieher im Begriff sei, unter anderem ca. 12.000 Patientenakten aus seinen Praxisräumen „abzuholen“. Er sei der Ansicht, dass er als Arzt diese Akten auf Grund seiner ärztlichen Schweigepflicht nach § 203 Abs. 1 StGB keinesfalls herausgeben dürfe.
Meine sofortige Nachfrage bei dem vom Amtsgericht als Insolvenzverwalter eingesetzten Rechtsanwalt ergab, dass dieser die Akten nicht gepfändet, sondern lediglich unter Verschluss genommen hatte. Er wolle sie mit Hilfe zweier ehemaliger Auszubildender des Arztes durchsehen, um offene Forderungen feststellen und geltend machen zu können.

Ich habe den Fall zum Anlass genommen, die Sächsische Landesärztekammer, das Staatsministerium des Innern (als oberste Aufsichtsbehörde für den Bereich der privaten Datenverarbeitung) und - beratend - das zuständige Amtsgericht auf folgendes aufmerksam zu machen:

Wenn es der Gläubigergemeinschaft, die sich ja des Insolvenzverwalters bedient, darauf ankommt, in den Patientenakten noch offenstehende Forderungen zu entdecken und geltend zu machen, so hat sie den Arzt zu verpflichten, ein Verzeichnis seines Vermögens - wozu auch offene Forderungen an Patienten und Krankenkassen gehören - vorzulegen und an Eides statt dessen Richtigkeit zu versichern, §§ 97 InsO (Auskunfts- und Mitwirkungspflichten des Schuldners), 807 ZPO (Eidesstattliche Versicherung). Ein Durchsuchen der Patientenunterlagen durch ehemalige Auszubildende, die dadurch auch erstmals von Patientendaten Kenntnis erhalten, ist mit dem von der Rechtsordnung garantierten besonderen Schutz dieser Daten nicht zu vereinbaren.

Insbesondere hatte der Arzt durch die Eröffnung des Insolvenzverfahrens nicht seine Verwaltungs- und Verfügungsrechte über die Patientenakten an den Insolvenzverwalter verloren. Denn Patientenunterlagen sind als „zur Ausübung des Berufs erforderliche (!) Gegenstände“ nicht pfändbar, § 811 Abs. 1 Nr. 7 ZPO, und zählen deshalb auch nicht zur Insolvenzmasse, §§ 80, 36 InsO. Der Schuldner darf sie auch nach eröffnetem Insolvenzverfahren weiter verwalten und über sie verfügen. Die darin enthaltenen Daten sind dem Arzt vom Patienten grundsätzlich persönlich anvertraut worden. Nur im Falle der persönlichen Verhinderung des Arztes (z. B. schwere Erkrankung oder Tod) dürften sie von einem anderen Arzt als Abwickler soweit verwendet werden, dass die Datenträger nach Wunsch oder auf Weisung des Patienten an einen anderen Arzt seines Vertrauens übergeben werden. Gegenüber einem Insolvenzverwalter und dessen Helfern darf die entstandene ärztliche Schweigepflicht nicht durchbrochen werden. Anders lautende Ansichten, wonach Patientenunterlagen zwar zur Insolvenzmasse gehören, aber nur mit Zustimmung des Schuldners verwertet werden dürfen, werden dem hohen Schutzgut nicht gerecht und verkomplizieren die Sache unnötig.

Mit anderen Worten: Das Berufsgeheimnis geht vor Insolvenzrecht; der insolvente Arzt muss selbst die notwendigen Verzeichnisse erstellen. Das liegt auch finanziell in seinem Interesse.

9 Wirtschaft und Arbeit

9.1 Straßenverkehrswesen

9.1.1 Automatisierter Abruf von Kfz-Halterdaten aus dem örtlichen Fahrzeugregister durch gemeindliche Vollzugsbedienstete, örtliche Bußgeldstellen und Sozialämter

Ich hatte mich mit der Frage zu befassen, ob dem gemeindlichen Vollzugsdienst (Überwachung des ruhenden Verkehrs), den örtlichen Bußgeldstellen und den Sozialämtern der automatisierte Abruf aus dem örtlichen Fahrzeugregister gestattet werden darf.

1. Online-Zugriff des gemeindlichen Vollzugsdienstes und der örtlichen Bußgeldstelle:

Nach § 36 Abs. 2 Satz 2 StVG dürfen den örtlich zuständigen Polizeidienststellen der Länder und Verwaltungsbehörden im Sinne des § 26 Abs. 1 aus den jeweiligen örtlichen Fahrzeugregistern durch Abruf im automatisierten Verfahren Kfz-Halterdaten übermittelt werden, und zwar gemäß § 36 Abs. 5 StVG nach Maßgabe einer Rechtsverordnung (hier der Fahrzeugregisterverordnung).

§ 12 Abs. 2 letzter Satz Fahrzeugregisterverordnung besagt, dass die entsprechenden Daten für die zuständigen Dienststellen des *Polizeivollzugsdienstes* zum Abruf bereitzuhalten sind. Dienststellen des *Polizeivollzugsdienstes* in Sachsen sind in § 71 Abs. 1 SächsPolG aufgezählt. Hierzu zählen demnach nicht die gemeindlichen Vollzugsbediensteten (§ 80 SächsPolG), die zwar Polizeiaufgaben nach § 1 GemPolVO zu erfüllen haben, jedoch nicht dem *Polizeivollzugsdienst* zuzurechnen sind.

Dies hat zur (wenig befriedigenden) Folge, dass dem gemeindlichen Vollzugsdienst kein Online-Zugriff auf das örtliche Fahrzeugregister eingerichtet werden darf, obwohl dort eindeutig Bedarf besteht. Gleiches gilt auch für die örtlichen Bußgeldstellen.

Da mir Städte bekannt sind, die ihrem gemeindlichen Vollzugsdienst bzw. der Bußgeldstelle einen Online-Zugriff auf das örtliche Fahrzeugregister gestattet haben und ich diese Städte in Anbetracht der Bedarfssituation nur ungern beanstanden würde, habe ich das SMI und das SMWA, die meine rechtliche Einschätzung teilen, um Initiative zur Ergänzung des § 12 Abs. 2 letzter Satz Fahrzeugregisterverordnung zugunsten der gemeindlichen Vollzugsdienste und der örtlichen Bußgeldstellen gebeten.

Die Angelegenheit ist noch im Fluss.

2. Online-Zugriff des Sozialamtes auf das örtliche Fahrzeugregister

§ 117 Abs. 3 BSHG lässt eine Überprüfung der Eigenschaft als Kraftfahrzeughalter im Wege des *automatisierten Datenabgleichs* mit dem örtlichen Fahrzeugregister zu.

Ich halte § 117 Abs. 3 Satz 3 BSHG unter der Voraussetzung, dass zunächst § 35 Abs. 1 StVG an diese BSHG-Bestimmung angepasst wird (siehe 8/10.2.3), für eine Rechtsgrundlage, die es erlaubt, zwei Datenbestände, nämlich des Sozialamtes und der Kfz-Zulassungsstelle miteinander abzugleichen und die „Treffer“ für das Sozialamt aufzulisten.

Ein Landkreis interpretierte § 117 Abs. 3 Satz 3 BSHG jedoch so, dass auch eine Online-Anbindung des Sozialamtes an das örtliche Fahrzeugregister zum Zwecke des einzelfallbezogenen *automatisierten Abrufs* zulässig sei.

Dieser Auffassung ist entgegenzuhalten, dass § 36 Abs. 2 Satz 2 StVG abschließend die Behörden nennt, die im automatisierten Abrufverfahren nach Maßgabe der Fahrzeugregisterverordnung (§ 36 Abs. 5 StVG) auf das örtliche Fahrzeugregister zugreifen dürfen. Die Sozialämter sind nicht genannt, so dass für deren Online-Anbindung ersichtlich keine Rechtsgrundlage existiert.

Ich habe das SMWA und das SMS für eine Unterrichtung der Sozialbehörden und der Kfz-Zulassungsstellen gebeten, sofern aus dortiger Sicht keine triftigen Gründen gegen meine Rechtsauffassung sprechen.

9.1.2 Laptopeinsatz im Fahrerlaubnisverfahren

Die Dekra Dresden stellte mir ein Konzept vor, wonach alle Fahrprüfer mit einem Laptop ausgerüstet werden sollen, auf dem die Daten sämtlicher Fahrerlaubnisbewerber (ca. 8.000 Datensätze) gespeichert sind.

Die Datei soll es jedem einzelnen Prüfer - unabhängig vom Prüfungsort und vom Prüfungstag - ermöglichen, auf die Daten des jeweiligen Prüflings zugreifen zu können, dessen Identität dem Prüfer erst unmittelbar vor der Prüfung bekannt wird. Dass mit einem solchen Verfahren den Prüfern weitaus mehr Daten anvertraut werden, als für deren Aufgabenerfüllung erforderlich, wurde dabei wohl nicht bedacht.

Aus datenschutzrechtlicher Sicht konnte ich das Verfahren nicht befürworten, weil
- *sich jeder Prüfer sämtliche Bewerberdaten auf seinen Laptop lädt, obwohl er nur einen Bruchteil für seine Aufgabenerfüllung benötigt,*
- *die Datensicherheit nicht gewährleistet ist (Laptops werden mit nach Hause genommen; Diebstahlgefahr, wenn Laptops unbeaufsichtigt im Auto der Prüfer liegen usw.).*

Dass Fahrerlaubnisbewerberdaten für Kfz-Händler, Versicherungen und nicht zuletzt für den Schwarzmarkt (Verkauf von gefälschten Führerscheinen) von großem Interesse sind, war den Dekra-Leuten fremd.

Die Dekra Dresden prüft nun, ob eine Laptopversion mit Funkanschluss an den zentralen Dekra-Server unter Berücksichtigung entsprechender Verschlüsselungsverfahren verwirklicht werden kann. Ein solches Verfahren hätte den Vorteil, dass jeder Prüfer nur die Bewerberdaten abrufen könnte, für deren Fahrprüfung er zustän-

dig ist. Nach Rückübertragung der Bewerberdaten einschließlich Prüfungsergebnis (bestanden/nicht bestanden) an den Dekra-Server, könnten die Daten auf den Laptops dann gelöscht werden.
Ich habe um weitere Beteiligung gebeten.

9.1.3 Übertragung von Aufgaben der Fahrerlaubnisbehörde auf die Gemeinden - hier: Aushändigung von umgetauschten Führerscheinen

Ein Landratsamt (Fahrerlaubnisbehörde nach § 73 FeV) fragte, ob die Aushändigung umgetauschter Führerscheine nicht im Wege einer Zweckvereinbarung gemäß § 71 SächsKomZG auf die Gemeinden übertragen werden könne.

Meine Stellungnahme: Gemeinden und Landkreise können Aufgaben, zu deren Erfüllung sie berechtigt oder verpflichtet sind, nach den Vorschriften des SächsKomZG *gemeinsam* wahrnehmen, soweit gesetzlich nichts anderes bestimmt ist (§ 1 SächsKomZG). So, wie ich diese Bestimmung verstehe, folgt daraus, dass nur eine allen beteiligten Stellen gleichermaßen obliegende Aufgabe auf eine (leistungsfähige) Körperschaft zur gemeinsamen Wahrnehmung z. B. im Wege der Zweckvereinbarung nach §§ 71, 72 SächsKomZG übertragen werden kann (z. B. Müllabfuhr, Abwasserbeseitigung). Da den Gemeinden keine Aufgaben der Fahrerlaubnisbehörde obliegen, wäre eine diesbezügliche Zweckvereinbarung rechtswidrig.

Auch im Wege der Amtshilfe (vgl. §§ 4 ff. VwVfG) kann die Aushändigung der Fahrerlaubnisse nicht auf die Gemeinden übertragen werden, weil die damit einhergehende Datenübermittlung nach der verbindlichen Rechtsprechung des Bundesverfassungsgerichts „amtshilfefest“ sein muss (BVerfGE 65,46), d. h. dass Datenübermittlungen nur unter den Voraussetzungen der Datenübermittlungsbestimmungen in Spezialvorschriften oder, wenn solche fehlen, im Datenschutzgesetz zulässig sind. Eventuell anderslautende Äußerungen „maßgeblicher“ Stellen sind deshalb unrichtig.

§ 52 Abs. 1 StVG, der gemäß § 2 Abs. 4 SächsDSG dem Sächsischen Datenschutzgesetz als Spezialgesetz vorgeht, lässt Datenübermittlungen *nur an zuständige Stellen zu, soweit dies zur Erfüllung der diesen Stellen obliegenden Aufgaben zu den in § 49 StVG genannten Zwecken jeweils erforderlich ist*. Auf die Gemeinden treffen diese Voraussetzungen mit der Folge nicht zu, dass Datenübermittlungen zum Zwecke der Aushändigung der umgetauschten Führerscheine nicht zulässig sind.

Schließlich dürfte die geplante Aufgabenübertragung auch aus Gründen der Verwaltungsökonomie unverhältnismäßig sein, zumal nach der VorlVwV-Fahrerlaubniswesen der Versand der umgetauschten Führerscheine *per Post* möglich ist. Einer Zwischenschaltung der Gemeinden bedarf es deshalb nicht.

9.1.4 „Kfz 2000“ - Das Zulassungsverfahren, angeboten von der Firma TÜV Online GmbH

Die Firma TÜV Online GmbH präsentierte mir ihr „Kfz 2000“-Verfahren, das folgende Möglichkeiten über das Internet bzw. Intranet bietet:

1. Wunschkennzeichenreservierung
2. Das komplette vorgelagerte Zulassungsverfahren (nur für den gewerblichen Kunden).

Anlässlich der Präsentation entstand der Eindruck, dass sämtliche Transaktionen *unverschlüsselt* über den Server von TÜV Online laufen, wo auch eine Speicherung von Grunddaten (Kfz-Kennzeichen, Zulassung erfolgt am, Zulassung nicht erfolgt) für statistische Zwecke erfolgt. Da das Kfz-Kennzeichen ein personenbeziehbares Datum i. S. v. § 3 Abs. 1 SächsDSG darstellt, könnte ein - wenn auch verkürztes - zentrales Kfz-Register entstehen, für dessen Zulässigkeit ich keine Rechtsgrundlage sehe.

Von meinem saarländischen Kollegen, der sich bereits mit dem Produkt befasst hat, erhielt ich ein 63seitiges IT-Sicherheitskonzept, aus dem u. a. zu ersehen ist, dass im Saarland die Datentransfers tatsächlich *verschlüsselt* erfolgen.

Der Firma TÜV Online GmbH habe ich mitgeteilt, dass ich geneigt bin, das „Kfz 2000"-Verfahren dann zu akzeptieren, wenn das saarländische IT-Sicherheitskonzept sinngemäß von den sächsischen Zulassungsstellen umgesetzt wird.

Eine Reaktion steht bislang aus.

9.2 Gewerberecht

Aufbewahrungsfristen von Gewerbeanzeigen nach § 14 GewO

Nach § 14 Abs. 1 Satz 3 GewO dient die Gewerbeanzeige dem Zweck, der zuständigen Behörde die Überwachung der Gewerbe*ausübung* zu ermöglichen. Die erhobenen Daten dürfen von den zuständigen Behörden *nur für diesen Zweck* verarbeitet und genutzt werden (§ 14 Abs. 1 Satz 4 GewO).

Da die Gewerbe*ausübung* mit der Gewerbeabmeldung endet, endet auch deren Überwachung mit der Folge, dass die Gewerbetreibendendaten (unverzüglich) zu löschen wären. Daran ändert auch § 14 Abs. 11 GewO nichts, wonach u. a. für das Löschen das Sächsische Datenschutzgesetz gilt. Nach § 19 Abs. 1 Nr. 2 SächsDSG sind nämlich personenbezogene Daten zu löschen, wenn ihre Kenntnis für die speichernde Stelle zur Erfüllung ihrer Aufgaben (hier die Überwachung der Gewerbe*ausübung*) nicht mehr erforderlich ist. Nach meiner Kenntnis sind die Löschungsbestimmungen in den Datenschutzgesetzen der anderen Bundesländer insoweit identisch, so dass das Rechtsproblem nicht nur in Sachsen besteht.

Das von mir eingeschaltete SMWA hat Argumente vorgetragen, die für sich gesehen zwar ein weiteres Vorhalten der Gewerbetreibendendaten rechtfertigen würden; jedoch lässt § 14 Abs. 1 Satz 4 GewO eine Verarbeitung oder Nutzung für andere Zwecke als zur Überwachung der Gewerbe*ausübung* nicht zu.

In der Gesamtschau ist festzuhalten, dass sämtliche Aufbewahrungsfristen - auch die in den anderen Bundesländern - mit dem eindeutigen Wortlaut des § 14 Abs. 1 Sätze 3 und 4 GewO nicht zu vereinbaren sind. Dies gilt insbesondere für die gegenwärtige Aufbewahrungspraxis in Sachsen, die nach Nr. 120.11 des Aktenplanes für die Kommunen des Freistaates Sachsen *zwanzig* Jahre beträgt, aber auch für die vom SMWA vorgeschlagenen *fünf* Jahre.

Die zugegebenermaßen unbefriedigende Situation wäre m. E. nur durch Ergänzung des § 14 Abs. 1 GewO zu bereinigen, indem weitere Zwecke (als die Überwachung der Gewerbe*ausübung*) genannt werden. Eine Gesetzesinitiative im Bundesrat habe ich deshalb angeregt.

9.3 Industrie- und Handelskammern; Handwerkskammern

Maßnahmenkatalog des SMI gegen Rechtsextremismus - Unterrichtung der Kammern über rechtsextremistische Aktivitäten

Das SMI hatte erwogen, die Präsidenten der Industrie- und Handelskammern sowie der Handwerkskammern über bekanntgewordene rechtsextremistische Aktivitäten Gewerbetreibender (z. B. Gastwirte) zu unterrichten. Ein möglicher Rechtfertigungsgrund für solche Datenübermittlungen wurde in § 1 IHKG gesehen, wonach es u. a. zu den Kammeraufgaben gehört, das Gesamtinteresse der ihnen zugehörigen Gewerbetreibenden ihres Bezirkes wahrzunehmen sowie „für Wahrung von Anstand und Sitte des ehrbaren Kaufmannes zu wirken“.

Auch der Beschluss des VG Arnsberg vom 23. Dezember 1998 - 1 L 2031/98, wonach eine Gewerbeausübung, die mit der Verharmlosung oder der Verherrlichung des Nationalsozialismus und mit der Verbreitung neonazistischen Gedankenguts verbunden ist, zur gewerberechtlichen Unzuverlässigkeit führt, wurde in die Überlegungen des SMI einbezogen, als man mich um datenschutzrechtliche Bewertung der Zulässigkeit solcher Datenübermittlungen bat.

Für eine Unterrichtung der Präsidenten der Industrie- und Handelskammern sowie der Handwerkskammern vermochte ich eine Rechtsgrundlage nicht zu erkennen. Weder das IHKG noch die Handwerksordnung sehen eine Unterrichtungspflicht anderer Behörden (wie beispielsweise § 76 Abs. 2 AuslG oder § 10 SächsVSG) vor.

Auch der Beschluss des VG Arnsberg ist wenig hilfreich, zumal er sich mit einem Gewerbeuntersagungsverfahren nach § 35 GewO befasst. Da weder die Industrie- und Handelskammern noch die Handwerkskammern Gewerbeuntersagungsbehörden sind, schienen sie mir nicht die richtigen Adressaten für die Datenübermittlungsabsichten des SMI zu sein.

Auch § 13 Abs. 1 SächsDSG kam nach meinem Dafürhalten als Übermittlungsbefugnis nicht in Betracht, weil die dort genannten Voraussetzungen ersichtlich nicht erfüllt sind.

In der Gesamtschau hielt ich Datenübermittlungen der beabsichtigten Art an die Kammerpräsidenten für unzulässig. Allerdings würde ich im Hinblick auf o. a. Beschluss des VG Arnsberg eine Datenübermittlung an die *Gewerbeuntersagungsbehörde* gemäß § 12 Abs. 1 SächsVSG (Übermittlung personenbezogener Daten durch das Landesamt für Verfassungsschutz an andere Behörden für Zwecke der öffentlichen Sicherheit) akzeptieren.

Das SMI hat signalisiert, von der Absicht, die Kammerpräsidenten über rechtsextremistische Umtriebe zu unterrichten, Abstand zu nehmen.

9.4 Offene Vermögensfragen

In diesem Jahr nicht belegt.

9.5 Sonstiges

9.5.1 Entwurf zum Neuerlass des Sächsischen Architektengesetzes (SächsArchG)

Das SMI beteiligte mich am Entwurf einer Neufassung des Sächsischen Architektengesetzes, weil verschiedene Bestimmungen den Umgang mit personenbezogenen Daten regeln, bzw. das Recht auf informationelle Selbstbestimmung tangieren.

Datenschutzrechtlich relevant ist beispielsweise § 4 Abs. 4 Satz 1, wonach jeder das Recht haben soll, Auskunft aus der Architekten-, Stadtplaner- und Sachverständigenliste und dem Verzeichnis der auswärtigen Architekten und Stadtplaner zu verlangen.

Da nicht ersichtlich ist, ob Auskunft aus den Listen oder Verzeichnissen nur einzelfallbezogen erfolgt, oder ob der Auskunftbegehrende auch Auskunft über sämtliche Eingetragenen erhält, habe ich im Hinblick darauf, dass der Auskunftbegehrende noch nicht einmal ein berechtigtes Interesse an der Auskunft glaubhaft zu machen braucht, angeregt, im Gesetz Auskünfte auf konkrete Einzelfälle zu beschränken, um umfangreiche Datensammlungen bei Dritten zu verhindern.

Nach § 4 Abs. 4 Satz 2 dürfen Familiennamen, Vornamen, akademische Grade, Anschrift der Hauptniederlassung (nicht der Wohnung), Fachrichtungen, Art und Weise der Berufsausübung und die Sachgebietsbezeichnung veröffentlicht oder an Dritte zum Zwecke der Veröffentlichung weitergegeben werden, sofern der Betroffene nicht widerspricht.

Mit der Widerspruchsregelung wird dem Recht auf informationelle Selbstbestimmung der Betroffenen in angemessener Weise Rechnung getragen. Allerdings habe ich noch folgende Ergänzung vorgeschlagen:

„Auf dieses Widerspruchsrecht ist der Betroffene bei seiner Antragstellung nach § 5 deutlich hinzuweisen."

Besondere Kritik übte ich aber an § 6, dessen Wortlaut ich hier wiedergebe:

§ 6
Versagung der Eintragung

(1) Die Eintragung in die Architekten- oder Stadtplanerliste oder in das Gesellschaftsverzeichnis ist einem Antragsteller trotz des Vorliegens der Eintragungsvoraussetzungen zu versagen, wenn Tatsachen die Annahme rechtfertigen, dass er nicht die für den Beruf des Architekten oder Stadtplaners erforderliche Zuverlässigkeit besitzt. Die erforderliche Zuverlässigkeit fehlt ihm insbesondere,

1. *solange ihm nach § 70 des Strafgesetzbuches oder nach § 132 a der Strafprozessordnung die Ausübung einer der in § 1 bezeichneten Tätigkeiten verboten oder vorläufig verboten ist;*
2. *wenn er wegen eines Verbrechens oder Vergehens rechtskräftig zu einer Strafe verurteilt ist und sich aus dem der Verurteilung zugrunde liegenden Sachverhalt ergibt, dass er zur Erfüllung der Berufsaufgaben nach § 1 nicht geeignet ist;*
3. *solange er wegen einer psychischen Krankheit oder einer geistigen oder seelischen Behinderung einzelne Angelegenheiten, die die Berufsausübung betreffen, ganz oder teilweise nicht besorgen kann oder*
4. *wenn im berufsgerichtlichen Verfahren rechtskräftig auf Löschung seiner Eintragung erkannt und die vom Berufsgericht bestimmte Frist (§ 22 Abs. 3 Satz 2, § 23 Abs. 2 Satz 1) nicht abgelaufen ist.*

(2) Die Eintragung kann einem Antragsteller versagt werden, wenn er innerhalb der letzten drei Jahre vor Stellung des Eintragungsantrags eine eidesstattliche Versicherung nach § 807 der Zivilprozessordnung abgegeben hat, ein Konkurs-, Gesamtvollstreckungs- oder Insolvenzverfahren über sein Vermögen eröffnet oder die Eröffnung mangels Masse abgelehnt worden ist.

Aus dieser Bestimmung ist nicht ersichtlich, woher die Informationen über die Unzuverlässigkeit der Antragsteller stammen und aufgrund welcher Rechtsgrundlage die Datenerhebung bzw. -übermittlung erfolgt. Entsprechende Befugnisse zur Datenerhebung und Verpflichtungen zur Datenübermittlung oder Verpflichtung der Betroffenen, entsprechende Nachweise zu erbringen (z. B. bei seiner Antragstellung auf Eintragung), vermag ich nicht zu erkennen.

Hier besteht noch Nachbesserungsbedarf ebenso wie bei § 7, wo die Löschung der Eintragung ebenfalls von Datenerhebungen oder -übermittlungen, für die es ersichtlich keine Rechtsgrundlagen gibt, abhängig ist.

Ich habe das SMI um weitere Beteiligung gebeten.

9.5.2 Veröffentlichung der Daten eines säumigen Beitragsschuldners durch die Ingenieurkammer

Im Deutschen Ingenieurblatt-Sachsen fand ich eine Bekanntmachung, in der unter Angabe des akademischen Grades, des Namens, der letzten Wohnadresse und des

Mitgliedschaftsverhältnisses mitgeteilt wurde, dass der Betroffene unbekannt verzogen sei und der Kammervorstand beabsichtige, die Mitgliedschaft u. a. wegen seit 1999 offener Beitragszahlungen zu löschen.

Da ein solcher „Pranger", für den es ersichtlich keine Rechtsgrundlage gibt, geeignet ist, massiv die schutzwürdigen Interessen des Betroffenen zu beeinträchtigen, habe ich die Ingenieurkammer im Beanstandungsverfahren nach § 26 SächsDSG aufgefordert, künftig solche „Bekanntmachungen" zu unterlassen. Dies wurde mir zugesichert.

9.5.3 Offenbarung personenbezogener Sachverhalte in Vorträgen

Eine Eingabe hat mich auf folgenden Sachverhalt aufmerksam gemacht:

Ein Vortrag der Leitstelle der Gleichstellung von Frau und Mann enthielt Interna (z. B. Besoldungsdaten), die geeignet waren, die schutzwürdigen Interessen der Geschäftsführerin eines Frauenverbandes massiv zu beeinträchtigen.

Datenschutzrechtlich stellten diese auf die Person der Geschäftsführerin bezogenen Äußerungen vor den Delegierten und vor anderen Personen eine Datenübermittlung an Private dar, die an § 15 Abs. 1 bis 3 SächsDSG zu messen gewesen wäre. Ich vermochte nicht zu erkennen, dass die in § 15 Abs. 1 SächsDSG genannten Voraussetzungen erfüllt waren und muss die Vorgehensweise wohl beanstanden. Allerdings steht die Stellungnahme der Leitstelle noch aus.

9.5.4 Korruptionsvorbeugung in der staatlichen Verwaltung

Über die Bemühungen der Sächsischen Staatsregierung, der Korruption in der staatlichen Verwaltung vorzubeugen, habe ich im 8. Tätigkeitsbericht ausführlich berichtet (8/9.5.1).

Nach nunmehr mehrjähriger Vorarbeit hat das federführende SMI den Entwurf einer „Verwaltungsvorschrift zur Korruptionsvorbeugung in der staatlichen Verwaltung des Freistaates Sachsen (VwV Korruptionsvorbeugung)" fertiggestellt und zur Mitzeichnung an die beteiligten Ressorts gegeben.

An der Erstellung des Entwurfs, der u. a.

- korruptionsgefährdete Bereiche der staatlichen Verwaltung beschreibt,
- die Einrichtung behördlicher „Ansprechpartner für Korruption" vorschreibt,
- das Verhalten beim Auftreten eines Korruptionsverdachts regelt sowie
- die besondere Bedeutung der strikten Einhaltung der vergaberechtlichen Vorschriften der Verdingungsordnungen für Bauleistungen (VOB), für Leistungen (VOL) und für freiberufliche Leistungen (VOF) betont,

wurde ich zwar laufend beteiligt. Bis zuletzt musste ich dabei allerdings u. a. gegen die bei einigen teilnehmenden Ressorts vorhandene Vorstellung ankämpfen, dass personenbezogene Daten allein auf der Grundlage der Verwaltungsvorschrift verar-

beitet werden dürfen (ohne dass eine verfassungsrechtlich zwingend notwendige gesetzliche Grundlage vorläge). So enthielt der Entwurf zunächst genaue und ausführliche Bestimmungen über die Prüfung der Zuverlässigkeit eines Bieters in einem Vergabeverfahren nach den vorgenannten Vergabevorschriften. Danach sollten die Behörden des Freistaates Sachsen in jedem Fall prüfen, „ob bei dem Bieter oder Bewerber schwere Verfehlungen vorliegen, die seine Zuverlässigkeit in Frage stellen und gemäß § 8 Nr. 5 Abs. 1 VOB/A den Wettbewerbsausschluss rechtfertigen". „Schwere Verfehlungen" des Bieters sollten dann als nachgewiesen gelten, wenn „sie zu einer gerichtlichen Verurteilung geführt haben, unbestritten sind oder ein Geständnis in einem Ermittlungsverfahren vorliegt.

Anhand welcher verlässlicher Kriterien und woher die zur Beurteilung „schwerer Verfehlungen" erforderlichen Daten stammen sollten (Betroffener, Staatsanwaltschaften, Gerichte, Bundeszentralregister, Gewerbezentralregister, andere Quellen?) und welche gesetzlichen Grundlagen hierfür evtl. vorhanden sind, war jedoch im Entwurfstext ungeregelt geblieben. Es war somit übersehen worden, dass jede Datenverarbeitung ausnahmslos einer (verfassungsgemäßen) gesetzlichen Grundlage bedarf; der Entwurf konnte daher so nicht bestehen bleiben. Hinzu kam, dass vergaberechtliche Vorschriften in einer Verwaltungsvorschrift über die Korruptionsvorbeugung auch rechtssystematisch fehl am Platze gewesen wären.

In der abschließenden Ressortbesprechung konnte ich erreichen, dass die Teile des Entwurfs, in denen eine Datenerhebung zum Zwecke der Prüfung der Zuverlässigkeit des Bieters ohne gesetzliche Ermächtigung stattgefunden hätte, gestrichen wurden. So wird in der Endfassung des Entwurfs lediglich auf den hohen Stellenwert hingewiesen, der der Zuverlässigkeit des Bieters, die sich nach den bereits existierenden Regeln des Vergaberechts bemisst, zukommt. Damit ist alles, aber mangels konkreter Daten eigentlich nichts gesagt - auch ein Ergebnis.

9.5.5 Vom Sparwillen des Bundesverteidigungsministeriums, Datenerhebung über Zahlungen an Reservisten unzulässig

Nach dem Unterhaltssicherungsgesetz erhalten Reservisten, die zu einer Wehrübung eingezogen werden und eine selbständige Tätigkeit ausüben, für diese Zeit eine Wirtschaftsbeihilfe. Diese wird in Sachsen von den Landratsämtern (USG-Behörden) gewährt.

Nun war im Bundesministerium der Verteidigung die Idee entstanden, die USG-Behörden könnten den Truppenteilen doch die an Selbständige geleisteten Zahlungen mitteilen. So sei künftig eine Prüfung möglich, ob ein „teurer" Selbständiger tatsächlich noch für den Verteidigungsfall üben müsse. Zum Glück hatte man nicht nur nach-, sondern auch an den Datenschutz gedacht und erkundete die Rechtslage in den Ländern.

Ich musste bedauern; denn es gibt keine spezialgesetzliche Vorschrift, die es den USG-Behörden erlaubt, den Truppenteilen die Höhe gewährter Leistungen an Selbständige zu übermitteln. Fehlen spezialgesetzliche Datenübermittlungsvorschriften,

darf eine öffentliche Stelle einer anderen personenbezogene Daten nur unter den Voraussetzungen des § 13 Abs. 1 SächsDSG mitteilen. Zu diesen Voraussetzungen gehört, dass die Datenübermittlung zur Aufgabenerfüllung des Empfängers oder der übermittelnden Stelle erforderlich *und* die in diesem Fall beabsichtigte Zweckänderung der Daten von den Erlaubnistatbeständen der §§ 12 Abs. 1 bis 4, 11 Abs. 4 SächsDSG erfasst ist.

Die Datenübermittlung scheitert schon an der Erforderlichkeit zur Aufgabenerfüllung. Zwar hat jede öffentliche Stelle im Zuge ihrer Aufgabenerfüllung auch wirtschaftliche Gesichtspunkte zu beachten, eine solche allgemeine Anforderung an die Verwaltung ist jedoch nach meiner Auffassung kein Kriterium, mit der sich die Erforderlichkeit einer Übermittlung von personenbezogenen Daten überzeugend begründen ließe. Selbst wenn man die Kenntnis dieser Daten als notwendiges Auswahlkriterium für die zu Wehrübungen heranzuziehenden Personen ansieht, wäre die Datenübermittlung unzulässig, weil die in §§ 12 Abs. 1 bis 4, 11 Abs. 4 SächsDSG genannten Voraussetzungen für eine Zweckänderung nicht erfüllt sind.

10 Soziales und Gesundheit

10.1 Gesundheitswesen

10.1.1 Regelungsbedarf im Sächsischen Krankenhausgesetz

Das SMS beabsichtigt eine Novellierung des Sächsischen Krankenhausgesetzes und bat um Mitteilung des Regelungsbedarfs. Aus meiner Sicht besteht dieser in Folgenden:

1. *Wartung, Fernwartung*
   Es sollte geregelt werden, unter welchen Voraussetzungen Personen oder Stellen außerhalb des Krankenhauses (Fremdfirmen) die Wartung und Fernwartung von Datenverarbeitungsanlagen mit Patientendaten durchführen dürfen; denn § 33 Abs. 10 SächsKHG (Datenverarbeitung im Auftrag) ist hier nicht einschlägig.

2. *Aufbewahrungsfristen*
   § 33 Abs. 6 SächsKHG regelt die Löschung von Patientendaten. Zu den Löschungsvoraussetzungen gehört u. a., dass vorgeschriebene Aufbewahrungsfristen abgelaufen sind. Für die Aufbewahrung von Patientenunterlagen, die im Zuge einer Krankenhausbehandlung entstehen, sind im Sächsischen Krankenhausgesetz bisher keine Fristen *vorgeschrieben*. Eine spezialgesetzliche Regelung erscheint angebracht, weil diese Problematik immer wieder Gegenstand von Anfragen aus dem Krankenhausbereich sind.

3. *Archivrechtliche Anbietepflicht*
   § 33 Abs. 6 SächsKHG lässt offen, ob Patientenunterlagen vor der Löschung einem Archiv anzubieten sind. Die nicht erwähnte Anbietepflicht könnte den -

falschen - Schluss zulassen, dass das Sächsische Archivgesetz auf Patientenunterlagen keine Anwendung findet, weil das Sächsische Krankenhausgesetz als spezielleres Gesetz dem Sächsischen Archivgesetz vorgeht. Insoweit scheint mir eine Klarstellung angebracht.

4. *Auftragsdatenverarbeitung*
   § 33 Abs. 10 SächsKHG erlaubt unter bestimmten Voraussetzungen, dass sich ein Krankenhaus zur Verarbeitung von Patientendaten anderer Personen oder Stellen bedienen darf. Außerhalb eines Krankenhauses unterliegen Patientendaten nicht mehr dem Beschlagnahmeschutz (§ 97 Abs. 2 Satz 2 StPO); hinzu kommt, dass Nichtärzten kein Zeugnisverweigerungsrecht zusteht. Vor diesem Hintergrund und mit Blick auf Art. 8 Abs. 3 EG-Datenschutzrichtlinie, wonach die Verarbeitung von Patientendaten ärztlichem Personal oder Personen vorbehalten ist, die einer entsprechendem Geheimhaltungspflicht unterliegen, ist eine grundlegende Überarbeitung der Vorschrift notwendig (Einzelheiten siehe Nr. 10.1.3).

5. *Zweckbindung und Forschungsvorhaben*
   Gemäß § 33 Abs. 4 SächsKHG dürfen Stellen oder Personen, denen Patientendaten befugt übermittelt wurden, diese nur zu dem die Befugnis begründenden Zweck verwenden. Diese Regelung schließt bei einem Datenempfänger, der nicht unter das Sächsische Krankenhausgesetz fällt, eine Nutzung für Forschungszwecke aus. Insbesondere an Daten aus der Qualitätssicherung, wie sie z. B. bei den Ärztekammern vorhanden sind, besteht wissenschaftliches Interesse. Ich halte es für überlegenswert, Forschungsvorhaben mit Patientendaten, die einem Datenempfänger außerhalb des Krankenhauses übermittelt wurden, unter den gleichen Voraussetzungen wie § 34 SächsKHG zuzulassen und damit von der strikten Zweckbindung auszunehmen.

6. *Definition „Qualitätssicherung“*
   Der Begriff „Qualitätssicherung“ oder die Terminologie „qualitätssichernde Maßnahmen in der Krankenversorgung“ sollte definiert werden. Immer wieder ergeben sich Abgrenzungsschwierigkeiten zwischen Datenübermittlungen nach § 33 Abs. 3 Nr. 4 SächsKHG (zur Durchführung qualitätssichernder Maßnahmen in der Krankenversorgung) und Forschungsvorhaben, deren Gegenstand die Qualitätssicherung in der Krankenversorgung ist (§ 34 SächsKHG). In beiden Fällen ist die Datenübermittlung (auch) ohne Einwilligung des Patienten zulässig. Die Voraussetzungen sind jedoch höchst unterschiedlich.

10.1.2 Viel Kritik am Entwurf der 15. Verordnung zur Änderung betäubungsmittelrechtlicher Vorschriften

In 8/10.1.1 habe ich mich kritisch über das zum 1. April 2000 in Kraft getretene Betäubungsmittel-Änderungsgesetz geäußert, insbesondere über die darin enthaltene Verordnungsermächtigung zum Aufbau eines zentralen Substitutionsregisters beim Bundesinstitut für Arzneimittel und Medizinprodukte (Bundesinstitut). In diesem Register werden die Daten der Ärzte gespeichert, die zur Behandlung Drogenabhän-

giger mit Substitutionsmitteln qualifiziert sind, außerdem die patientenbezogenen Verschreibungen von Substitutionsmitteln. Dies soll zum einen der Kontrolle dienen, ob die verschreibenden Ärzte über die entsprechende Qualifikation verfügen, zum anderen soll verhindert werden, dass ein Patient von mehreren Ärzten Substitutionsmittel verordnet erhält und sie dann missbräuchlich verwendet (Überdosis oder Verkauf).

Auch an dem vom Bundesministerium für Gesundheit im Herbst 2000 vorgelegten Verordnungsentwurf zur Änderung der Betäubungsmittel-Verschreibungsverordnung gab es eine Menge zu kritisieren. Jeder Umgang mit personenbezogenen Daten bedarf - insbesondere im Gesundheitswesen - einer normenklaren Rechtsgrundlage. Deshalb muss jede Rechtsverordnung nach Inhalt, Zweck und Ausmaß der Datenverarbeitung im Gesetz eine nachvollziehbare, besser: vorhersehbare Grundlage haben. So schreiben es das Volkszählungsurteil (BVerfGE 65, 1 ff) und Art. 80 Abs. 1 Satz 2 Grundgesetz vor. Der Verordnungsentwurf jedoch entsprach dieser Anforderung nicht. Teilweise ging er sogar über die gesetzliche Ermächtigung hinaus.

Zum Beispiel:

1. *Genehmigungsvorbehalt*
   Vorgesehen war, dass ein Arzt einem Patienten größere Mengen eines Substitutionsmittels zur eigenverantwortlichen Einnahme nur mit behördlicher Genehmigung verschreiben darf. Offen blieben die Genehmigungsvoraussetzungen. Sie hätten jedoch angegeben werden müssen, da sie Grundlage für die Datenerhebung der Genehmigungsbehörde sind. Ohne Kenntnis der Genehmigungsvoraussetzungen kann niemand beurteilen, welche Daten für die Entscheidung benötigt werden.
   Problematisch war dabei, dass die Betäubungsmittel-Verschreibungsverordnung einen Arzt aus rechtssystematischen Gründen nicht zur Offenbarung des von § 203 Abs. 1 StGB geschützten Patientengeheimnisses verpflichten kann. Folglich hätte der Arzt den Patienten vor dem Genehmigungsantrag um eine Schweigepflichtentbindung bitten müssen. Da für die Aufsichtsbehörden jedoch die personenbezogene Kenntnis einer Verschreibung von größeren Mengen eines Substitutionsmittels aus Gründen der Sicherheit und Kontrolle des Betäubungsmittelverkehrs notwendig ist und eine einfache Anzeige denselben Zweck erfüllt, ist der Entwurf in diesem Sinne geändert worden.
2 *Codierung des Patientennamens*
   Die Ermächtigungsgrundlage im Betäubungsmittelgesetz sieht anonyme Meldungen der verschreibenden Ärzte an das Bundesinstitut vor. Anonymisieren bedeutet das Verändern personenbezogener Daten in der Weise, dass sie nicht mehr einer bestimmten oder bestimmbaren Person zugeordnet werden können oder dass eine Zuordnung nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft möglich ist. Diese Anforderung erfüllt die vorgesehene „Anonymisierung“ nicht (1. und 2. Buchstabe des Vornamens, 1. und 2. Buchstabe des Nachnamens, Geschlecht, letzte Ziffer von Geburtstag, -monat, -jahr). Mit einfachsten Zusatzdaten, z. B. aus dem regionalen Fernsprechbuch oder dem Einwohnermelderegister, lässt sich der Code mit einiger Treffsicherheit einer bestimmten Person zuordnen, nicht zuletzt deshalb, weil Name und Anschrift des

Arztes unverschlüsselter Bestandteil der Meldung sind und Patienten regelmäßig einen Arzt in ihrer Umgebung wählen. Das Risiko einer Identifizierung dürfte sich vermindern, wenn einem zur Substitutionsbehandlung qualifizierten Arzt für seine Meldungen eine Schlüsselnummer zugeteilt würde.

Diesen Bedenken trägt auch der überarbeitet Verordnungsentwurf keine Rechnung.

3. *Halbjährliche Meldungen von Weiterverschreibungen*
Es war eine Regelung vorgesehen, wonach die Ärzte zum 31. März und 30. September eines jeden Jahres die Codes ihrer noch substituierten Patienten hätten melden müssen. Der Sinn erschloss sich mir nicht. Das Erfordernis einer Meldung habe ich nur im Fall des erstmaligen und letztmaligen Verschreibens gesehen. Deshalb habe ich angeregt, auf Datenübermittlungen über das Weiterverschreiben zu verzichten, nicht zuletzt deshalb, weil der Patientencode keine Anonymität und damit keine Datensicherheit gewährleistet (s. o.). Es erschien mir unverhältnismäßig (von Aufwand und Kosten für Ärzte und Verwaltung ganz abgesehen), wenn bundesweit zweimal jährlich die Daten *aller* Substitutionspatienten dem Risiko unbefugter Kenntnisnahme ausgesetzt werden.
Mein Vorschlag wurde umgesetzt. Nach dem geänderten Entwurf haben die Ärzte nur noch Beginn und Ende einer Suibstitutionsbehandlung zu melden.

4. *Wer findet die „schwarzen Schafe" unter den Ärzten?*
Das Betäubungsmittelgesetz enthält eine Verfahrenskonzeption, wonach die Ärztekammern dem Bundesinstitut die zur Substitutionsbehandlung qualifizierten Ärzte melden, damit das Bundesinstitut durch einen Abgleich dieser Daten mit den gemeldeten Verschreibungen die Ärzte „herausfiltern" kann, die trotz fehlender Qualifikation Substitutionsmittel verschreiben. Wird ein solcher Arzt festgestellt, informiert das Bundesinstitut die zuständigen Überwachungsbehörden.

Der Verordnungsentwurf stellte diese Konzeption auf den Kopf und wies den Ärztekammern die Aufgabe zu, zweimal im Jahr die nicht zur Substitutionsbehandlung qualifizierten Ärzte selbst festzustellen und über diese *nicht* qualifizierten Ärzte dem Bundesinstitut Rückmeldung zu erstatten. Damit die Ärztekammern den Abgleich überhaupt hätten durchführen können, sollte das Bundesinstitut den Ärztekammern diejenigen Ärzte mitteilen, die Substitutionsmittel verschrieben haben. Der Haken an der Sache: Das Betäubungsmittelgesetz führt die Mitteilungspflichten des Bundesinstituts abschließend auf; solche Mitteilungen an die Ärztekammern sind darin nicht enthalten.

Der überarbeitete Entwurf hat das Verfahren wieder auf die Füße gestellt. Wie in der Verordnungsermächtigung vorgesehen, führt das Bundesinstitut den Datenableich durch, um die Ärzte „herausfiltern", die trotz fehlender Qualifikation Substitutionsmittel verschreiben.

Hier sei die Frage erlaubt, ob jemand ernsthaft damit rechnet, dass ein nicht zur Substitutionsbehandlung qualifizierter Arzt die Verschreibung von Substitutions-

mitteln an das Bundesinstitut meldet und so auf sein ungesetzliches Handeln aufmerksam macht. Die Bürokratie treibt merkwürdige Blüten.

10.1.3 Patientendatenschutz in Krankenhäusern in öffentlich-rechtlicher Trägerschaft - Verarbeitung von Patientendaten im Auftrag durch Private

Nach § 33 Abs. 10 SächsKHG kann sich das Krankenhaus zur Verarbeitung von Patientendaten anderer Personen oder Stellen bedienen, wenn sichergestellt ist, dass diese die Datenschutzbestimmungen dieses Gesetzes und die § 203 StGB entsprechende Schweigepflicht einhalten.

Die Auftragserteilung bedarf der vorherigen Zustimmung durch die zuständige Behörde (Regierungspräsidium).

Seit geraumer Zeit befasst sich eine Arbeitsgruppe aus Vertretern der zustängigen Ressorts, der Sächsischen Ärztekammer und der Sächsischen Krankenhausgesellschaft unter meiner Beteiligung damit, das vorgeschriebene Zustimmungsverfahren durch eine Verwaltungsvorschrift einheitlich zu regeln. Problematisch ist insbesondere die Frage, wie und durch wen das Personal privater Auftragnehmer auf Einhaltung einer § 203 StGB entsprechenden Schweigepflicht verpflichtet werden können.

An der lang diskutierten Auffassung, dass der Hinweis auf § 203 StGB in § 33 Abs. 10 SächsKHG eine Auftragsdatenverarbeitung durch Private zulässt, die nicht unbedingt der ärztlichen Schweigepflicht (§ 203 Abs. 1 und Abs. 3 StGB) unterliegen, ändert auch Art. 8 Abs. 3 EG-Datenschutzrichtlinie nichts. Danach darf die Verarbeitung von Patientendaten (in jedweder Form) *nur durch ärztliches Personal*, das nach dem einzelstaatlichen Recht, einschließlich der von den zuständigen einzelstaatlichen Stellen erlassenen Regelungen, *dem Berufsgeheimnis unterliegt* (ärztliche Schweigepflicht nach der Berufsordnung), oder durch sonstige Personen, *die einer (der ärztlichen Schweigepflicht) entsprechenden Geheimhaltungspflicht unterliegen*, erfolgen. Meine ursprüngliche Meinung, dass diese EG-rechtliche Bestimmung die Verarbeitung von Patientendaten im Auftrag durch Private, die nach dem Verpflichtungsgesetz zur Verschwiegenheit verpflichtet wurden, nicht zulässt, habe ich - nicht zuletzt durch die vom SMS geleistete Überzeugungsarbeit - revidiert. Weil die nach dem Verpflichtungsgesetz für den öffentlichen Dienst besonders Verpflichteten in strafrechtlicher Hinsicht Amtsträgern gleichgestellt worden sind (§§ 11 Abs. 1 Nr. 4 a, 203 Abs. 2 Nr. 2 StGB), ist von einer „entsprechenden Geheimhaltungspflicht“ i. S. v. Art. 8 Abs. 3 EG-Datenschutzrichtlinie auszugehen; die Auftragsdatenverarbeitung durch „verpflichtete“ Private ist daher nach Maßgabe des § 33 Abs. 10 SächsKHG zulässig. Das hat zur Folge, dass z. B. die Aufbewahrung von Krankenunterlagen in einem privat betriebenen Archiv im Auftrag eines Krankenhauses ebenso zulässig ist, wie z. B. die Mikroverfilmung solcher Unterlagen in einem Privatunternehmen, vorausgesetzt, die Mitarbeiter stehen nach dem Verpflichtungsgesetz unter einem strafbewehrten Schweigegebot.

10.1.4 Auswertung von Patientenakten eines Krankenhauses für eine Dissertation (Doktorarbeit)

Ein Krankenhaus fragte, ob und unter welchen Voraussetzungen ein dort angestellter Arzt Patientenakten für seine Dissertation auswerten dürfe. Ich habe dem Krankenhaus die Rechtslage wie folgt erläutert:

Der Arzt darf die Patientenakten seiner Fachabteilung gemäß § 34 Abs. 1 SächsKHG für seine Dissertation, also zu einem wissenschaftlichen Forschungsvorhaben, verarbeiten und nutzen. Sofern er Patientenakten einer anderen Fachabteilung benötigt, findet § 34 Abs. 2 SächsKHG Anwendung. Diese Vorschrift sieht grundsätzlich die Einwilligung des Patienten vor. Unter den Voraussetzungen des § 34 Abs. 3 kann von einer Einwilligung abgesehen werden. Zu diesen Voraussetzungen gehört, dass der Zweck des Forschungsvorhabens auf andere Weise nicht erfüllt werden kann *und* das berechtigte Interesse der Allgemeinheit an der Durchführung des Forschungsvorhabens das Geheimhaltungsinteresse des Patienten erheblich überwiegt. Für den Fall jedoch, dass es nicht zumutbar ist, die Einwilligung einzuholen und schutzwürdige Interessen des Patienten nicht beeinträchtigt werden, darf der Arzt die Patientendaten einer anderen Fachabteilung für seine Dissertation auswerten.

Auf jeden Fall aber gilt: Sobald es der Forschungszweck erlaubt, sind die Patientendaten so zu verändern, dass sie keine Rückschlüsse auf eine bestimmte oder bestimmbare Person zulassen. Wo dies nicht möglich ist, sind die Merkmale, die einen Patienten bestimmbar machen, gesondert zu speichern und zu löschen, sobald der Forschungszweck erreicht ist (§ 34 Abs. 4 SächsKHG).

10.1.5 Zertifizierungsverfahren interessierter Krankenhäuser durch Visitoren der „Kooperation für Transparenz und Qualität im Krankenhaus (KTQ)“ in Siegburg

Meinen Informationen zufolge nehmen im Freistaat Sachsen drei Krankenhäuser an dem Zertifizierungsverfahren durch die KTQ teil.
Datenschutzrechtlich problematisch ist die Einsichtnahme in Patientenunterlagen, aber auch in Personalakten sowie die anschließende Dokumentation im Zertifizierungsverfahren durch die Visitoren der KTQ.

§ 33 Abs. 3 Nr. 4 SächsKHG enthält zwar eine Rechtsgrundlage für die Übermittlung von Patientendaten, soweit sie zur Durchführung von qualitätssichernden Maßnahmen in der Krankenversorgung *erforderlich* ist und wenn das Interesse der Allgemeinheit an der Durchführung der beabsichtigten Maßnahme die schutzwürdigen Belange des Patienten *erheblich* überwiegt. Wegen des generell zu beachtenden Erforderlichkeitsgrundsatzes und dem Abwägungsgebot „Allgemeininteresse gegen schutzwürdige Patientenbelange“ ist jedoch stets zu prüfen, ob der angestrebte Zweck ohne personenbezogene Patientendaten erreicht werden kann. Bevorzugt sollten deshalb nur anonymisierte/pseudonymisierte Patientendaten zur Verfügung gestellt werden, nicht zuletzt um Konflikte mit der ärztlichen Schweigepflicht von vornherein zu vermeiden. Auch § 113 Abs. 2 SGB V (Verpflichtung der Krankenhäuser und ihrer

Mitarbeiter, dem Prüfer die *notwendigen* Unterlagen vorzulegen und Auskünfte zu erteilen) würde m. E. daran nichts ändern, wenn die Qualitätskontrolle auf den Vorschriften des SGB V fußen würde, wofür ich allerdings keinen Anhaltspunkt habe.

Soweit öffentlich-rechtliche Krankenhäuser betroffen sind, gilt es bezüglich der Personaldaten § 31 Abs. 2 SächsDSG und § 121 SächsBG zu beachten, die einer Offenbarung von Beschäftigtendaten an externe Dritte enge Grenzen setzen.

Ich hoffe, dass mein Appell an die Krankenhäuser nicht ungehört verhallt.

10.1.6 EU-Projektvorschlag „Elektronischer Impfpass“ der Debis-Systemhaus SfH

Das SMS informierte mich über die Absicht, einen digitalen Impfpass im Rahmen eines Pilotprojekts für Deutschland, Polen und Tschechien zu entwickeln, zu testen und schließlich einzuführen und bat mich um datenschutzrechtliche Stellungnahme.
In meiner Antwort an das SMS machte ich deutlich, dass ich nur für sächsische öffentliche Stellen und nicht für die niedergelassenen Ärzte, die in erster Linie für den Inhalt des elektronischen Impfpasses verantwortlich sein werden, zuständig bin. Deshalb vermochte ich mich nur allgemein zum Einsatz medizinischer Chipkarten zu äußern und habe auf die Entschließung der 50. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 9./10. November 1995 zu „datenschutzrechtlichen Anforderungen an den Einsatz von Chipkarten im Gesundheitswesen“ hingewiesen (siehe 4/16.1.4).

Da mir eine Rechtsgrundlage für die Einführung eines elektronischen Impfpasses nicht ersichtlich ist, halte ich die Verwendung solcher Chipkarten grundsätzlich nur mit *Einwilligung* der Betroffenen für denkbar. Diese Einwilligung muss informiert, freiwillig und jederzeit widerrufbar sein.
Es ist allerdings unerfindlich, weshalb die impfungsrelevanten Daten der komplizierten und teuren Chipkartentechnik bedürfen sollten. Ein digitaler Impfpass setzt nämlich voraus, dass die zuständigen Stellen über entsprechende Lese- und Schreibgeräte verfügen (fehlende Lese- und Schreibtechnik macht den Impfpass zum Nachteil des Inhabers wertlos). Aber auch die Betroffenen müssen wissen, welche Informationen auf der Chipkarte gespeichert sind, um beispielsweise anstehende Impftermine wahrnehmen zu können. Auch ihre Einsichtsrechte müssten über eine entsprechende Technik garantiert sein.

Die Empfehlungen der EU zur Einführung einer (manuellen) europäischen Notfall-Gesundheitskarte, die u. a. auch Impfnachweise enthält, weisen deshalb m. E. in die richtige Richtung, zumal die Angaben in mehreren Amtssprachen verfügbar sind, was insbesondere für das vorgesehene Einsatzgebiet (Deutschland, Polen, Tschechien) von Bedeutung sein dürfte.

Das von mir untersuchte „Exposé“ der Debis Systemhaus SfH hat mich keinesfalls von der Erforderlichkeit eines digitalen Impfpasses überzeugt, so dass ich mich

außerstande sah, das Projekt zu befürworten. Mit anderen Worten: Das Modell halte ich - vorbehaltlich näherer Informationen - für technisch überzogen aufwendig und deshalb für wertlos.

Eine Reaktion steht noch aus.

10.1.7 Veröffentlichungen der Landesärztekammern über Ruhen, Entzug, Widerruf und Rücknahme von Approbationen im Sächsischen Ärzteblatt

Die Frage, ob die Landesärztekammer die Namen von Ärzten, deren Approbation ruht, entzogen, widerrufen oder zurückgenommen wurde, veröffentlichen darf, wird von den Landesdatenschutzbeauftragten kontrovers diskutiert. Die Befürworter argumentieren mit der Abwägung der Rechtsgüter, wonach der Gesundheitsschutz des einzelnen Patienten (z. B. keine Überweisung von Patienten an einen solchen Arzt) höher zu bewerten ist als das Interesse des betroffenen Arztes an der Nichtveröffentlichung seines Namens.

Ich habe der Sächsischen Landesärztekammer mitgeteilt, dass in Sachsen eine Veröffentlichung im Sächsischen Ärzteblatt mangels Rechtsgrundlage nicht in Betracht kommt.

Jede Veröffentlichung ist eine Datenübermittlung an einen unbestimmten (privaten) Personenkreis, die nur unter den in § 15 Abs. 1 i. V. m. § 12 Abs. 1 SächsDSG genannten Voraussetzungen und den in § 11 Abs. 4 Nr. 1 bis 8 SächsDSG abschließend aufgezählten Zwecken zulässig wäre. Keinem der genannten Zwecke dient die Veröffentlichung, auch nicht dem in Nr. 6 genannten „zur Abwehr erheblicher Nachteile für das Gemeinwohl“. Selbst wenn die Berufsausübung eines nicht approbierten Arztes den Tatbestand eines erheblichen Nachteils für das Gemeinwohl erfüllen sollte, wäre es nach meiner Auffassung der falsche Ansatz, dem durch eine Veröffentlichung im *Sächsischen Ärzteblatt* begegnen zu wollen. Hier sehe ich die Behörden in der Pflicht, wirksamere Maßnahmen zu ergreifen, damit ein Patient „im schlimmsten Fall“ vor einer geschlossenen Praxis steht.

Auch eine Übermittlung nach § 15 Abs. 1 Nr. 2 SächsDSG ist schon deshalb ausgeschlossen, weil die Leserschaft des Ärzteblatts kein berechtigtes Interesse an der Kenntnis dieser Ärzte darzulegen vermag. Denkbare schutzwürdige Interessen des Arztes am Unterbleiben der Übermittlung müssten im Übrigen gemäß § 15 Abs. 3 SächsDSG vor einer Übermittlung durch Anhörung in die Entscheidung einbezogen werden.

10.1.8 Aufbewahrungsfrist für Labordaten

Der Leiter eines Krankenhauslabors fragte nach der Aufbewahrungsfrist für die im laboreigenen EDV-System gespeicherten Patientendaten. Dies seien Name, Vorname, Geburtsdatum, Station, die Parameter der Analyse und ggf. Zusatzbemerkungen. Ein Ausdruck dieser Daten werde der Station zugeleitet, wo er zur Krankenakte des

Patienten genommen und zusammen mit dieser die für Patientenakten üblichen 30 Jahre aufbewahrt werde. Der Laborleiter fragte, ob die nach der „Richtlinie der Bundesärztekammer zur Qualitätssicherung in medizinischen Laboratorien“ für mindestens fünf Jahre aufzubewahrenden Labordaten nach Ablauf dieser Frist gelöscht werden könnten oder ob sie wie die Krankenakte 30 Jahre vorgehalten werden müssten.

Ich habe mich dazu wie folgt geäußert:

Datenschutzrechtlich bestehen gemäß § 33 Abs. 6 SächsKHG keine Bedenken gegen die Löschung nach fünf Jahren; denn diese Vorschrift besagt, dass Patientendaten zu löschen sind, wenn sie
- zur Durchführung des Behandlungsvertrages nicht mehr erforderlich sind,
- vorgeschriebene Aufbewahrungsfristen abgelaufen sind und
- kein Grund zu der Annahme besteht, dass durch die Löschung schutzwürdige Belange des Betroffenen beeinträchtigt werden.

Diese Voraussetzungen dürften erfüllt sein. Spezialgesetzliche Aufbewahrungsfristen für Labordaten bestehen derzeit nicht. Das Krankenhaus genügt mit der Speicherung der Labordaten in der Krankenakte seiner Dokumentationspflicht, die dem Patienten als Nebenleistung aus dem Behandlungsvertrag geschuldet wird. Somit bleiben die schutzwürdigen Belange des Patienten auch nach der Löschung seiner Daten im EDV-System des Labors gewahrt. Für Zwecke der Mit-, Nach- und Weiterbehandlung können die Daten ggf. 30 Jahre lang der Krankenakte entnommen werden.

10.1.9 Kariesprophylaxe in Kindergärten und Schulen; zu Risiken und Nebenwirkungen fragen Sie mal Ihren Datenschützer

Grundlage für die Kariesprophylaxe in Kindergärten und Schulen (Gruppenprophylaxe) ist § 21 SGB V. Danach haben die Krankenkassen im Zusammenwirken mit den für die Zahngesundheitspflege in den Ländern zuständigen Stellen Maßnahmen zur Erkennung und Verhütung von Zahnerkrankungen zu fördern und sich an den Kosten zu beteiligen. Einzelheiten sind in einer Rahmenvereinbarung zu regeln. Diese wurde in Sachsen zwischen den Verbänden der verschiedenen Krankenkassen, dem Freistaat Sachsen, dem Sächsischen Landkreistag, Sächsischen Städte- und Gemeindetag, der Landeszahnärztekammer, der Kassenzahnärztlichen Vereinigung sowie der Landesarbeitsgemeinschaft für Jugendzahnpflege des Freistaates Sachsen e. V. (LAGZ) geschlossen.

Nach dieser Rahmenvereinbarung gehört es u. a. zu den Aufgaben der LAGZ, in sächsischen Kindergärten und Schulen die Fluoridierung der Zähne zu organisieren. Als Fluoridierungsmaßnahmen kommen das Einputzen eines Gelees, die Touchierung der Zähne mit einem Fluoridlack oder das Spülen mit einer Fluoridlösung in Betracht. Die beiden letztgenannten Maßnahmen sind approbierten Zahnärzten bzw. ausgebildetem zahnärztlichem Personal vorbehalten. Welche Maßnahme in einer Gruppe durchgeführt wird, entscheidet und verantwortet der zur Prophylaxe berechtigte Zahnarzt. Dies kann sowohl der Jugendzahnarzt des Gesund-

heitsamtes als auch ein niedergelassener Zahnarzt sein. Niedergelassene Zahnärzte haben „neutral“ aufzutreten und dürfen die Maßnahmen nicht in der eigenen Praxis durchführen.

Da die Fluoridierung eine ärztliche Behandlung, aber keine Zwangsmaßnahme ist, bedarf sie der Einwilligung. Bei Gruppenprophylaxen in der Schule wurde dies von Beginn an parktiziert, wenn auch mit einem nicht datenschutzgerechten Formbatt (s. u.). Dagegen sind ohne Wissen der Eltern zumindest in den Kindergärten einer sächsischen Großstadt jahrelang die vom Gesundheitsamt kostenlos zur Verfügung gestellten Flouridgelees verwendet worden. Ein Fluoridgelee ist jedoch ein Medikament, das ein Kind unter 6 Jahren nicht erhalten soll. Als sich auf den Zähnen von Kindern auffällige, weiße Flecken zeigten, war das für den Hauszahnarzt der Hinweis auf eine mögliche *Überflouridierung.* Die weitere Recherche ergab die Verwendung von Flouoridgelees im Kindergarten.
Anstatt die Maßnahme einzustellen, erhielten die Kindergärten vom Jugendzahnärztlichen Dienst dieser Stadt ab August 2000 Formblätter (von der LAGZ für den Schulbereich konzipiert), mit denen die Eltern erklären sollten, ob ihr Kind die Zähne weiterhin mit einem Flouridgelee putzen darf oder nicht, an welchen Allergien es leidet, ob es Asthma hat und ob es vom Hauszahnarzt bereits individualprophylaktisch behandelt wird. Zu Risiken und Nebenwirkungen, zur Altersgrenze, zum Verbleib des Formblatts wurde nichts gesagt, auch nicht, warum die *Ablehnung* der Flouridierungsmaßnahme schriftlich erklärt werden sollte. Mit diesen Fragen kamen die Eltern zu mir.
Wie sich herausstellte, hatten die Jugendzahnärzte Fluoridgelees fahrlässig als Kosmetikum und nicht als Medikament betrachtet. Und keiner von ihnen hinterfragte, warum das Formblatt die Angabe von Schuljahr, Schule und Klasse verlangte. Die LAGZ hat inzwischen ein aufklärendes Rundschreiben versandt.

Das für den Schulbereich konzipierte Formblatt war nicht datenschutzgerecht:
- Es fehlte die „aufgeklärte Einwilligung“ (Hinweise auf Wirkungsweise, Risiken und Nebenwirkungen, Freiwilligkeit der Teilnahme und Möglichkeit zum Widerruf, Aufbewahrung des Formblatts bei der ärztlichen Dokumentation, Vernichtung nach 10 Jahren gemäß Zahnärztlicher Berufsordnung).
- Es hätte nicht pauschal nach Allergien gefragt werden dürfen. Ausreichend wäre es gewesen, die Allergien zu nennen, die eine Flouoridierung ausschließen, damit erst gar keine Einwilligung erteilt wird.
- Einer ausdrücklichen Erklärung über die *Nichtteilnahme* eines Kindes bedarf es nicht.
- Ein Hinweis auf die Weitergabe des Formblatts im verschlossenen Umschlags fehlte.
- Die mögliche Anwesenheit Dritter (z. B. Mitschüler, Lehrer, Erzieher) erfordert eine Schweigepflichtentbindung.

Vor diesem datenschutzrechtlichen Hintergrund und mit Blick auf die unterschiedlichen Fluoridierungsmöglichkeiten (Lack, Gelee, Fluoridlösung) sowie die ganz unterschiedlichen Nebenwirkungen der einzelnen Präparate sind von der LAGZ vollständig neue Formblätter konzipiert und mit mir abgestimmt worden.

Ich habe das SMS von der Angelegenheit in Kenntnis gesetzt. Im Zusammenhang mit der anstehenden Änderung des Gesetzes über den öffentlichen Gesundheitsdienst, des Schulgesetzes, des Gesetzes zur Förderung von Kindern in Kindertageseinrichtungen sowie der Folgeänderungen in der Schulgesundheitspflegeverordnung (siehe Nr. 7.1.2) soll nun auch die Durchführung der Kariesprophylaxe klar geregelt werden.

10.2 Sozialwesen

10.2.1 Übermittlung arzt- und patientenbezogener Daten durch Luftrettungsdienstunternehmen an die Krankenkassen zu Zwecken der Abrechnung von Rettungsdiensteinsätzen

Bei Luftrettungseinsätzen stellt der Notarzt, der daran teilnimmt, die sog. Verordnung des Fluges aus, in der er dessen medizinische Notwendigkeit im Einzelfall begründet. Im Falle der Verlegung eines Patienten von einem Krankenhaus in ein anderes (sog. Sekundär-Rettung) verordnet der abgebende (Krankenhaus-)Arzt, der auch den Hubschrauber angefordert hat, den Einsatz des Rettungshubschraubers.
Die gesetzlichen Krankenkassen verlangen von den Luftrettungsdienstunternehmen zum Zweck der Abrechnung von Einsätzen des Rettungshubschraubers diese Verordnung des Notarztes sowie das Notfallprotokoll. Im Falle einer sog. Sekundär-Rettung verlangen die gesetzlichen Krankenkassen von den Ärzten bzw. Krankenhäusern Auskunft darüber, weshalb sie die Inanspruchnahme des Luftrettungsdienstes für erforderlich erachtet haben.
Ein Luftrettungsdienstunternehmen hat mich gebeten, zu prüfen, ob dieses Verlangen der Krankenkassen begründet, ob also insbesondere die entsprechende Datenübermittlung an die Krankenkasse rechtmäßig sei.

1. Gesetzliche Krankenkassen als Körperschaften des öffentlichen Rechts dürfen personenbezogene Daten nur erheben und weiterverarbeiten, wenn ein Gesetz dies erlaubt oder soweit der Betroffene eingewilligt hat. Zu Abrechnungszwecken dürfen die Krankenkassen Sozialdaten auf der Grundlage des § 284 Abs. 1 S. 1 Nr. 8 SGB V im Rahmen des Erforderlichen erheben. Je nach dem, mit welchem Leistungserbringer (Arzt, Apotheker, Krankenhaus, Heil- und Hilfsmittelerbringer, sonstige Leistungserbringer) abzurechnen ist, konkretisieren die Übermittlungsvorschriften der §§ 294 ff. SGB V, welche Daten zur Abrechnung erforderlich sind.

   Einschlägig ist hier § 302 SGB V: Die Vorschrift regelt, welche Daten die sog. *sonstigen Leistungserbringer* zu Abrechnungszwecken an die Krankenkassen zu übermitteln haben.
   Diejenigen, die Krankentransporte oder Fahrten zur Notfallrettung (so die Unterscheidung nach §§ 1 f. SächsRettDG) durchführen, wozu im Rechtssinne auch Rettungsflüge gehören (§ 11 Abs. 1 SächsRettDG), sind Leistungserbringer im Sinne des SGB V. Zwar werden diese Leistungen in der Aufzählung der Leistungsarten der Krankenversicherung in § 11 SGB V nicht erwähnt. Aber in § 60 SGB V ist die sog. Fahrkostenübernahme durch die Krankenkasse geregelt.

Fahrkosten sind keine Hauptleistung der Krankenversicherung, sondern eine unselbständige Nebenleistung (Gerlach in: Hauck, Kommentar zum SGB V, § 60 Rdnr. 8; als Hauptleistung kommen alle in § 11 SGB V aufgeführten Leistungsarten in Betracht, wenn sie im Inland in Anspruch genommen werden).
Diejenigen, die Krankentransporte und Notfallrettungen durchführen, sind daher „weitere“, d. h. sonstige Leistungserbringer im Sinne von § 302 Abs. 1 SGB V.

Nach § 302 Abs. 1 SGB V sind die Leistungserbringer verpflichtet, die von ihnen erbrachten Leistungen nach Art, Menge und Preis zu bezeichnen und den Tag der Leistungserbringung sowie die Arztnummer des verordnenden Arztes, die Verordnung des Arztes mit der Diagnose und den erforderlichen Angaben über den Befund und die Angaben nach § 291 Abs. 2 Nr. 1 bis 6 SGB V (Krankenversichertenkarte) anzugeben. Das Nähere über Form und Inhalt des Abrechnungsverfahrens bestimmen Richtlinien (§ 302 Abs. 2 S. 1 SGB V), hier die sog. Krankentransport-Richtlinien in der Fassung vom 17. Juni 1992).

2. Die *ärztliche Verordnung* gibt der Krankenkasse Aufschluss darüber, ob die Voraussetzungen des § 60 Abs. 1 SGB V vorliegen und sie damit zur Übernahme der sog. Fahrkosten verpflichtet ist. Welchen Inhalt die Verordnung haben muss, regelt § 302 Abs. 1 und Abs. 2 SGB V i. V. m. der Krankentransport-Richtlinien. In der Verordnung hat der Arzt die Diagnose anzugeben und die erforderlichen Angaben über den Befund zu machen.
   Erforderlich sind solche Angaben, die den Einsatz gerade dieses Transportmittels begründen. § 60 Abs. 1 und Abs. 2 SGB V sowie die Krankentransport-Richtlinien bestimmen, wann welche Art von Beförderungsmittel durch den Arzt zu verordnen ist. Rettungshubschrauber sind dann anzufordern, wenn die Notwendigkeit einer schnellen Heranführung des Notarztes an den Unfallort zur Durchführung lebensrettender Maßnahmen und zur Herstellung der Transportfähigkeit des Patienten mit dem jeweils geeigneten Transportmittel besteht (4.2.4 der Krankentransport-Richtlinien). Der Befund muss also Aussagen darüber enthalten, weshalb die schnelle Durchführung lebensrettender Maßnahmen am Unfallort notwendig war und gegebenenfalls zusätzlich, weshalb der schnelle Transport durch Hubschrauber in ein Krankenhaus erforderlich war.
   Solche Angaben sind Aussagen zu den drei grundlegenden Lebensfunktionen (Kreislauf, Atmung, Herz), Aussagen über Verletzungen, über vom Notarzt eingeleitete Maßnahmen sowie die Diagnose. Im oben genannten Fall des irrtümlichen oder absichtlichen Fehlalarms ist entsprechend zu verfahren.

   Zusammengefasst:
   Die Verordnung des Arztes mit Diagnose und erforderlichen Angaben zum Befund ist gemäß § 302 Abs. 1, Abs. 2 SGB V i. V. m. der Krankentransport-Richtlinie durch den Leistungserbringer, d. h. das Luftrettungsunternehmen, der Krankenkasse zu übermitteln.

3. *Protokolle eines Notarzteinsatzes* dienen der Information des weiterbehandelnden Arztes im Krankenhaus. Sie werden nicht für die Abrechnung der ärztlichen Leistung mit den gesetzlichen Krankenkassen verwendet. (Für die Abrechnung

der ärztlichen Leistung übermittelt der Notarzt der Kassenärztlichen Vereinigung die in § 295 Abs. 1 Satz 1 Nr. 2 SGB V genannten Daten, d. h. Angaben zu den erbrachten Leistungen einschließlich des Tages der Behandlung sowie Diagnosen.) Genausowenig sind sie für die Abrechnung des Rettungsdienst-Unternehmers gemäß § 302 Abs. 1 SGB V geeignet.

Das sog. Notfallprotokoll, das der Information des weiterbehandelnden Arztes dienen soll, kann nämlich Daten enthalten, die über das nach § 302 Abs. 1 SGB V geforderte erforderliche Maß hinausgehen. In der Regel enthält ein solches Protokoll Angaben zum Befund (Kreislauf, Atmung, Herz, neurologische Befunde, Verletzungen), zur (vorläufigen) Diagnose und zu den durch den Notarzt vorgenommenen Maßnahmen. Je nach Einzelfall können aber auch alle Angaben, die in dem Notfallprotokoll enthalten sind, erforderlich sein, um zu begründen, weshalb der Einsatz des Rettungshubschraubers notwendig war. Dann wären alle diese Angaben auch der Krankenkasse zu übermitteln. Da das Notfallprotokoll jedoch einem anderen Zweck dient als dem, den Einsatz des Rettungshubschraubers zu begründen, deckt sich der Datensatz des Protokolls eben nicht ohne weiteres mit dem nach § 302 Abs. 1 SGB V erforderlichen Datensatz. Ein Verfahren, das vorsieht, beim Einsatz eines Notarztwagens oder Rettungshubschraubers statt der Verordnung des Notarztes das Notfallprotokoll zu Zwecken der Abrechnung der Fahrtkosten an die Krankenkasse zu übermitteln, wäre unzulässig, da nicht gewährleistet ist, dass die Krankenkasse nicht mehr Daten erhält, als ihr für ihre Abrechnung zustehen.

Im Falle des Verlegungsfluges gilt Entsprechendes: Nicht alle Daten, die der abgebende Arzt dem begleitenden Notfallarzt oder dem aufnehmenden Krankenhaus zur ordnungsgemäßen (fachgerechten) Übergabe des Patienten mitteilen muss, werden für die Abrechnung des Hubschraubereinsatzes benötigt.

Die der Erhebungsbefugnis der Krankenkasse korrespondierende Übermittlungsbefugnis des die Notfallrettung oder den Krankentransport durchführenden Unternehmers ergibt sich aus § 28 Abs. 1 Nr. 4 SächsRettDG i. V. m. § 302 SGB V. Die Übermittlungsbefugnis des Notarztes ergibt sich aus § 302 SGB V.

Zusammengefasst:

Zur Abrechnung von Fahrtkosten hat der Unternehmer die in § 302 SGB V genannten Daten an die Krankenkassen zu übermitteln. Die sog. Notarztprotokolle enthalten zum Teil solche Daten. Sie gehen aber, je nach Einzelfall, darüber hinaus. Deshalb dürfen sie nicht als „Verordnungsersatz“ an die Krankenkasse übermittelt werden. Vielmehr hat der Notarzt eine Verordnung zum Einsatz des Hubschraubers auszustellen, die sich auf die für die Abrechnung der Fahrtkosten erforderlichen Daten beschränkt.

Zweckmäßig wäre ein eigener Vordruck mit entsprechend vermindertem Umfang.

Unzutreffend war die - naheliegende - Auffassung des Luftrettungsdienstunternehmens, dass für die Überprüfung der Notwendigkeit von Krankentransportleistungen der Medizinische Dienst der Krankenkassen zuständig sei. Die Aufgaben des Medizinischen Dienstes beschreibt § 275 SGB V. Er hat Gutachten darüber zu erstellen, welche Leistungen die Krankenkasse für einen bestimmten Versicherten in Zukunft erbringen sollte, um dessen Gesundheit wieder herzustellen. Der MDK ist,

abgesehen von einigen Fallgestaltungen, die hier nicht einschlägig sind, nicht dafür zuständig, die Notwendigkeit bereits erbrachter Leistungen zu überprüfen.

Ich habe meine Rechtsauffassung dem SMI als oberster Fachaufsichtsbehörde für das Rettungsdienstwesen (§ 16 Abs. 1 Satz 3 SächsRettDG), dem SMS sowie den Krankenkassen und der Landesärztekammer mitgeteilt. Grundsätzlicher Widerspruch ist nicht geäußert worden. Allerdings fehlt es auch noch an Vorschlägen, wie der von der Krankenkasse erlaubterweise zu erhebende Teil des (Datensatzes des) Notarztprotokolls genau zu bestimmen ist. Auch scheint sich die AOK Sachsen noch nicht bereitgefunden zu haben, ein wirklich sicheres Verfahren für die Übermittlunng dieses Teil-Datensatzes einzuführen. Für die hier in Frage stehenden (ärztlich erhobenen) Daten reicht ein Schwärzen von Hand oder die Verwendung einer selbstgestrickten Kopier-Schablone nicht aus. In Betracht kommt nur ein (definierter) Vordruck, etwa auch in Gestalt eines Teildurchschreibsatzes.

10.2.2 Verarbeitung von Sozialdaten durch Private zu Marktforschungszwecken der AOK

Die AOK Sachsen hatte vor, ein privatrechtlich organisiertes Unternehmen damit zu beauftragen, ehemals bei ihr Versicherte zu befragen, welche guten oder auch schlechten Erfahrungen sie mit der AOK Sachsen gemacht und welche Gründe sie zu einem Krankenkassenwechsel bewogen hätten. Um die Befragung durchführen zu können, benötigte das Unternehmen die Adresse der ehemals Versicherten sowie das Datum des Endes der Mitgliedschaft. Diese Daten wollte die AOK Sachsen dem Unternehmen übermitteln.
Ich habe dazu gegenüber der AOK und dem SMS folgende Rechtsauffassung vertreten:

(1) Die Anschriften der ehemals Versicherten sowie die Tatsache und der Zeitpunkt der Beendigung der Mitgliedschaft sind Sozialdaten, auch wenn der Betroffene nicht mehr Mitglied der AOK Sachsen ist. Die Definition des Begriffes Sozialdatum in § 67 Abs. 1 Satz 1 SGB X stellt darauf ab, dass die Angaben über den Betroffenen von einer in § 35 SGB I genannten Stelle im Hinblick auf ihre Aufgaben nach dem Sozialgesetzbuch erhoben, verarbeitet oder genutzt werden. Da die AOK Sachsen diese Daten erhoben hatte, speicherte und übermitteln bzw. nutzen wollte, handelte es sich um Sozialdaten.

Die Verarbeitung personenbezogener Daten durch eine öffentliche Stelle greift in das Grundrecht auf informationelle Selbstbestimmung ein. Dieser Eingriff ist nur zulässig, wenn eine Rechtsvorschrift dies erlaubt oder der Betroffene eingewilligt hat.
Die in Betracht kommenden Erlaubnisnormen unterscheiden hinsichtlich der Zulässigkeitsvoraussetzungen zwischen verschiedenen Datenverarbeitungschritten. Bei der hier geplanten Weitergabe der Daten an den privaten Unternehmer würde es sich um eine Übermittlung von Daten durch die AOK handeln, nicht lediglich um eine Nutzung durch die AOK.
Übermitteln ist in § 67 Abs. 6 Nr. 3 SGB X definiert als das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener Sozialdaten an einen Dritten (Empfänger). Wer Dritter ist, bestimmt § 67 Abs. 10 SGB X. Das ist jede Person oder

Stelle außerhalb der speichernden Stelle. Dritte sind nicht der Betroffene sowie diejenigen Personen und Stellen, die im Geltungsbereich des Sozialgesetzbuches Sozialdaten im Auftrag verarbeiten oder nutzen; für diese Datenverarbeitung im Auftrag gemäß § 80 SGB X gelten Sondervorschriften. Eine Datenverarbeitung im Auftrag kam hier jedoch nicht in Frage, weil diese voraussetzt, dass der Unternehmer Sozialdaten in vollständiger Abhängigkeit von den Vorgaben des Auftraggebers, die Art und den Umfang der Datenverarbeitung betreffend, verarbeitet. Den Darlegungen der AOK war ein solches Auftragsverhältnis nicht zu entnehmen. Die Daten sollten hier also an eine (juristische) Person außerhalb der speichernden Stelle weitergegeben werden, d. h. an einen Dritten. Die Daten sollten also übermittelt werden.
(Anders möglicherweise Schroeder-Printzen Rdnr. 4 zu § 75 SGB X: bloße Nutzung; wie hier der LfD Baden-Württemberg in seiner nachstehend zitierten Stellungnahme.)

(2) Die einzig in Betracht kommende Rechtsgrundlage war § 284 Abs. 3, 2. Halbsatz SGB V i. V. m. §§ 67 d Abs. 1 i. V. m. 75 Abs. 1 Nr. 2 SGB X.
Ob das Betreiben von Marktforschung, das Zweck der Übermittlung sein sollte, ein Planungsvorhaben im Sozialleistungsbereich i. S. d. § 75 Abs. 1 Nr. 2 SGB X ist, kann dann dahingestellt bleiben, wenn nach § 75 Abs. 1 Nr. 2 eine Übermittlung zu Planungszwecken nur erlaubt ist, wenn diese Übermittlung an eine öffentliche Stelle erfolgt. (Hier war ja demgegenüber die Übermittlung an ein privatrechtliches Unternehmen geplant.) Diese Voraussetzung macht eine in der Literatur wohl vorherrschende Meinung: Hauck/Haines Rdnr. 18 und Scholz, in: Kasseler Kommentar, Rdnr. 14, jeweils zu § 75 SGB X und jeweils ohne Begründung; übereinstimmend vermutlich auch der Rentenversicherungsträger-Kommentar, 6. Aufl. 1998, Anmerkung 5 (anders Anmerkung 9!) zu § 75 SGB X.
Diese Auffassung setzt voraus, dass die - für Übermittlungen an nicht-öffentliche Stellen Regelungen treffenden - Absätze 3 und 4 der Vorschrift sich nur auf § 75 Abs. 1 Satz 1 Nr. 1, also den Verarbeitungszweck Forschung, nicht aber auch auf Nr. 2, eben die Planung als Verarbeitungszweck, beziehen. Dafür gibt der Wortlaut der Vorschrift jedoch nichts her, und in den Kommentierungen des Rentenversicherungsträger-Kommentars (a.a.O. Anmerkung 9) und durch Schroeder-Printzen (a.a.O. Rdnrn. 12 f.) wird dergleichen auch nicht behauptet.
Zu folgen ist aufgrund des Wortlautes der bemerkenswerterweise schon zu § 75 a.F. SGB X deutlich von Walz im GK-SGB X 2 (Rdnr. 39) dargelegten Gegenmeinung: *Plant eine SGB-Stelle, kann die das Planungsprojekt durchführende Institution auch ein privates Institut sein.*

Demnach fragt es sich, ob die beabsichtigte Maßnahme als „Planung“ im Sinne des Gesetzes aufgefasst werden kann. Um klassische Planung im Sinne von Bedarfs- oder Finanzplanung handelte es sich sicher nicht. Aber von der *Festlegung künftigen Verhaltens auf der Grundlage der Abschätzung künftiger Tatsachen, die anhand gegenwärtiger oder vergangener Tatsachen abgeschätzt werden*, wie der Begriff bei Hauck/Haines Rdnr. 18 zu § 75 SGB X umschrieben wird, und auch von der *Erfassung und Auswertung aller auf die Erreichung eines gewollten Ergebnisses einwirkenden Faktoren*, wie man in Anlehnung an den Rentenversicherungsträger-Kommentar (Anmerkung 1 a.a.O.) formulieren könnte, war die beabsichtigte Maßnahme kaum entfernt:

Anders als bei klassischer Planung ging es weniger um Anpassung an künftige objektive Veränderungen der Handlungsbedingungen als um Überprüfung der eigenen Qualität, d. h. um Fehlersuche zwecks Verbesserung der Handlungsweise und damit eine Verhaltensänderung der Organisation, welche dieser helfen würde, in der Zukunft ihre Aufgaben ausreichend erfüllen zu können, wozu ja auch die Sicherung der eigenen Existenz im Verhältnis zu Mitbewerbern (vgl. §§ 173 bis 175 SGB V) gehört.
Die Einführung von Wettbewerbselementen in die gesetzliche Krankenversicherung erweitert den notwendigen Handlungszweck der Anpassung der Krankenkassen an objektive Gegebenheiten um die Anpassung an subjektive Bedürfnisse der Versicherten, die sich in deren (im Sinne statistischer Vorhersagen) zu erwartendem Wahlverhalten niederschlagen. Die in § 75 Abs. 1 Satz 1 Nr. 2 SGB X ausgesprochene Anerkennung eines Annex-Zweckes umfasst daher meines Erachtens auch die Überprüfung der eigenen Leistungen einer gesetzlichen Krankenversicherung anhand einer Befragung ausgeschiedener Mitglieder, die zu anderen Krankenversicherungen gewechselt sind: Eine *Prognose, die unter Berücksichtigung der Bedarfslage und der Zielvorstellungen als Orientierung für das zukünftige Verwaltungshandeln dienen soll*, wie der Kasseler Kommentar (Rdnrn. 16 zu § 67 c SGB X und 12 zu § 75 SGB X) in Anlehnung an das Bundesverwaltungsgericht formuliert, sollte ja auch hier erarbeitet werden.

Im praktischen Ergebnis besteht daher Übereinstimmung mit der Stellungnahme des baden-württembergischen Landesdatenschutzbeauftragten, der in seinem 20. Tätigkeitsbericht (1999, LT-DS 12/4600, unter 1.5.1) eine als rechtlich gleich anzusehende Aktion zwar für rechtswidrig hält, sie jedoch, wenn die Maßnahme im übrigen datenschutzgerecht abgewickelt wird, im Sinne einer Duldung hinnimmt.

(3) Die beabsichtigte Übermittlung an das Unternehmen war gemäß § 75 Abs. 1 Satz 2 SGB X jedoch erst zulässig, wenn die AOK vorher die Einwilligung der Betroffenen, also der ehemaligen Mitglieder, ggf. auch der mitversicherten Familienmitglieder, in die Übermittlung an das Unternehmen sowie in die Speicherung und Nutzung durch das Unternehmen (vgl. Walz a.a.O. Rdnr. 59) eingeholt haben würde. Es musste eine schriftliche Einwilligung eingeholt werden, und den Betreffenden musste der Zweck der Aktion, nämlich die Erforschung der Gründe für das Verlassen der AOK, erläutert werden.

Zwar kann dann, wenn lediglich Namen und Anschriften einer Vielzahl von Personen weitergegeben wird, wegen Unverhältnismäßigkeit des Verwaltungs- bzw. Kostenaufwandes die Einholung der Einwilligung im Sinne des § 75 Abs. 1 Satz 2 SGB X unzumutbar sein (Walz a.a.O. Rdnr. 61). Jedoch ist der Auffassung zuzustimmen, dass in all denjenigen Fällen, in denen die Betroffenen an der Untersuchung - wie im vorliegenden Falle - mitwirken sollen, es auch zumutbar ist, sie vorher um ihr Einverständnis in die Übermittlung der Daten an die untersuchende Stelle zu bitten (Walz a.a.O. Rdnr. 65 m.w.N.).

Die Prüfung, inwieweit schutzwürdige Interessen des Betroffenen beeinträchtigt sein könnten (§ 75 Abs. 1 Satz 1 SGB X), entfällt im Falle der Einwilligung (Walz a.a.O. Rdnrn. 20, 70).

(4) Zwei weitere Voraussetzungen waren jedoch zu beachten:
Zum einen würde die Verwendung der Daten über Namen, Anschriften und den Umstand der Beendigung der Mitgliedschaft in der AOK zum Zweck der Einholung der Einwilligung eine Nutzung der bei der AOK noch gespeicherten Daten darstellen. Eine solche Nutzung bedarf gemäß § 284 Abs. 3 SGB V ebenfalls einer Rechtsgrundlage. Diese Rechtsgrundlage ist § 67 c Abs. 2 Nr. 3 SGB X, wobei allerdings vorausgesetzt ist, dass auch hier, wie in § 75 Abs. 1 Satz 1 Nr. 2 SGB X, der Begriff „Planung" so weit verstanden wird, dass er auch die Marktforschung umfasst, wie oben dargestellt.

Außerdem würde die Übermittlung gemäß § 75 Abs. 2 Satz 1 SGB X der vorherigen Genehmigung durch die zuständige oberste Aufsichtsbehörde bedürfen, im Falle der AOK Sachsen also des SMS.
Das Genehmigungserfordernis gilt auch im Falle der erteilten Einwilligung. Dies folgt aus der Systematik der Vorschrift, die in Absatz 2 Satz 1 keine Beschränkung auf bestimmte Fallgestaltungen des Absatzes 1 erkennen lässt. Zweck der Regelung ist, dass die Genehmigungsbehörde gerade auch die Ordnungsmäßigkeit der Einwilligungserklärungen überprüfen soll (Walz a.a.O. Rdnrn. 69 und 93; übereinstimmend Scholz, in: Kasseler Kommentar Rdnr. 28 zu § 75; anderer Ansicht, ohne Begründung, Rentenversicherungsträger-Kommentar Anmerkung 8 zu § 75 unter Berufung auf ein Schreiben des BMA).

Das lange Schweigen von AOK und SMS darf als Zustimmung gewertet werden. Auch im Kreis meiner Kollegen in Bund und Ländern ist kein Widerspruch laut geworden.

10.2.3 Auskunftsersuchen der Krankenkasse an Krankenhäuser bei Anhaltspunkten für die Verantwortung dritter Schadensverursacher

Zieht eine gesetzliche Krankenkasse aus den ihr nach den §§ 294 ff. SGB V von Ärzten und Krankenhäusern übermittelten Sozialdaten den Schluss, dass Ursache der Notwendigkeit der Erbringung von Leistungen an einen Versicherten ein Schadensereignis sei, aufgrund dessen dieser einen Schadensersatzanspruch gegen einen Dritten als Verursacher des Schadensereignisses (gehabt) haben und dass diese Forderung gemäß § 116 Abs. 1 Satz 1 SGB X auf die Krankenkasse übergegangen sein könnte, so schickt sie dem Versicherten einen sog. Unfallfragebogen. In diesem fragt sie den Versicherten nach den Gründen einer stationären Aufnahme im Krankenhaus, im Formular der AOK Sachsen differenziert nach Verkehrsunfall, Schlägerei, häuslichem Unfall, Arbeitsunfall und mit einem zusätzlichen Freitextfeld. Außerdem wurde nach einer möglichen Drittbeteiligung gefragt; als Rechtsgrundlage dieser Datenerhebung hat die AOK Sachsen in diesem Fragebogen § 100 Abs. 1 SGB X angegeben.
Hatte der Betroffene den Fragebogen nicht ausgefüllt, wurde er von der AOK Sachsen unter Hinweis auf Mitwirkungspflichten gemäß den §§ 60 ff. SGB I nochmals dazu aufgefordert. Danach ersuchte die AOK das Krankenhaus um die entsprechende Auskunft. (Diese AOK-Praxis war nicht auf Sachsen beschränkt.)
Die AOK Sachsen hat diese Datenerhebung beim Krankenhaus mir gegenüber zunächst auf § 100 Abs. 1 SGB X gestützt, später dann auf § 301 Abs. 1 Satz 1 Nr. 3

SGB V i. V. m. Anlage 2 der Datenübermittlungs-Vereinbarung zwischen den Spitzenverbänden der Krankenkassen und der Deutschen Krankenhausgesellschaft. (Andere von mir befragte in Sachsen tätige gesetzliche Krankenkassen hingegen haben mir versichert, sie verzichteten auf eine solche Datenerhebung.)

Ich habe der AOK dargelegt, dass es derzeit keine Rechtsvorschrift gebe, die diese Datenerhebung zu diesem Zweck erlaubte, insbesondere seien weder § 100 Abs. 1 SGB X noch § 301 Abs. 1 Satz 1 Nr. 3 SGB V einschlägig:

(1) *§ 100 Abs. 1 SGB X* begründet eine Auskunftspflicht des Arztes oder Angehörigen eines anderen Heilberufes. Diese besteht aber nach dem klaren Gesetzeswortlaut nur unter bestimmten Voraussetzungen, nämlich nur dann, wenn die Auskunftserteilung gesetzlich zugelassen ist oder der Betroffene im Einzelfall eingewilligt hat. § 100 Abs. 1 SGB X kann für sich allein niemals Rechtsgrundlage einer Datenverarbeitung sein.
Wenn eine Einwilligung des Betroffenen nicht vorliegt, was wohl immer dann der Fall sein dürfte, wenn der Betroffene den Unfallfragebogen nicht ausfüllt, ist eine Datenerhebung beim Krankenhaus nur dann zulässig, wenn eine gesetzliche Vorschrift die Übermittlung von Daten durch das Krankenhaus an die Krankenkasse zulässt. Die einzige in Betracht kommende Rechtsgrundlage ist § 301 SGB V.

(2) Nach *§ 301 Abs. 1 Satz 1 Nr. 3 SGB V* sind die Krankenhäuser verpflichtet, den Krankenkassen u. a. den Grund der Aufnahme, die Einweisungs- und Aufnahmediagnose sowie die voraussichtliche Dauer der Krankenhausbehandlung mitzuteilen.
Das Merkmal „Aufnahmegrund“ wird durch die Anlage 2 der Datenübermittlungs-Vereinbarung dahingehend konkretisiert, dass das Krankenhaus den Aufnahmegrund differenziert nach Normalfall, Arbeits-, Wegeunfall oder Berufskrankheit, Verkehrs-, Sport- oder sonstiger Unfall, Hinweis auf Einwirkung von äußerer Gewalt, Kriegsbeschädigten- oder BVG-Leiden sowie nach Notfall anzugeben hat.
Diese Konkretisierung in der Datenübermittlungs-Vereinbarung hält sich nicht an die gesetzlichen Vorgaben und ist somit unbeachtlich. Zwar darf gemäß § 301 Abs. 3 SGB V das Nähere über Form und Inhalt der erforderlichen Vordrucke sowie das Verfahren der Abrechnung auf maschinell verwertbaren Datenträgern zwischen den Spitzenverbänden der Krankenkassen und der Deutschen Krankenhausgesellschaft vereinbart werden. Konkretisiert werden darf in der Vereinbarung aber nur das, was das Gesetz als Rahmen vorgibt. Das ist aus verfassungsrechtlichen Gründen auch nicht anders möglich, denn eine solche Vereinbarung kann niemals für sich alleine Rechtsgrundlage einer Datenverarbeitung durch öffentliche Stellen sein.
Für die hier in Frage stehenden Daten bestimmt § 301 Abs. 1 Satz 1 Nr. 3 SGB V den Rahmen. Mitzuteilen durch die Krankenhäuser ist danach der Grund der Aufnahme. Gemeint ist der Grund der Aufnahme gerade in ein Krankenhaus, nicht hingegen, dass Daten erfasst werden sollen, die die Ermittlung und Verfolgung von Erstattungsansprüchen der Krankenkasse gegen Dritte zulassen. Dies ergibt sich aus dem Zweck der Vorschrift. Die Datenübermittlung soll nämlich eine ordnungsgemäße Abrechnung mit den Krankenhäusern gewährleisten und die für die Erfüllung der gesetzlichen Aufgaben der Krankenkassen, u. a. die Überprüfung der Notwendigkeit der Krankenhausbehandlung (§ 112 Abs. 2 Satz 1 Nr. 2 SGB V) und die Wirtschaft-

lichkeitsprüfungen der Krankenhäuser (§ 113 SGB V), erforderlichen Daten zur Verfügung zu stellen (Begründung zu § 301 SGB V, BT-Drs. 12/3608 S. 104, 125).

Abgestellt wird in der Begründung zum einen also auf die Beziehung Krankenkasse - Krankenhaus, nicht auf Beziehungen der Krankenkasse zu weiteren Leistungsträgern oder sonstigen Dritten.
Zum anderen gehört es zwar zu den gesetzlichen Aufgaben der Krankenkasse, eigene mögliche Erstattungsansprüche gegen andere Leistungsträger oder Dritte zu verfolgen. Aus diesem Grund verpflichtet § 301 Abs. 1 Satz 1 SGB V aber nicht gerade das Krankenhaus, die hierfür notwendigen Daten zu übermitteln. Es wäre ein Zufall, wenn das Krankenhaus dazu verbindliche Informationen hätte. Für Aufnahme, Behandlung und Abrechnung von Seiten des Krankenhauses, also für den Betrieb des Krankenhauses insgesamt, ist es nämlich gleichgültig, ob der Patient nun wegen eines Wege-, Arbeits-, Sport- oder sonstigen Unfalls eingeliefert wurde. Das kann und will der Krankenhausarzt gar nicht wissen oder beurteilen. § 33 Abs. 2 SächsKHG, der dem Krankenhaus die Erhebung von Patientendaten erlaubt, erwähnt deshalb solche Arten von Daten nicht. Solche „Aufnahmegründe“ sind dem Krankenhaus nicht nur gleichgültig, sie müssen ihm sogar gleichgültig sein.

Untermauert wird diese Auslegung durch den Gesetzentwurf zur Reform der gesetzlichen Krankenversicherung ab dem Jahr 2000 (BT-Drs. 14/1245).
Dieser hat die Einfügung eines § 294 a SGB V vorgesehen, nach dem die Krankenhäuser verpflichtet sein sollten, bei Vorliegen von Anhaltspunkten dafür, dass eine Krankheit u. a. eine Berufskrankheit im Sinne der Unfallversicherung ist oder die Folge eines Unfalls oder einer Körperverletzung, oder bei Vorliegen von Hinweisen auf drittverursachte Gesundheitsschäden, die erforderlichen Daten, einschließlich der Angaben über Ursachen und den möglichen Verursacher den Krankenkassen mitzuteilen.
Die Begründung zum Gesetzentwurf führt hierzu aus:
„Die Befugnis zur Mitteilung von Anhaltspunkten über die Zuständigkeit eines anderen Kostenträgers ist bisher nur im Bundesmantelvertrag (§ 58) geregelt. Da es sich um die Übermittlung personenbezogener Daten handelt, bedarf diese Verpflichtung einer gesetzlichen Grundlage. Eine vertragliche Vereinbarung reicht nicht aus. Die Verpflichtung betrifft Vertragsärzte, ärztlich geleitete Einrichtungen und die nach § 108 zugelassenen Krankenhäuser. Auch über drittverursachte Gesundheitsschäden ist eine Mitteilungspflicht erforderlich. Um Schadensersatzansprüche nach § 116 SGB X geltend machen zu können, benötigen die Krankenkassen alle Leistungsdaten, die für drittverursachte Gesundheitsschäden entstanden sind. Die Kassenärztliche Vereinigung hat daher auch diese Angaben versichertenbezogen den Krankenkassen zu übermitteln.“
Daraus, dass die Schaffung eines solchen § 294 a SGB V für notwendig erachtet wird, lässt sich schließen, dass der bereits existierende § 301 Abs. 1 Satz 1 Nr. 3 SGB V die Übermittlung solcher Daten gerade nicht erfasst.

(3) Das SMS hat die Zulässigkeit der Erhebung beim Krankenhaus mit einer seiner Meinung nach zugunsten der Krankenhäuser bestehenden Übermittlungsbefugnis gemäß § 33 Abs. 3 Satz 1 Nr. 6 SächsKHG begründen wollen (zweifelhaft, weil nicht die Leistungspflicht, sondern nur die Regressmöglichkeit der Krankenkasse der Klä-

rung bedarf). Das war, wie ich dem SMS im Einzelnen auseinandergesetzt habe, nicht überzeugend. Denn eine solche Übermittlungsbefugnis, wenn es sie insoweit denn geben sollte, führt noch nicht zur Erlaubtheit der Datenerhebung. Denn als Datenerhebung bei einem Dritten, der nicht Sozialleistungsträger ist, wäre diese Datenerhebung nur unter den Voraussetzungen des § 67 a Abs. 2 Satz 2 Nr. 2 SGB X zulässig.
Buchstabe b der Vorschrift kommt nicht in Betracht, und zwar meines Erachtens auch nicht in der Variante (bb) des unverhältnismäßigen Aufwandes der Erhebung beim Betroffenen. Das Gebrauchmachen von der Möglichkeit der Krankenkasse, über § 307 Abs. 1 Nr. 2 i. V. m. § 206 Abs. 1 Satz 1 SGB V mittels eines Bußgeldes Druck auf den Versicherten zwecks Erzwingung der Erfüllung der Auskunftspflicht auszuüben, stellt meines Erachtens keinen „unverhältnismäßigen Aufwand" dar, vielmehr ist es das gesetzliche Verfahren.
Auch § 67 a Abs. 2 Satz 2 Nr. 2 *Buchst. a, 1. Fall SGB X* hilft nicht weiter. Nach dieser Vorschrift ist eine Erhebung bei den Krankenhäusern zulässig, wenn eine Rechtsvorschrift die Erhebung bei ihnen zulässt. Als eine Rechtsvorschrift käme § 284 Abs. 1 Nr. 4 SGB V in Betracht (man kann die Geltendmachung von Regressansprüchen nach § 116 SGB X mit Hauck/Noftz Rdnr. 9 zu § 284 als *Annex der Leistungsgewährung* ansehen, wenn die Leistungspflicht durch eine zu Schadensersatz verpflichtende Handlung eines Dritten verursacht worden ist). Allerdings wird durch die Worte „bei ihnen" in § 67 a Abs. 2 Satz 2 Nr. 2 Buchst. a SGB X deutlich gemacht, dass in der vorausgesetzten Rechtsvorschrift sowohl die erhebende Stelle als auch die Stelle, bei der die Daten erhoben werden, genannt werden müssen. Dies ergibt sich bereits aus dem Wortlaut und ist in der Begründung des Gesetzentwurfes der Bundesregierung zu § 67 a SGB X ausgeführt (BT-Drs. 12/5187 S. 36/37). § 284 Abs. 1 SGB V erlaubt der Krankenkasse zwar die Datenerhebung, sagt aber nichts darüber, bei wem die Daten erhoben werden dürfen. Damit bleibt es beim Grundsatz der Datenerhebung beim Betroffenen, wie er in § 67 a Abs. 2 Satz 1 SGB X festgeschrieben ist.
Auch die *2. Variante* des § 67 a Abs. 2 Satz 2 Nr. 2 *Buchst. a* SGB X ist nicht einschlägig. Danach darf die Krankenkasse bei den Krankenhäusern personenbezogene Daten erheben, wenn eine Rechtsvorschrift die Übermittlung an die Krankenkasse ausdrücklich vorschreibt. Dass § 301 Abs. 1 Satz 1 Nr. 3 SGB V als solche Vorschrift nicht in Frage kommt, ist vorstehend unter 2 dargelegt. § 33 Abs. 3 Satz 1 Nr. 6 SächsKHG aber kommt ebenfalls nicht als eine Rechtsvorschrift im Sinne des § 67 a Abs. 2 Satz 2 Nr. 2 Buchst. a, 2. Fall SGB X in Betracht. Denn die genannte Voraussetzung, dass die Rechtsvorschrift, welche die Übermittlung vorschreibt, die erhebende Stelle ausdrücklich nennt, ist nicht erfüllt; § 33 Abs. 3 SächsKHG nennt eben nicht die Krankenkasse ausdrücklich als diejenige Stelle, an die die Daten übermittelt werden. Dass es sich der Vorschrift nach um die Übermittlung an Stellen außerhalb des Krankenhauses handeln muss, reicht nicht aus, erforderlich ist eine konkrete Benennung. Außerdem stellten sich möglicherweise Fragen der Gesetzgebungszuständigkeit, nämlich die Frage, inwieweit der sächsische Krankenhausgesetzgeber in die Zuständigkeit des Bundesgesetzgebers, von der dieser Gebrauch gemacht hat, eingriffe.

Das SMS hat dagegen keine Einwände erhoben. Vielleicht deswegen, weil in der Zwischenzeit die AOK Sachsen mir - allerdings erst, nachdem ich mit einer öffentli-

chen Beanstandung gedroht hatte - zugesagt hatte, diese Daten zu diesem Zweck in Zukunft nicht mehr zu erheben, bis der Gesetzgeber eine gesetzliche Grundlage (wohl § 294 a SGB V) geschaffen hat.
Der Datenwunsch, um den es hier gegangen ist, wird von den Datenschutzbeauftragten als legitim angesehen - aber die Datenerhebung wäre eben nicht legal, bis zur Schaffung der erwähnten gesetzlichen Grundlage. Unserer Verfassungsrecht, d. h. die Bindung an die Grundrechte und der Grundsatz der Vorbehalts des Gesetzes, lässt kein anderes Ergebnis zu.

10.2.4 Verarbeitung von Sozialdaten für die Zwecke einer Untersuchung des Bedarfs an Krankenhäusern, mit welcher die AOK Sachsen einen externen Gutachter beauftragt hat (Beanstandung)

Die AOKen der neuen Bundesländer haben eine GmbH (mit Sitz in Schleswig-Holstein) beauftragt, das Angebot und den Bedarf an Krankenhausbehandlungen zu untersuchen. Die AOK Sachsen hat hierzu dem Auftragnehmer personenbezogene Daten der Versicherten, nämlich die ihr nach § 301 SGB V von den Krankenhäusern übermittelten Daten, zum Teil verschlüsselt, aber in immer noch personenbeziehbarer Form, an die GmbH übermittelt.
Ich erfuhr davon erst nachträglich durch Kollegen, die von ihren Ministerien, freilich auch erst im Nachhinein, unterrichtet worden waren.

Sowohl die Nutzung als auch die Übermittlung der Daten war mangels Rechtsgrundlage rechtswidrig. Diese Vorgehensweise der AOK Sachsen habe ich förmlich gemäß § 26 SächsDSG beanstandet.

(1) Die AOK Sachsen hat die ihr nach § 301 SGB V von den Krankenhäusern übermittelten personenbezogenen Daten der Versicherten (und mittelbar auch von Ärzten) genutzt, indem sie unmittelbar identifizierende Angaben wie Namen, Geburtsdatum und Anschrift (in einer für den Auftragnehmer nicht verstehbaren Weise) verschlüsselt und für die Datenübermittlung technisch aufbereitet hat. Zweck dieser Nutzung war, die Daten so zu bearbeiten, dass sie der GmbH zum Zweck der Vertragserfüllung zur Verfügung gestellt werden konnten.

Diese Datennutzung wäre nur zulässig gewesen, wenn eine Rechtsvorschrift sie erlaubt hätte. Dies war jedoch nicht der Fall.

Nach § 284 Abs. 3 SGB V darf eine gesetzliche Krankenkasse rechtmäßig erhobene Daten nur für die Zwecke der in Absatz 1 der Vorschrift genannten Aufgaben nutzen, für andere Zwecke nur, soweit dies durch Rechtsvorschriften *des SGB* erlaubt ist.

Die AOK hat die Daten zur Erfüllung des Vertrages genutzt, dessen Zweck die Bereitstellung eines umfangreichen Zahlenwerkes als Grundlage von Überlegungen zur Krankenhausplanung war. Das fiel nicht unter die in § 284 Abs. 1 SGB V genannten Aufgaben.

Als andere Rechtsvorschrift des SGB wäre höchstens § 67 c Abs. 2 Nr. 3, *2. Fall* SGB X in Betracht gekommen, die Datennutzung für Zwecke der *Planung* im Sozialbe-

reich, und zwar, wegen der Verweisung auf § 75 Abs. 1 Satz 1 Nr. 2 SGB X, durch eine öffentliche Stelle im Rahmen ihrer Aufgaben.

Die Mitwirkung der einzelnen gesetzlichen Krankenkassen mit vier von vierzehn Beisitzern im gemäß § 5 Abs. 1 SächsKHG i. V. m. § 7 Abs. 1 KHG gebildeten Sächsischen Krankenhausplanungsausschuss bei der Krankenhausplanung gemäß § 5 Abs. 3 Satz 1 SächsKHG begründet noch keine eigene Aufgabe im Sinne von § 75 Abs. 1 Satz 1 Nr. 2 SGB X. Die Krankenhausplanung ist keine Aufgabe der AOK oder anderer im Freistaat Sachsen tätiger gesetzlicher Krankenversicherungen, sondern gemäß § 1 i. V. m. § 6 Abs. 1 und Abs. 4 KHG i. V. m. § 3 SächsKHG eine Aufgabe des zuständigen Ministeriums, d. h. des SMS. Mit dieser Feststellung wird keineswegs der AOK, wie sie mir gegenüber gemeint hat, „die Beteiligung der gesetzlichen Krankenkassen an der sächsischen Krankenhausplanung“ bestritten oder dieser Beteiligung dem Gesetz zuwider ein bloßer „dekorativer Charakter“ zugebilligt. Denn mit „Aufgabe“ ist in § 75 Abs. 1 Nr. 2 der Bereich der Kompetenzen, der Zuständigkeiten gemeint, und keine bloßen Beteiligungsrechte als eines unter vielen. Solche rechtfertigen nicht die Verarbeitung personenbezogener Daten im großen Stil wie hier, wo aus den Daten der AOK ein Werk von 350 Seiten mit Tabellen und Übersichten mitsamt Erläuterungen geworden ist.

Um ein bestimmtes Vorhaben der wissenschaftlichen Forschung im Sinne von § 67 c Abs. 2 Nr. 3, *1. Fall* SGB X - wie die AOK mir gegenüber dann geltend gemacht hat -, hat es sich ebenfalls nicht gehandelt; die Anwendung bereits anderweitig erarbeiteter wissenschaftlicher Ergebnisse bei Anfertigung der „Bedarfsanalyse“ hat diese nicht zu einem Forschungsvorhaben gemacht.

Hinzu kommt: Es war nicht ersichtlich, dass die AOK auf die weiteren Voraussetzungen einer Datennutzung, die gemäß § 75 Abs. 1 Satz 1 SGB X in beiden Fällen des § 67 c Abs. 2 Nr. 3 SGB X zu beachten sind, einen Gedanken verschwendet gehabt hätte. Schon solche Leichtfertigkeit ist ein *Mangel bei der Verarbeitung personenbezogener Daten* im Sinne des § 26 SächsDSG.

(2) Daneben war auch die Übermittlung der Daten rechtswidrig.
Trotz der bereits erwähnten Verschlüsselung unmittelbar identifizierender Angaben, wie Name, Geburtsdatum und Anschrift, waren die Daten personenbezogen. So ließ sich z. B. über das Geburtsjahr, die ersten vier Stellen der Postleitzahl des Wohnortes des Patienten, die Fachabteilung des Krankenhauses, in das der Patient eingeliefert worden war, Aufnahme- und Entlassungsdatum, Abrechnungsdatum, Operations- bzw. Entbindungsdatum ohne unverhältnismäßigen Aufwand an Zeit und Arbeitskraft der Betroffene bestimmen.

Darin habe ich - wie meine drei anderen betroffenen Kollegen (Sachsen-Anhalt war aus dem Vertrag ausgestiegen, also nicht mehr beteiligt gewesen) - keine hinreichende Anonymisierung im Sinne von § 67 Abs. 8 SGB X gesehen; eine stärkere Anonymisierung wäre - meiner Einschätzung nach ohne Schaden für die Untersuchung - zu erreichen gewesen, wenn man beispielsweise statt des Aufnahme- und Entlassungstages die Aufenthaltsdauer, vielleicht mit Angabe des jeweiligen Wochentages des

Beginnes und des Endes des Aufenthaltes, erfasst hätte, und beim Operationstag hätte vermutlich die Angabe des Monats oder des Quartals sowie die Wochentages ausgereicht; auch hätte man die Diagnosen vielleicht zu größeren Gruppen zusammenfassen können. Hier hat man es sich schlicht zu einfach gemacht.

Die AOK Sachsen hat auch nicht etwa im Hinblick auf § 75 Abs. 2 und 3 SGB X vorher das SMS als Genehmigungsbehörde vorsorglich gefragt, ob es eine Genehmigung mangels Personenbezuges für unnötig halte. Die AOK hat es insoweit darauf ankommen lassen, während andere beteiligte AOKen einen Genehmigungsantrag nach § 75 SGB X gestellt haben. Immerhin hatte die AOK Sachsen selbst mit dem Auftragnehmer nach sieben Monaten vorsorglich einen „Ergänzungsvertrag zur Gewährleistung des Datenschutzes“ abgeschlossen, war demnach also selbst von einem Personenbezug der von ihr gelieferten Daten ausgegangen.

Die Weitergabe der Daten durch die AOK an die GmbH war eine Weitergabe an Dritte und damit ein Übermitteln (§ 67 Abs. 6 Nr. 3 i. V. m. Abs. 10 SGB X). Denn die GmbH hatte die Daten nicht lediglich im Auftrag der AOK zu verarbeiten, sondern mittels ihrer eigenständig die ‘Bedarfsanalyse’ zu erarbeiten, insoweit völlig unabhängig von Vorgaben der AOK.

Eine Rechtsvorschrift, die es der AOK erlaubt hätte, die - eben personenbezogenen - Daten an die GmbH zu übermitteln, gab es nicht; überdies hätte eine solche Übermittlungsbefugnis der Einschränkung des § 76 SGB X unterlegen. Nach § 76 Abs. 1 SGB X dürfen Sozialdaten, die eine in § 35 SGB I genannten Stelle von einem Arzt oder einer anderen in § 203 Abs. 1 mitsamt Abs. 3 StGB genannten Person zugänglich gemacht worden sind, nur unter den Voraussetzungen übermittelt werden, unter denen diese Personen selbst übermittlungsbefugt wären. Die AOK hat die Daten von Krankenhäusern gemäß § 301 SGB V erhalten. Die in dieser Vorschrift genannten Daten werden größtenteils von Ärzten beim betroffenen Patienten erhoben. Damit handelt es sich insoweit um besonders schutzwürdige Sozialdaten, deren Übermittlung durch § 76 SGB X zusätzlichen Einschränkungen unterworfen wird. Eine Rechtsvorschrift, die dem Arzt zur Übermittlung von Daten seiner Patienten an einen privaten Dritten zu Planungszwecken erlaubte, gibt es nicht. Von den Ausnahmetatbeständen des § 76 Abs. 2 SGB X war keiner erfüllt; insbesondere handelte es sich seitens der AOK nicht um eine Übermittlung zwecks Erfüllung einer ihr im SGB gesetzlich zugewiesenen Aufgabe (§ 76 Abs. 2 Nr. 1 i V. m. § 69 Abs. 1 Nr. 1, 1. Fall SGB X).

Die AOK hat meinen Rechtsstandpunkt nicht akzeptiert, jedoch erklärt, mittelfristig gedenke sie nicht, eine gleichartige Nutzung und Übermittlung von Daten zu wiederholen. Das SMS hat sich mir gegenüber einfach nicht geäußert.

10.2.5 Nachweis beitragspflichtiger Einnahmen freiwilliger Mitglieder der gesetzlichen Krankenversicherung durch Vorlage des Einkommensteuerbescheides

Die Beiträge freiwilliger Mitglieder der gesetzlichen Krankenversicherung, die hauptberuflich selbständig erwerbstätig sind, richten sich nach der monatlichen Bei-

tragsbemessungsgrenze (§ 223 i. V. m. § 240 Abs. 1 und Abs. 4 Satz 2 SGB V). § 240 Abs. 4 Satz 2 SGB V fingiert als beitragspflichtige Einnahme für den Kalendertag den 30. Teil der sog. monatlichen Beitragsbemessungsgrenze, beim Nachweis niedrigerer Einnahmen mindestens den 40. Teil der sog. monatlichen Bezugsgröße im Sinne von § 18 SGB IV. In diesem Zusammenhang mussten aus Anlass von Eingaben zwei Fragen geklärt werden, die sich aus Folgenden ergaben: Bisher hatte der Nachweis solcher niedrigerer Einnahmen durch eine Bestätigung des Steuerberaters über die Höhe des Einkommens des freiwilligen Mitgliedes geführt werden können. Nunmehr war das Bundesversicherungsamt dazu übergegangen, von den seiner Aufsicht unterstehenden gesetzlichen Krankenversicherungen zu verlangen, dass die Höhe des Einkommens durch Vorlage des Einkommensteuerbescheides nachgewiesen wird. Dem ist die AOK Sachsen gefolgt, was vom Ansatz her auch in Ordnung war:

Aus der Rechtsprechung des Bundessozialgerichts ergibt sich, dass sich die Krankenkassen zur Betragsbemessung freiwillig versicherter Selbständiger die Bescheide der Finanzämter, insbesondere die Einkommensteuerbescheide, vorlegen lassen dürfen (und müssen, BSG Urt. v. 26. September 1996 - 12 RK 46/95; E 79, 133, 139).
Das Gericht stützt (a. a. O. S. 137) seine Auffassung nicht zuletzt auf die amtliche Begründung (Ausschussbericht) der Änderung des § 240 SGB V durch das Gesundheits-Strukturgesetz vom 21. Dezember 1992 (BT-Drs. 12/3973 S. 17).
Der Entscheidung ist jedoch nicht zu entnehmen, dass alle im Steuerbescheid enthaltenen Angaben von der Krankenkasse zur Beitragsbemessung benötigt würden. Das Gericht stellt lediglich fest, dass die bloßen eigenen Angaben des Selbständigen für die nötige objektive Ermittlung des Einkommens nicht ausreichend seien, vielmehr amtliche Unterlagen der Finanzverwaltung herangezogen werden müssten.

(1) Das erste Problem ergibt sich in Hinblick auf den Datensatz. Soweit der Einkommensteuerbescheid mehr als die zur Beitragsbemessung notwendigen Angaben enthält, dürfen diese Angaben in dem Bescheid durch den Betroffenen geschwärzt werden, bevor er an die Krankenkasse übermittelt wird. Denn die Krankenkasse benötigt diese Daten zur Aufgabenerfüllung nicht und sie darf sie daher nicht erheben, d. h. sich willentlich beschaffen.
Dementsprechend hat der BfD bereits in seinem 15. TB (1995), BT-Drs. 13/1150 in Abschnitt 12.6) als auch von den Spitzenverbänden der gesetzlichen Krankenkassen unterstützte datenschutzgerechte Lösung empfohlen, dass sich die Krankenkasse

- entweder eine Ablichtung eines Einkommensteuerbescheides vorlegen lasse, in dem nach vorherigem entsprechendem Hinweis durch die Krankenkasse nur die für die Beitragsberechnung erforderlichen Angaben lesbar bleiben, die übrigen Angaben jedoch geschwärzt werden können,
- oder eine vom Finanzamt bestätigte persönliche Erklärung des Versicherten über das beitragserhebliche Einkommen,
- oder eine vom Finanzamt bestätigte Erklärung des Steuerberaters über dieses Einkommen.

Darüber, wie der im ersten Falle nötige Hinweis gestaltet sein muss, hat noch keine Einigkeit erzielt werden können. Anders als das Bundesversicherungsamt meint, dürfen die Krankenkassen sich nicht auf den Hinweis beschränken, dass sie nicht

sämtliche Daten aus dem Einkommensteuerbescheid erheben dürfen (und wollen). Die Krankenkasse hat in ihrem Hinweis zu verlangen, dass die Daten, die sie nicht benötigt - und diese muss sie näher spezifizieren - weggelassen (geschwärzt) werden. Legt der Betroffene trotz dieses Hinweises der Krankenkasse ungeschwärzte Originalbescheide vor, so handelt die Krankenkassen nicht rechtswidrig, wenn sie Einsicht in die Unterlagen nimmt. Und zwar nicht etwa deshalb, weil eine Einwilligung vorläge oder weil § 296 SGB V eine Rechtsgrundlage böte, sondern deshalb, weil die Krankenkasse diese Daten, die für ihre Aufgabenerfüllung nicht erforderlich sind, sich nicht beschafft, weil sie gegen ihren erklärten Willen durch den Betroffenen an sie herangetragen werden.

Nicht ausreichend hingegen wäre, wenn der Hinweis in dem Sinne formuliert würde, dass der Betroffene, wenn er das Schwärzen trotz des Hinweises unterlässt, implizit seine Einwilligung in die Erhebung der nicht erforderlichen Daten erklären würde.

Ich gehe davon aus, dass mit Unterstützung des Bundesdatenschutzbeauftragten das Bundesversicherungsamt hiervon überzeugt wird, und dass dann andere Aufsichtsbehörden bzw. die nur der Aufsicht durch Landesbehörden unterliegenden Krankenkassen, wie z. B. die AOK Sachsen, dem folgen werden.

(2) Darüber hinaus hat es sich herausgestellt, dass die AOK Sachsen es sich anscheinend zur Regel gemacht hatte, den Einkommensteuerbescheid unmittelbar beim Finanzamt anzufordern, wenn sie Zweifel hinsichtlich der Richtigkeit der Angaben des Versicherten hatte (z. B. Verdacht auf Fälschung der Ablichtung des Einkommensteuerbescheides) und diese Angaben überprüfen wollte. Zumindest in einem Einzelfall hatte sie es einfach deswegen getan, weil der freiwillig Versicherte keinerlei Unterlagen vorgelegt hatte.
Die AOK Sachsen hat als Rechtsgrundlage für diese Erhebung bei Dritten § 21 Abs. 1 i. V. m. Abs. 4 SGB X sowie § 31 Abs. 2 AO genannt. Das SMS will die Datenerhebung auf § 67 a Abs. 2 Satz 2 Nr. 2 Buchst. b aa SGB X stützen.

Beide Rechtsauffassungen überzeugen nicht, und zwar aus folgenden Gründen:

a) § 21 SGB X ist nicht maßgeblich, da nach § 37 Satz 3 SGB I das Zweite Kapitel des Zehnten Buches dessen Erstem Kapitel vorgeht, soweit sich die Ermittlung des Sachverhalts auf Sozialdaten erstreckt. Kurz: Gerade auch der Sozialdatenschutz ist amtshilfefest. Das sollte sich bis zur Leitungsebene der AOK Sachsen herumgesprochen haben.

b) § 31 Abs. 2 AO ist keine ausreichende Rechtsgrundlage für eine Datenerhebung bei Dritten. Zwar sind die Finanzbehörden gemäß § 31 Abs. 2 AO berechtigt, den Trägern der gesetzlichen Sozialversicherung zum Zweck der Festsetzung von Beiträgen die durch das Steuergeheimnis geschützten Verhältnisse mitzuteilen. Die Vorschrift besagt jedoch - was auf den ersten Blick vielleicht verblüffen mag - noch nicht, dass die Krankenkasse bei der Finanzbehörde Daten erheben darf, und wenn ja, welche Daten sie erheben darf. Das folgt aus besonders strengen Regeln des Sozialdatenschutzes:

Diese Datenerhebung ist als Datenerhebung bei Dritten gemäß § 35 Abs. 2 SGB I, § 67 a Abs. 2 SGB X (Verbot mit abschließendem Katalog von Erlaubnistatbeständen als Ausnahmen) nur unter den Voraussetzungen des § 67 a Abs. 2 Satz 2 Nr. 2 SGB X zulässig. Von den dort genannten Tatbeständen kommt lediglich § 67 a Abs. 2 Satz 2 Nr. 2 Buchst. a SGB X in Betracht. Danach ist eine Erhebung bei anderen als den in § 35 SGB I oder § 69 Abs. 2 SGB X genannten Stellen zulässig, wenn eine Rechtsvorschrift die Erhebung bei ihnen zulässt (1. Fall) oder die Übermittlung an die erhebende Stelle ausdrücklich vorschreibt (2. Fall).
Als Vorschrift, die eine Erhebung der in Frage stehenden Daten durch die Krankenkasse zulässt, kommt nur § 284 Abs. 1 Satz 1 Nr. 3 i. V. m. § 240 Abs. 4 Satz 2 SGB V in Betracht. Allerdings wird durch die Worte „bei ihnen“ in § 67 a Abs. 2 Satz 2 Nr. 2 Buchst. a SGB X deutlich gemacht, dass in der Rechtsvorschrift sowohl die erhebende Stelle als auch die Stelle, bei der die Daten erhoben werden, genannt werden müssen. Dies ergibt sich bereits aus dem Wortlaut und ist in der Begründung des Gesetzentwurfes der Bundesregierung zu § 67 a SGB X ausgeführt (BT-Drs. 12/5187 S. 36 und 37). Zulässig wäre eine Datenerhebung durch die Krankenkasse bei der Finanzbehörde also nur, wenn die Rechtsvorschrift das Finanzamt als diejenige Stelle, bei der die Daten erhoben werden, ausdrücklich nennen würde. Gerade dies ist aber nicht der Fall. § 284 Abs. 1 Satz 1 Nr. 3 SGB V erlaubt der Krankenkasse die Datenerhebung, sagt aber nichts darüber aus, bei wem die Daten erhoben werden dürfen. Damit bleibt es beim Grundsatz der Datenerhebung beim Betroffenen, wie er in § 67 a Abs. 2 Satz 1 SGB X festgeschrieben ist.
Eine Vorschrift, welche die Übermittlung durch die Finanzbehörde an die Krankenkasse vorschriebe, gibt es, im Unterschied zu Regelungen zugunsten anderer Sozialversicherungsträger (§ 197 SGB VII - eindeutig Übermittlungs*pflichten* der Finanzämter bzw. Grundsteuerämter), nicht.

Legt also der Betroffene den Einkommensteuerbescheid der Krankenkasse nicht vor, so ist damit der Nachweis niedrigerer Einnahmen nicht erbracht und die Krankenkasse hat bei der Beitragsbemessung die behaupteten, aber nicht nachgewiesenen niedrigeren Einnahmen nicht zugrunde zu legen. Die Nachweise sozusagen auf eigene Faust ohne Mitwirkung des Betroffenen beim Finanzamt zu besorgen ist der Krankenkasse also verwehrt.

c) § 67 a Abs. 2 Satz 2 Nr. 2 Buchst. b aa SGB X lässt eine Erhebung bei Dritten zu, wenn die Aufgaben des Sozialleistungsträgers nach dem Sozialgesetzbuch „ihrer Art nach“ eine Erhebung bei Dritten erforderlichen machen. Die Aufgabe macht eine Erhebung bei Dritten erforderlich, wenn ohne diese Erhebung die Aufgabe nicht zu erfüllen wäre. Das ist z. B. dann der Fall, wenn das Gesetz die Krankenkasse verpflichtet, eine gutachtliche Stellungnahme des Medizinischen Dienstes einzuholen.
Zwar gehört es zu den Aufgaben der Krankenkasse, Angaben des Versicherten zu überprüfen, wenn begründete Zweifel an der Richtigkeit der Angaben bestehen. Die Überprüfung ist aber nicht notwendigerweise mit einer Erhebung bei Dritten verbunden. Eine Überprüfung gefälschter Kopien der Einkommensteuerbescheide

z. B. kann so durchgeführt werden, dass die Behörde sich vom Versicherten eine beglaubigte Kopie besorgen oder amtliche Bescheinigungen sonstiger Art vorlegen lässt.

Ich gehe davon aus, dass die AOK und das SMS sich meiner Rechtsauffassung zu diesem zweiten Problem anschließen werden.

10.2.6 Generelles Verlangen der Sozialhilfebehörde nach Vorlage der Kontoauszüge des letzten halben Jahres zur Bearbeitung des Erstantrages auf Sozialhilfe; Zulässigkeit der Anfertigung von Fotokopien für die Akte der Behörde

Um diese - durch Eingaben aufgeworfenen - Fragen richtig beantworten zu können, muss man sich zunächst Folgendes klarmachen:

- Kontoauszüge haben einen Beweiswert in Bezug auf Zahlungsabgänge (= Sollbuchungen), jedoch nicht in Bezug auf deren Rechtsgrund und deren Wirksamkeit. (Handelt es sich um Luftnummern, also nur um einen scheinbaren Abfluss - weil z. B. die Rückzahlung in bar erfolgt?)
- Kontoauszüge beweisen auch Zuflüsse; sie schließen aber zusätzliche Zuflüsse in bar oder in Naturalien (z. B. Tisch + Bett) nicht aus.
- Deshalb sollten die Sozialhilfebehörden sich wohl auch gelegentlich Auszüge zeigen und erläutern lassen, aber deren Wert nicht hoch einschätzen.
  Wichtiger ist die wirkliche Erforschung der Einkommens-, Belastungs- und Lebensumstände der Antragsteller und ihrer Angehörigen. Das persönliche Gespräch (mit darüber angefertigter kurzer Niederschrift), das gemeinsame Ausfüllen von Fragebögen, das Erheben von Daten an Ort und Stelle („Wo kann ich Sie denn tagsüber oder abends ohne Anmeldung antreffen?“) und das Überprüfen fraglicher Angaben durch Datenerhebung bei Dritten, auch der Einsatz lebenskluger und fachkundiger Kontrolleure - dies sind die wichtigen und erlaubten Methoden einer effizienten Datenerhebung.

Im Ergebnis gilt meines Erachtens folgendes: Das Verlangen des Sozialamtes nach den Kontoauszügen des letzten halben Jahres ist zulässig. Abweichend von anderen dazu vertretenen Meinungen bin ich zu der Auffassung gelangt, dass es keine Regel gibt, wonach die Texte zu Sollbuchungen über kleinere Beträge (etwa unter DM 100) vom Antragsteller vorher geschwärzt werden dürfen. Inwieweit das Schwärzen *der Texte* zu einzelnen Sollbuchungen zulässig ist, hängt von den Umständen des Einzelfalles ab.
Auf die Möglichkeit, Schwärzungen dieser Art vorzunehmen, ist der Antragsteller ausdrücklich hinzuweisen.
Das Kopieren vom Antragsteller vorgelegter Kontoauszüge durch die Behörde ist nur hinsichtlich solcher Buchungen zulässig, die für die Feststellung der Einkommens- und Vermögensverhältnisse des Betroffenen erforderlich sind.
Reicht der Antragsteller die Original-Kontoauszüge ein, besteht demgemäß zum Teil eine Pflicht der Behörde, Schwärzungen in einer Ablichtung vorzunehmen, die sie im Rahmen des Erforderlichen zur Akte nimmt.

Im Einzelnen ergibt sich das aus Folgendem:

1. Die Zulässigkeit der Datenerhebung richtet sich nach § 60 SGB I. Diese Vorschrift ist anwendbar, weil eine Sozialleistung im Sinne des § 11 SGB I beantragt wird (§ 28 SGB I), und gibt eine Befugnis, Daten zu erheben. Das ist bei den Normen, die eine Auskunfts- bzw. Mitteilungspflicht enthalten, der Fall (Hauck/Haines Rdnr. 32 zu § 67 a SGB X). Um eine solche handelt es sich bei § 60 SGB I.

2. Nach dessen Absatz 1 Nr. 3 sind dem Leistungsträger, hier dem Sozialamt, Beweisurkunden vorzulegen. Beweisurkunden sind Urkunden, die entweder selbst den zu beweisenden Umstand enthalten oder ihn verkörpern oder die über einen außerhalb ihrer liegenden Umstand berichten. Die Vorlagepflicht bezieht sich jedoch nur auf solche Beweisurkunden, die leistungs- und entscheidungserhebliche und beweisbedürftige Tatsachen betreffen (Seewald, in: Kasseler Kommentar Rdnr. 30 zu § 60 SGB I). Welche Tatsachen entscheidungserheblich sind, richtet sich nach den auf den Verfahrensgegenstand anzuwendenden Rechtsnormen, d. h. nach den Tatbestandsmerkmalen, die diese Rechtsnormen für die Zulässigkeit und Begründetheit des Begehrens aufstellen. Tatbestandsmerkmale, die nicht bereits festgestellt, nicht offenkundig oder gesetzlich zu vermuten sind oder als wahr unterstellt werden können, sind beweisbedürftig (Hauck/Haines Rdnr. 7 zu § 20 SGB X; ähnlich Seewald a.a.O. Rdnr. 13).
   Vorliegend ist Aufgabe des Sozialamtes die Prüfung des Erstantrages auf Sozialhilfe. Bei dieser Prüfung sind gemäß den §§ 76 ff. BSHG u. a. zu berücksichtigen: Sämtliche Einkünfte abzüglich Steuern, bestimmter Beiträge und mit der Erzielung des Einkommens verbundener notwendiger Ausgaben, Zuwendungen, das Vermögen des Antragstellers sowie Ansprüche gegen Dritte.
   Die Kontoauszüge betreffen zumindest zum Teil für die Prüfung des Sozialhilfeantrages leistungs- und entscheidungserhebliche Tatsachen. Insbesondere können die vollständigen Kontoauszüge das Fehlen z. B. eines Einkommens oder Vermögens plausibel machen.
   Regelmäßig werden für die Bestimmung der Einkommens- und Vermögenssituation des Betroffenen Sollbuchungen auch über kleinere Beträge von Bedeutung sein. Aus diesem Grund dürfen die Texte zu solchen Buchungen nicht geschwärzt werden.

   Der Betroffene ist beim Anfordern der Kontoauszüge gemäß § 67 a Abs. 3 Satz 2 SGB X darauf hinzuweisen, dass die Vorlage der Kontoauszüge Voraussetzung einer positiven Entscheidung über den Antrag ist.

3. Der Zulässigkeit des Verlangens, die Kontoauszüge beizubringen, steht der Untersuchungsgrundsatz (§ 20 SGB X) nicht entgegen, bei dessen Anwendung das Ausmaß der Ermittlungen im am Verfahrensgegenstand auszurichtenden Ermessen der Behörde steht. Dabei gilt das Gebot der Einfachheit und Zweckmäßigkeit des Verfahrens, § 9 Satz 2 SGB X (Hauck/Haines Rdnr. 6 zu § 20 SGB X). Die Kontoauszüge können, wie dargelegt, ein recht aussagekräftiges Bild von der Einkommenslage, zum Teil auch der Vermögenslage, des Antragstellers verschaffen, was für die Prüfung der Voraussetzungen des Antrages auf Sozialhilfe

unerlässlich ist. Auch bringt die Vorlage der Kontoauszüge für den Antragsteller keine unzumutbaren Schwierigkeiten mit sich.

4. Etwas anderes ergibt sich auch nicht dadurch, dass durch die Vorlage der Kontoauszüge auch Daten zu Kontobewegungen erhoben werden, deren Kenntnis für die Behörde nicht erforderlich ist. Die festzustellende Tatsache besteht gerade darin, dass bestimmte Zahlungen nicht erfolgt sind. Dies kann nur durch Vorlage vollständiger Kontoauszüge ermittelt werden.

5. Das Verlangen nach Beibringung der vollständigen Kontoauszüge ist auch gemäß § 65 Abs. 1 Nr. 2 SGB I angemessen, d. h. verhältnismäßig i. e. S. Das heißt, die mit der Mitwirkung verbundenen Nachteile dürfen insgesamt die Vorteile nicht überwiegen (Seewald a.a.O. Rdnr. 8 zu § 65 SGB I). Nach Auffassung des Gesetzgebers des Jahres 1973 besteht insoweit ein Vorrang des öffentlichen Interesses an der Feststellung des wahren Sachverhaltes vor den Privatinteressen Beteiligter (Seewald a.a.O. Rdnr. 1 der Vorbemerkung zu §§ 60 - 67 SGB I mit Verweisung auf BT-Drs. 7/910 S. 48, 49). Darin wird man das Interesse an einem Unterbleiben eines Eingriffes in das als Grundrecht geschützte Recht des Antragstellers auf informationelle Selbstbestimmung einzuschließen haben. Handelt es sich bei der Sozialhilfe doch um die Auszahlung erheblicher Beträge aus vom Steuerzahler aufgebrachten Mitteln. Hinter diesem Interesse hat das Recht des Antragstellers zurückzutreten, seine Kontobewegungen nicht zu offenbaren. Wer wegen Bedürftigkeit Geld will, das der Staat anderen, nämlich Steuerzahlern, hat wegnehmen müssen, muss seine Bedürftigkeit nachweisen und daher darauf verzichten, seine wirtschaftlichen Verhältnisse, die sich nun einmal weitgehend in den Kontenbewegungen widerspiegeln und daher dort am ehesten erkennen lassen, vor der betroffenen Behörde zu verbergen.
   Weitere Grenzen der Mitwirkungspflicht sind nicht ersichtlich.

6. Nicht zulässig wäre es jedoch, wenn die Behörde die ihr vorgelegten Kontoauszüge vollständig für ihre Akte kopierte.
   Da es sich dabei um das Speichern von Daten handelt, müssen die Voraussetzungen des § 67 c Abs. 1 Satz 1 SGB X erfüllt sein. Die in dieser Vorschrift vorausgesetzte Erforderlichkeit zur Aufgabenerfüllung nach dem SGB fehlt, soweit es sich um Kontobewegungen handelt, die keine Bedeutung für die weitere Bearbeitung des Antrages auf Sozialhilfe haben. Wie oben ausgeführt, soll durch die Vorlage vor allem das Fehlen bestimmter Kontenbewegungen dargelegt werden, wodurch die Kenntnisnahme von Daten notwendig wird, die für sich gesehen nicht zur Bearbeitung des Antrages auf Sozialhilfe erforderlich sind. Wird bei der Prüfung der Kontoauszüge festgestellt, dass es sich um derartige Kontobewegungen handelt, so ist die Speicherung dieser Daten nicht erforderlich und daher nicht zulässig. Dem steht nicht entgegen, dass die Behörde für jeden Einzelfall, der ihr zur Bearbeitung vorliegt oder vorgelegen hat, Unterlagen benötigt, anhand deren sich der Verfahrensgang nachvollziehen lässt. In Anbetracht des mit der Aufbewahrung personenbezogener Unterlagen verbundenen Grundrechtseingriffs ist die Aufbewahrung nur so weit zulässig, als dies für ein ordnungsgemäßes Verwaltungsverfahren nötig ist. Dazu gehört es nicht, wenn Unterlagen nur

kopiert werden, um im Nachhinein beweisen zu können, dass diese vorgelegen haben. Hierzu reicht ein entsprechender Vermerk in der Akte (vgl. 7/10.4).
Insofern habe ich aber keine Einwände dagegen, wenn die Kontoauszüge kopiert und die für die weitere Bearbeitung des Antrages auf Sozialhilfe nicht erforderlichen Informationen geschwärzt werden. Bedenken dagegen, dass es erforderlich ist, die notwendigen Daten in Ablichtung zur Akte zu nehmen, ergeben sich nicht daraus, dass man diese auch abschreiben und in einem Vermerk deren Nachweis durch die Kontoauszüge festhalten könnte. Im Fotokopieren liegt kein weitergehender Eingriff als im Abschreiben.

Das SMS teilt meine Rechtsauffassung hinsichtlich der Zulässigkeit des Verlangens nach Vorlage von Kontoauszügen (und des Umfangs der notwendigen Schwärzungen), schätzt deren Aussagegehalt aber beträchtlich höher ein als ich. Eine wirkliche Erforschung der Einkommensverhältnisse der Antragsteller und ihre Angehörigen durch Erhebungen vor Ort ist nach Auffassung des SMS mit dem bestehenden Personal nicht zu schaffen.

Ich möchte, auf die Gefahr hin, mich zu wiederholen, meine gegensätzliche Meinung noch einmal unterstreichen:
- Kontoauszüge dienen weitgehend einer nur scheinbaren und deshalb überflüssigen Überprüfung der Angaben des Antragstellers.
- Hoheitliches Handeln ohne stichprobenhafte wirksame Kontrollen sollte es nicht geben.

10.2.7 Kann der Antragsteller die Befugnis der Behörde, Ablichtungen ihr von ihm eingereichter Unterlagen anzufertigen, beschränken?

In einem der vorstehend unter 10.2.6 erörterten Fälle war ein eifriger Petent auf den Gedanken gekommen, bei Einreichen der Unterlagen im Sozialamt der betreffenden Stadt gegenüber zu erklären, die Behörde dürfe die ihm zurückzugebenden Originalunterlagen gar nicht bzw. nur mit seiner Zustimmung ablichten und zu den Akten nehmen.

Eine solche mit der Hingabe von Unterlagen im Original - im vorliegenden Falle eben Kontoauszügen - verbundene Untersagung der Anfertigung von Ablichtungen ist ohne rechtliche Wirkung. Soweit die Ablichtungen den erforderlichen Umfang übersteigen, sind sie auch ohne den Vorbehalt rechtswidrig. Soweit sich die Ablichtungen auf das rechtlich Erlaubte beschränken - im Falle von Teil-Inhalten eben durch entsprechende Schwärzungen durch die Behörde -, ist der Vorbehalt meiner Auffassung nach unbeachtlich, weil er angesichts der legitimen Datenbedürfnisse der Behörde sowie moderner Arbeitstechnik *widersprüchlich* ist: Entweder gibt man die Daten, soweit sie für die Behörde erforderlich sind, hin und nimmt damit hin, dass diese sie, soweit erforderlich, zur Kenntnis nehmen und auch, soweit dies wiederum erforderlich ist, mit moderner, arbeitssparender Technik, also Ablichtungen mit Schwärzungen statt Abschreiben, speichern darf - oder aber der Antragsteller verweigert die Daten, mit der selbstverständlichen Folge der Möglichkeit der Leistungsversagung, wie sie im Gesetz vorgesehen ist (§ 66 Abs. 1 Satz 1 SGB I).

In dem mir vorgelegten Falle hatte ein Bediensteter den vom Antragsteller einfallsreich formulierten Vorbehalt unterzeichnet, dann hatte die Verwaltung gleichwohl Ablichtungen angefertigt. Darin liegt kein Grund, dem Sozialamt der betreffenden Stadt einen Tadel auszusprechen. Ich habe die Behörde lediglich aufgefordert, die von den Kontoauszügen angefertigten Ablichtungen in dem vorstehend unter 10.2.6 dargestellten Umfang zu schwärzen und in Zukunft gegenüber Antragstellern von vornherein klarzustellen, dass die Kontoauszüge entweder gar nicht oder aber mit der grundsätzlichen Möglichkeit der Ablichtung (mit Teilschwärzung) einzureichen sind. Ob ich den Petenten überzeugt habe bleibt offen.

10.2.8 Erhebung von Sozialdaten für Wirtschaftlichkeits- und Qualitätsprüfungen durch den Sozialhilfeträger bei einem freien Träger

Schuldnerberatung als Teil der Sozialhilfe (§ 17 BSHG) wird vielfach von freien Trägern durchgeführt, finanziert vom Sozialhilfeträger auf der Grundlage eines mit dem freien Träger abzuschließenden Vertrages. In solchen Verträgen sind gemäß § 93 a Abs. 3 BSHG auch Verfahren zur Durchführung von Wirtschaftlichkeit- und Qualitätsprüfungen zu vereinbaren. Der von einer kreisfreien Stadt, als Sozialhilfeträger, ausgearbeitete Entwurf eines solchen Vertrages sah vor, dass die Stadt berechtigt sein sollte, den Umfang der abgerechneten Erst- und Intensivberatungen anhand der vom freien Träger zu führenden Akten zu überprüfen, wobei im Vertrag zusätzlich bestimmt werden sollte, dass diese Akten bestimmte personenbezogene Daten sowohl des Hilfesuchenden als auch dessen Gläubiger zu enthalten hätten.

Entgegen der Erwartung des freien Trägers, der sich deswegen an mich gewandt hat, hat sich die in dem Vertrag vorgesehene Verarbeitung von Sozialdaten durch den Sozialhilfeträger als datenschutzrechtlich unbedenklich erwiesen:

Rechtsgrundlage der Datenerhebung durch einen Sozialhilfeträger ist § 67 a Abs. 1 i. V. m. Abs. 2 Satz 2 Nr. 2 Buchst. b aa SGB X. Danach ist das Erheben von Sozialdaten durch eine in § 35 SGB I genannte Stelle zulässig, wenn ihre Kenntnis zur Erfüllung einer Aufgabe der erhebenden Stelle nach diesem Gesetzbuch erforderlich ist. Die Sozialdaten dürfen ohne Mitwirkung des Betroffenen bei einer anderen Person oder Stelle als den in § 35 SGB I oder in § 69 Abs. 2 SGB X genannten Stellen erhoben werden, wenn die Aufgaben nach diesem Gesetzbuch ihrer Art nach eine Erhebung bei anderen Personen oder Stellen erforderlich machen und keine Anhaltspunkte dafür bestehen, dass überwiegende schutzwürdige Interessen des Betroffenen beeinträchtigt werden.
Laut Vertragsentwurf sollte der Sozialhilfeträger berechtigt sein, Sozialdaten beim freien Träger zu erheben. Der Träger der Sozialhilfe (gemäß § 96 Abs. 1 Satz 1 BSHG) ist eine in § 35 SGB I genannte Stelle, da er Leistungsträger gemäß § 12 Satz 1 i. V. m. § 28 Abs. 2 SGB I ist. Die personenbezogenen Daten der Hilfesuchenden und ihrer Gläubiger, die der Sozialhilfeträger zur Erfüllung seiner Aufgaben erheben wollte, waren Sozialdaten nach § 67 Abs. 1 Satz 1 SGB X.

Die Aufgabe, um deren Erfüllung es in solchen Fällen geht, ist die Prüfung der Wirtschaftlichkeit und Qualität der durch Einrichtungen der Träger der freien

Wohlfahrtspflege erbrachten Sozialhilfe. Die Schuldnerberatung ist eine Beratung in sog. sonstigen sozialen Angelegenheiten und gehört zur persönlichen Hilfe im Sinne des § 8 Abs. 2 Satz 1 BSHG. Diese Beratung soll gemäß § 8 Abs. 2 Satz 2 BSHG zunächst von den Verbänden der freien Wohlfahrtspflege wahrgenommen werden. Das bedeutet aber nicht, dass der Träger der Sozialhilfe damit von seiner Aufgabe befreit ist. Er bleibt vielmehr dem Hilfesuchenden gegenüber für die ordnungsgemäße Gewährung der Sozialhilfe verantwortlich. Dies schreibt § 10 Abs. 5 Satz 2 BSHG ausdrücklich vor. Um dieser Verantwortung gerecht zu werden, muss er die durch den Verband der freien Wohlfahrtspflege erbrachte Leistung überprüfen können. Wäre dem nicht so, erübrigten sich auch die Vorschriften der § 93 ff. BSHG zu den Leistungs-, Vergütungs- und Prüfungsvereinbarungen, insbesondere § 93 Abs. 2 Satz 1 Nr. 3 und § 93 a Abs. 3 Satz 1 BSHG.

§ 67 a Abs. 1 SGB X lässt eine Datenerhebung nur im erforderlichen Umfang zu. Die im Vertragsentwurf genannten Angaben, die der Stadt zu übermitteln sein sollten, überschritten das erforderliche Maß nicht. Ohne diese Angaben könnte der Sozialhilfeträger nicht wirklich überprüfen, ob eine angemessene und ordnungsgemäße Beratung im Einzelfall durchgeführt worden ist. Wenn der Sozialhilfeträger die Schuldnerberatung selbst durchführte, müsste er, um interne Aufsicht zu ermöglichen, ebenfalls diese Angaben in seinen Akten festhalten.

Dazu verpflichtet, die im Vertrag genannten Daten zu übermitteln, wird der freie Träger durch Abschluss eines solchen Vertrages. Er ist zu dieser Datenübermittlung auch berechtigt, und zwar nicht nach sozialrechtlichen, sondern nach allgemeinen datenschutzrechtlichen Regeln:
Anders als der Sozialhilfeträger ist der freie Träger als Verband der freien Wohlfahrtspflege kein Sozialleistungsträger, weshalb auf die durch ihn vorgenommene Verarbeitung personenbezogener Daten die Vorschriften des Sozialgesetzbuches nicht anwendbar sind. Nimmt er Beratungsaufgaben nach dem BSHG wahr, so nimmt er Aufgaben der öffentlichen Verwaltung wahr, und gilt daher gemäß § 2 Abs. 2 Satz 1 SächsDSG als öffentliche Stelle im Sinne des Datenschutzgesetzes. Rechtsgrundlage seiner Datenübermittlung an den Sozialhilfeträger ist § 13 Abs. 1 i. V. m. § 12 Abs. 2 Nr. 1 i. V. m. § 11 Abs. 4 Nr. 1 SächsDSG.

Weder der freie Träger noch das SMS haben Einwände gegen meine Auffassung geltend gemacht.

10.2.9 Aktenübermittlung durch ein Jugendamt an die Rechtsaufsichtsbehörde

Ein Regierungspräsidium hatte bei einem Jugendamt die Übermittlung einer bestimmten Akte zum Zweck der Ausübung der Rechtsaufsicht (als Teil der allgemeinen Kommunalaufsicht) angefordert. Das Jugendamt hatte eingewandt, die Akte enthalte Sozialdaten, die als persönlich anvertraute Daten dem besonderen Vertrauensschutz des § 65 SGB VIII unterfielen, weshalb dem Ersuchen nicht nachgekommen werden könne.

Dieser Einwand erwies sich als unbegründet. Denn einem bestimmten Mitarbeiter des Jugendamtes in dem von § 65 SGB VIII gemeinten Sinne, nämlich ausdrücklich besonders und ganz persönlich anvertraute Daten hat dieser gesondert zu speichern; sie haben in der Sachakte des Jugendamtes nichts zu suchen. Solche Daten sind gar nicht in der üblichen Weise behördenverfügbar.

Eine Sachakte, die demnach Daten, die dem besonderen Vertrauensschutz des § 65 SGB VIII unterliegen, gar nicht enthalten darf, darf das Jugendamt dem Regierungspräsidium zum Zweck der Ausübung der Rechtsaufsicht übersenden. Die Befugnis ergibt sich aus § 64 Abs. 2 SGB VIII i. V. m. § 69 Abs. 5, § 67 Abs. 3 Satz 1 SGB X. Nach § 64 Abs. 1 SGB VIII dürfen Sozialdaten nur zu dem Zweck übermittelt werden, zu dem sie erhoben worden sind. Eine Übermittlung zu Zwecken der Rechtsaufsicht verstößt scheinbar gegen den Zweckbindungsgrundsatz, da das Jugendamt die Daten ja eigentlich nicht zu solchen Zwecken erhoben hat. Jedoch enthält § 67 c Abs. 3 Satz 1 SGB X eine Konkretisierung des Zweckbindungsgrundsatzes, indem er klarstellt, dass die Wahrnehmung von Aufsichts- und Kontrollbefugnissen keine Änderung des ursprünglichen Erhebungszweckes ist. Dem Regierungspräsidium dürfen also zur Wahrnehmung von Aufsichtsbefugnissen Sozialdaten übermittelt werden, jedoch nur im für diesen Zweck erforderlichen Umfang. Da die Rechtsaufsicht nur dann effektiv wahrgenommen werden kann, wenn die Rechtsaufsichtsbehörde sich anlassfrei über jeden beliebigen Einzelfall umfassend, namentlich anhand der vollständigen Behördenakte, informieren darf, ist der Begriff „erforderlich“ in § 67 c Abs. 3 Satz 1 SGB X und § 13 SächsGemO insoweit weit auszulegen.

Die gesondert gespeicherten Sozialdaten, die einem Mitarbeiter des Jugendamtes persönlich anvertraut worden sind, dürfen allerdings nur unter den Voraussetzungen des § 65 Abs. 1 Satz 1 SGB VIII weitergegeben werden, also nur, wenn einer der in Nr. 1 bis Nr. 3 der Vorschrift genannten Ausnahmetatbestände erfüllt ist. Hier kam nur der letztgenannte in Betracht:
§ 65 Abs. 1 Satz 1 Nr. 3 SGB VIII lässt eine Weitergabe unter den Voraussetzungen zu, unter denen eine in § 203 Abs. 1 oder Abs. 3 StGB genannte Person dazu befugt wäre. Die Rechtsprechung hat den nach § 203 StGB schweigepflichtigen Personen bestimmte Offenbarungsbefugnisse zuerkannt. Diese Offenbarungsbefugnisse sollen auch im Rahmen des § 65 SGB VIII Berücksichtigung finden.
Die Rechtsprechung zu § 203 StGB hat sich mit Offenbarungsbefugnissen, die aus Kontroll- und Aufsichtsrechten hergeleitet werden, nur im Zusammenhang mit Übermittlungen zu Zwecken der Rechnungsprüfung und der Beweiserhebung durch einen parlamentarischen Untersuchungsausschuss beschäftigt. Aus diesen Entscheidungen lassen sich jedoch für den vorliegenden Fall keine Folgerungen ziehen, da der Gesetzgeber für Datenübermittlungen zu Aufsichtszwecken eine eindeutige Aussage getroffen hat: § 65 Abs. 1 SGB VIII enthält ein behördeninternes Weitergabeverbot (vgl. § 65 Abs. 2 SGB VIII). Darf schon der Kollege oder der Dienstvorgesetzte desjenigen, dem die Daten anvertraut worden sind, keine Kenntnis von den Daten erhalten, dann erst recht nicht die Rechtsaufsichtsbehörde. Hätte der Gesetzgeber eine Weitergabe anvertrauter Daten zu Zwecken der Rechtsaufsicht erlauben wollen, dann hätte er dies in den Katalog der Ausnahmetatbestände des § 65 Abs. 1 SGB VIII aufgenommen und nicht den Umweg über die Rechtsprechung zu § 203 Abs. 1 StGB gemacht.

Der Gesetzgeber hat auch nicht etwa „vergessen“ zu regeln, inwieweit Sozialdaten einer Aufsichtsbehörde übermittelt werden dürfen, denn eine solche Regelung findet sich, wie gesagt, in § 69 Abs. 5, § 67 c Abs. 3 Satz 1 SGB X.

Im Ergebnis dürfen besonders und ganz persönlich anvertraute Sozialdaten zu Zwecken der Rechtsaufsicht an die Aufsichtsbehörde nur dann weitergegeben werden, wenn derjenige, der die Daten anvertraut hat, seine Einwilligung hierzu erteilt hat (§ 65 Abs. 1 Satz 1 Nr. 1 SGB VIII).
Andererseits ist die gelegentlich in Jugendämtern anzutreffende Vorstellung, Aufsicht über die Mitarbeiter sowie über das Jugendamt als ganzes sei wegen des Sozialdatenschutzes unzulässig, in dieser pauschalen Weise ganz falsch. Soweit es sich um die in der üblichen Weise behördenverfügbaren, also nicht unter die ganz besonderen Entstehungsbedingungen des § 65 SGB VIII fallenden Akten handelt, unterliegen die Daten der im Wege der Rechtsaufsicht stattfindenden Kontrolle. Die aus § 113 SächsGemO (ggf. in Verbindung mit § 65 Abs. 2 SächsLKrO) folgende Erhebungsbefugnis des RP bzw. Übermittlungsbefugnis des Landkreises bzw. der kreisfreien Stadt dient der Rechtsaufsicht und damit der Kontrolle der Tätigkeit staatlicher Organe. An dieser Kontrolle besteht ein im Einzelfall überwiegendes Allgemeininteresse, wie es für Eingriffe in das Grundrecht auf informationelle Selbstbestimmung erforderlich ist. Die im Wege der Rechtsaufsicht stattfindende Kontrolle dient nämlich allen, die vom Verwaltungshandeln der betreffenden Behörde betroffen sind und dem allgemeinen Interesse an einer Gewährleistung der Einhaltung der Rechtsvorschriften und damit der Rechtsbindung der Verwaltung (Art. 20 GG, Art. 3 Abs. 3 SächsVerf). Verwaltungsinterne Kontrollverfahren finden zudem in der Praxis meist nur statt, wenn Betroffene sich beschweren.

10.2.10 Auskunftsrecht des Betroffenen gegenüber der Betreuungsbehörde im Hinblick auf mögliche Hinweisgeber

Eine Betreuungsbehörde hatte von privater Seite Hinweise erhalten, aufgrund deren sie mit dem Betroffenen gesprochen und ihm vorgeschlagen hatte, sich unter Betreuung stellen zu lassen.
Der Betroffene wollte nun wissen, woher die Betreuungsbehörde seine Daten erhalten, insbesondere, wer der Betreuungsbehörde den Hinweis auf die - angebliche - Betreuungsbedürftigkeit gegeben hat.

Mit einer solchen Fragestellung habe ich auf vielen Rechtsgebieten immer wieder zu tun. Zunächst musste ich auch in diesem Fall die Erwartung enttäuschen, dass die Auskunft bei mir zu holen ist: Die Auskunftserteilung durch die Behörde darf ich nicht an mich ziehen, wie § 17 Abs. 6 Satz 4 SächsDSG deutlich zeigt (aber auch § 83 Abs. 6 SGB X besagt nichts anderes). Das bedeutet: Ich kann nur - selbstverständlich ohne Einschränkung meines Einblickes in die Unterlagen, vgl. § 25 SächsDSG! - prüfen, ob die Auskunft meiner Auffassung nach zu erteilen ist oder verweigert werden darf - oder aus persönlichkeitsrechtlichen Gründen sogar muss; selbst Auskunft über meine so gewonnenen Kenntnisse darf ich aber nicht geben.

Der Anspruch des Betroffenen auf Auskunftserteilung und Gewährung von Akteneinsicht durch die Betreuungsbehörde richtete sich hier nach § 17 SächsDSG, nicht nach

SGB. Gemäß § 17 Abs. 1 SächsDSG ist dem Betroffenen von der speichernden Stelle auf Antrag kostenfrei Auskunft zu erteilen über die zu seiner Person gespeicherten Daten, den Zweck der Speicherung sowie die Herkunft der Daten und die Empfänger von Übermittlungen sowie die übermittelten Daten. Sind die personenbezogenen Daten in Akten gespeichert, die zur Person des Betroffenen geführt werden, so hat ihm die speichernde Stelle auf Verlangen Einsicht in die Akten zu gewähren (§ 17 Abs. 3 Satz 1 SächsDSG). Gemäß § 17 Abs. 5 SächsDSG unterbleibt die Auskunftserteilung, soweit die personenbezogenen Daten oder die Tatsache ihrer Speicherung nach einer Rechtsvorschrift oder wegen überwiegender Geheimhaltungsinteressen der speichernden Stelle oder eines Dritten geheimgehalten werden müssen und deswegen das Interesse des Betroffenen an der Auskunftserteilung zurücktreten muss. Dies gilt für die Gewährung von Akteneinsicht entsprechend.

Grundsätzlich hat also der Betroffene ein Auskunftsrecht über „seine“ Daten. Das datenschutzrechtliche Auskunftsrecht ist ja eine der wichtigsten Ausprägungen des Grundrechtes auf informationelle Selbstbestimmung. Deswegen ist die Darlegung eines schützenswerten Auskunftsinteresses nicht erforderlich; das Gesetz erkennt von vornherein ein derartiges Interesse des Einzelnen an. Verlangt der Betroffene Auskunft über die Herkunft der ihn betreffenden Informationen, also über den Hinweisgeber, so muss er zunächst nicht darlegen, welches Ziel er damit verfolgt und ob dieses Ziel schützenswert ist.

Dieser im Grundsatz bestehende Auskunftsanspruch ist aber gesetzlich eingeschränkt. Nach § 17 Abs. 5 Satz 1 SächsDSG unterbleibt die Auskunftserteilung, wenn ein Geheimhaltungsgrund vorliegt und eine Abwägung zwischen dem Interesse des Betroffenen an der Auskunftserteilung einerseits und dem im Geheimhaltungsgrund zum Ausdruck kommenden Geheimhaltungsinteresse andererseits zu dem Ergebnis kommt, dass das Auskunftsinteresse des Betroffenen zurücktreten muss. Geheimhaltungsgründe sind zum einen Rechtsvorschriften, die eine Geheimhaltung vorschreiben, zum anderen Geheimhaltungsinteressen der speichernden Stelle oder eines Dritten, also hier, das Interesse unseres Hinweisgebers, vom Betroffenen unerkannt zu bleiben.

Ein Geheimhaltungsinteresse der speichernden Stelle besteht immer dann, wenn die Auskunft die ordnungsgemäße Erfüllung der in der Zuständigkeit der speichernden Stelle liegenden Aufgaben gefährden würde.
Welche Aufgaben die Betreuungsbehörde hat, regeln die §§ 4 bis 9 Betreuungsbehördengesetz (BtBG). Die Behörde berät und unterstützt die Betreuer, sie unterstützt das Vormundschaftsgericht, insbesondere für die Feststellung des Sachverhalts, den das Gericht für aufklärungsbedürftig hält, und für die Gewinnung geeigneter Betreuer. Nach § 7 Abs. 1 BtBG kann die Behörde dem Vormundschaftsgericht Umstände mitteilen, die die Bestellung eines Betreuers oder eine andere Maßnahme in Betreuungssachen erforderlich machen, soweit dies unter Beachtung berechtigter Interessen des Betroffenen erforderlich ist, um eine erhebliche Gefahr für das Wohl des Betroffenen abzuwenden. Diese Aufgabenzuweisung des § 7 Abs. 1 BtBG knüpft an § 1896 Abs. 1 BGB an. Dieser nennt die formellen und materiellen Voraussetzungen der Betreuung. Zuständig für die Bestellung eines Betreuers ist danach das

Vormundschaftsgericht, das auf Antrag des Betroffenen oder von Amts wegen tätig wird. Von Amts wegen kann das Vormundschaftsgericht nur dann tätig werden, wenn ihm bekannt ist, dass bei einem Betroffenen die Voraussetzungen für die Bestellung eines Betreuers vorliegen. Diese Kenntnis verschafft ihm die Betreuungsbehörde. An diese Behörde können sich Angehörige und sonstige Personen aus dem Umfeld des Betroffenen wenden, wenn sie der Ansicht sind, es sei erforderlich, für den Betroffenen einen Betreuer zu bestellen oder eine andere Maßnahme in Betreuungssachen zu treffen. Die Betreuungsbehörde beurteilt nach ihren Erkenntnissen, ob die Einleitung eines Betreuungsverfahrens zu Abwendung einer erheblichen Gefahr für das Wohl des Betroffenen erforderlich ist. Bejaht sie dies, so teilt sie dem Vormundschaftsgericht ihre Erkenntnisse mit.
Diese Aufgabe kann die Betreuungsbehörde nur dann erfüllen, wenn Hinweise von Angehörigen oder von Personen aus dem Umfeld des Betroffenen erfolgen. Solche Hinweise werden nur dann erfolgen, wenn die Hinweisgeber sicher sein können, dass ihre Identität geheimgehalten wird, soweit sie an der Geheimhaltung ein Interesse haben.
Müsste die Behörde in jedem Fall dem Betroffenen Auskunft über den Hinweisgeber geben, so liefe sie Gefahr, dass sich niemand an die Betreuungsbehörde wendet, um familiäre, nachbarschaftliche oder ähnliche Auseinandersetzungen zu vermeiden. Damit wäre die Erfüllung eines Teils der Aufgaben der Betreuungsbehörde gefährdet. Allerdings kann die Betreuungsbehörde kein Interesse daran haben, unrichtige Hinweise zu erhalten. Sie müsste auch diesen Hinweisen nachgehen. Dies verursachte unnötigen Verwaltungsaufwand und macht viel Ärger. Solche Hinweise dienen also nicht der Aufgabenerfüllung der Behörde. Die Behörde hat deshalb auch kein Interesse daran, einen solchen „falschen“ Hinweisgeber zu schützen, d. h. seine Identität geheimzuhalten. Dies gilt für einen Hinweisgeber, der bewusst unwahre Behauptungen aufstellt. Es gilt aber auch für den Fall, dass der Hinweisgeber leichtfertig handelt, er also mit der Möglichkeit rechnet, dass seine Informationen falsch sind, er sie aber dennoch als gewiss weitergibt (vgl. BVerwG, DVBl. 1992, 298 und RhPfVerfGH NJW 1999, 2264). Nur gegen einen solchen Informanten kann der Betroffene strafrechtlich bzw. zivilrechtlich mit überwiegender Erfolgsaussicht vorgehen (vgl. OVG Koblenz, Urt. v. 9. März 1988 - 13 A 154/87, CR 1990, 730, 731 rSp.).
Das Geheimhaltungsinteresse der Behörde besteht also nur hinsichtlich eines „redlichen“ Hinweisgebers.

Dieses Geheimhaltungsinteresse der Behörde ist abzuwägen gegen das Auskunftsinteresse des Betroffenen.
Auch hier ist die Redlichkeit bzw. Unredlichkeit des Hinweisgebers von Bedeutung. Gegen einen unredlichen Hinweisgeber stehen dem Betroffenen unter Umständen straf- und zivilgerichtliche Rechtsmittel zur Verfügung. Benötigt der Betroffene die Daten des Hinweisgebers zur Einleitung eines solchen Verfahrens, so überwiegt sein Auskunftsinteresse. In den anderen Fällen überwiegt das schutzwürdige *Geheimhaltungsinteresse* des Hinweisgebers, also *des Dritten* im Sinne des § 17 Abs. 5 Satz 1 SächsDSG, das ja auch für sich genommen, neben demjenigen der Behörde, zu beachten ist. Dieser Dritte hat bei seriösem Handeln gegenüber der Behörde ein rechtlich anerkanntes Interesse, gegenüber dem Hinweis-Betroffenen ‘anonym’ zu

bleiben, d. h. daran, dass eine Übermittlung seine Person identifizierender Daten unterbleibt.

10.2.11 Datenerhebung für die Ausstellung des „Dresden-Passes“

Der sog. Dresden-Pass ist eine gesetzlich nicht geregelte Leistung, die die Landeshauptstadt Dresden für sozial schwache Einwohner seit 1998 gewährt.
Stellt jemand einen Antrag auf Ausstellung eines Dresden-Passes, so ist es Aufgabe der zuständigen Stelle (Sozialamt) zu prüfen, ob die in seiner Richtlinie festgelegten Voraussetzungen für die Gewährung der Leistung vorliegen. Die Voraussetzungen nennt Punkt 2 der Richtlinie.
Punkt 3 der Richtlinie zählt auf, welche Unterlagen der Antragsteller zur Prüfung des Vorliegens der Voraussetzungen vorzulegen hat. Lässt das Sozialamt sich die Unterlagen vorlegen, erhebt es Daten. Diese Datenerhebung ist nur zulässig, wenn eine Rechtsvorschrift dies erlaubt oder der Betroffene eingewilligt hat. Die Richtlinie ist als Verwaltungsvorschrift keine Rechtsgrundlage für die Verarbeitung personenbezogener Daten. Rechtsgrundlage ist vielmehr § 11 SächsDSG.
Nach § 11 Abs. 1 SächsDSG ist das Erheben personenbezogener Daten nur zulässig, wenn ihre Kenntnis zur Erfüllung der Aufgaben der erhebenden Stelle erforderlich ist. Die Richtlinie regelt in Punkt 3, welche Daten das Sozialamt kennen muss, um seine Aufgaben zu erfüllen, was also erforderlich ist im Sinne des § 11 Abs. 1 SächsDSG. Die Regelung ist nur dann wirksam, wenn sie dem Grundsatz der Verhältnismäßigkeit entspricht. Das Wort „erforderlich“ in § 11 Abs. 1 SächsDSG ist nämlich eine Ausprägung des Verhältnismäßigkeitsgrundsatzes. Das heißt, durch das Verarbeiten personenbezogener Daten darf in das Grundrecht auf informationelle Selbstbestimmung nur eingegriffen werden, wenn dieser Eingriff im Hinblick auf den Zweck des Eingriffes (hier: Ausstellung des Dresden-Passes) geeignet und angemessen ist; das Sozialamt darf also nicht mehr verlangen, als es zur Prüfung benötigt.

Nach Punkt 3 der Richtlinie sind die aktuellen Einkommensnachweise aller zur Bedarfsgemeinschaft zählenden Personen sowie die Nachweise über vorhandenes Barvermögen vorzulegen. Neben Verdienstbescheinigungen und Bescheiden über gewährte Sozialleistungen können auch andere Nachweise, z. B. Kontoauszüge, erforderlich sein.
Kontoauszüge können ein (allerdings nur bruchstückhaftes) Bild von der Einkommenslage, zum Teil der Vermögenslage, des Antragstellers verschaffen (siehe dazu auch 10.2.6). Die Vorlage der Kontoauszüge bringt für den Antragsteller keine unzumutbaren Schwierigkeiten mit sich.
Etwas anderes ergibt sich auch nicht dadurch, dass durch die Vorlage der Kontoauszüge auch Daten zu Kontobewegungen erhoben werden, deren Kenntnis für die Behörde nicht erforderlich ist. Die festzustellende Tatsache besteht gerade darin, dass bestimmte Zahlungen nicht erfolgt sind. Dies kann nur durch Vorlage vollständiger Kontoauszüge ermittelt werden.
Das Verlangen nach Beibringung der vollständigen Kontoauszüge ist auch angemessen. Wer wegen Bedürftigkeit Geld will, das der Staat anderen, nämlich Steuerzahlern, hat wegnehmen müssen, muss seine Bedürftigkeit nachweisen und daher darauf verzichten, seine wirtschaftlichen Verhältnisse, die sich nun einmal weitgehend in

den Kontobewegungen wiederspiegeln und sich daher dort am ehesten erkennen lassen, vor der betreffenden Behörde zu verbergen.

Nicht zulässig wäre es jedoch, wenn die Behörde die ihr vorgelegten Kontoauszüge vollständig für die Akte kopierte.
Da es sich dabei um das Speichern von Daten handelt, ist Rechtsgrundlage nicht § 11 SächsDSG, sondern § 12 Abs. 1 SächsDSG. Dieser setzt voraus, dass die Speicherung zur Erfüllung der Aufgaben der öffentlichen Stelle erforderlich ist. Diese Erforderlichkeit fehlt, soweit es sich um Kontobewegungen handelt, die keine Bedeutung für die weitere Bearbeitung des Antrages auf Ausstellung des Dresden-Passes haben. Durch die Vorlage der Kontoauszüge soll vor allem das Fehlen bestimmter Kontobewegungen dargelegt werden, wodurch die Kenntnisnahme von Daten notwendig wird, die für sich gesehen nicht zur Bearbeitung des Antrages erforderlich sind. Wird bei der Prüfung der Kontoauszüge festgestellt, dass es sich um solche Kontobewegungen handelt, so ist die Speicherung dieser Daten nicht erforderlich und daher nicht zulässig. Dem steht nicht entgegen, dass die Behörde für jeden Einzelfall, der ihr zur Bearbeitung vorliegt oder vorgelegen hat, Unterlagen benötigt, anhand deren sich der Verfahrensgang nachvollziehen lässt.
In Anbetracht des mit der Aufbewahrung personenbezogener Unterlagen verbundenen Grundrechtseingriffs ist die Aufbewahrung nur insoweit zulässig, als dies für ein ordnungsgemäßes Verwaltungsverfahren nötig ist. Dazu gehört es nicht, wenn Unterlagen nur kopiert werden, um im Nachhinein beweisen zu können, dass diese vorgelegen haben. Hierzu reicht ein entsprechender Vermerk in der Akte (vgl. 7/10.4).
Insofern habe ich aber keine Einwände dagegen, wenn die Kontoauszüge kopiert und die für die weitere Bearbeitung des Antrages auf Ausstellung des Dresden-Passes nicht erforderlichen Informationen geschwärzt werden.

Im Ergebnis bleibt festzuhalten, dass das Sozialamt die Vorlage der Kontoauszüge, die Aufschluss über die aktuelle Einkommens- und Vermögenslage des Antragstellers geben können, zur Prüfung des Antrages auf Ausstellung eines Dresden-Passes verlangen darf. Sie darf auch Kopien dieser Kontoauszüge zu den Akten nehmen, allerdings müssen diejenigen Informationen, die für die weitere Bearbeitung des Antrages nicht erforderlich sind, geschwärzt werden. Ob die Auszüge aber die Einkommens- und Vermögenslage widerspiegeln, ist äußerst fragwürdig.

10.2.12 Kennzeichnung verbilligter Monatskarten für die Benutzung der Verkehrsmittel der Dresdner Verkehrsbetriebe

Der Inhaber des sog. Dresden-Passes erhält vom Sozialamt Wertmarken; in den Verkaufsstellen der Dresdner Verkehrsbetriebe erhält er dann bei Vorlegen des Dresden-Passes und der Wertmarke verbilligte Fahrausweise. Die Wertmarke erhalten die Dresdner Verkehrsbetriebe zur Abrechnung mit dem Sozialamt.
Erwirbt der Inhaber des Dresden-Passes einen Einzelfahrschein, so wird dieser mit dem Buchstaben „W“ gekennzeichnet. An diesem Buchstaben erkennt der Kontrolleur, dass dieser Fahrausweis lediglich den Inhaber eines Dresden-Passes zur Nutzung der Verkehrsmittel berechtigt. Der Buchstabe „W“ wurde gewählt, weil er für Außen-

stehenden keinen Rückschluss auf die Gründe zulässt, derentwegen der Fahrschein so gekennzeichnet wurde.
Ein Abonnement (z. B. Monatskarte, Schülerkarte) erwirbt der Inhaber des Dresden-Passes, indem er zunächst den regulären Preis zahlt. Im sog. ABO-Kundenservice der Dresdner Verkehrsbetriebe wird dem Inhaber des Dresden-Passes bei Vorlegen der ABO-Karte, der Wertmarke und des Dresden-Passes der Wert der Wertmarke (16 DM) ausgezahlt. Die Wertmarke verbleibt zur Abrechnung bei den Dresdner Verkehrsbetrieben.
Diese Verfahrensweise ist - entgegen der Meinung einiger Beschwerdeführer - datenschutzrechtlich unbedenklich.
Die Kennzeichnung der Einzelfahrausweise mit dem Buchstaben „W“ ist erforderlich, um sicherzustellen, dass lediglich der Inhaber des Dresden-Passes den verbilligten Fahrschein zum Nachweis seiner Berechtigung zur Nutzung der Verkehrsmittel verwendet. Wäre der Schein nicht gekennzeichnet, so könnte der Inhaber eines Dresden-Passes beliebig viele Einzelfahrausweise verbilligt erwerben und diese an andere Personen, die keine Berechtigung zur verbilligten Nutzung der Verkehrsmittel haben, weiterreichen. Das Sozialamt hat festgestellt, dass ein solcher Missbrauch vor Einführung des nun bestehenden Verfahrens sehr oft stattgefunden hat.
Das gewählte Verfahren ist angemessen. Der Buchstabe „W“ hat für Außenstehende, sofern sie den Aufdruck auf dem Fahrschein überhaupt bemerken, keine Aussagekraft. Dass die Berechtigung zur verbilligten Nutzung von Verkehrsmitteln auf Fahrscheinen gekennzeichnet wird und bei einer Kontrolle nachgewiesen werden muss, ist ein übliches Verfahren, das im alltäglichen Leben weder auffällt noch diskriminierend ist. So muss z. B. jeder Inhaber einer Bahn-Card dem Schaffner diese Karte vorzeigen.

10.2.13 Anforderung von Anwesenheitsnachweisen von Studenten bei sächsischen Hochschulen durch einen Sozialleistungsträger

Ein Student hat für seine Fahrten zur Hochschule beim Rentenversicherungsträger Reisekostenersatz beantragt. Der Versicherungsträger, der prüfen muss, ob diese Kosten tatsächlich entstanden sind, hat den Studenten aufgefordert, sich von der Hochschule bestätigen zu lassen, dass er an den Lehrveranstaltungen teilgenommen habe. Darüber hinaus hat der Versicherungsträger direkt bei der Hochschule nachgefragt.

Fordert der Versicherungsträger den Studenten einer Hochschule dazu auf, solche von der Hochschule bestätigten Nachweise seiner Anwesenheit bei den Vorlesungen zu erbringen, so versucht er, Daten beim Betroffenen zu erheben, die dieser nicht liefern kann. Dies ist datenschutzrechtlich zunächst unbedenklich, wenn auch unsinnig.
Denn nach § 106 Abs. 1 Satz 1 SächsHG dürfen die Hochschulen von Studenten die personenbezogenen Daten verarbeiten, die insbesondere für Immatrikulation, Rückmeldung, Teilnahme an Lehrveranstaltungen, Prüfungen sowie die Nutzung von Hochschuleinrichtungen, Hochschulplanung und Kontaktpflege mit ehemaligen Hochschulmitgliedern erforderlich sind. Das Nähere regelt die Sächsische Studentendatenverordnung. Die Anwesenheit des Studenten bei Lehrveranstaltungen ist kein Datum, das nach den genannten Vorschriften als für die Aufgabenerfüllung der

Hochschule erforderliches Datum von der Hochschule erhoben und gespeichert werden darf.

Fordert der Versicherungsträger jedoch nicht den Studenten, sondern die sächsische Hochschule auf, diese Anwesenheitsnachweise zu erbringen, so wäre dies eine Datenerhebung bei Dritten. Diese ist gemäß § 67 a Abs. 2 Satz 2 Nr. 2 SGB X nur unter bestimmten Voraussetzungen zulässig, die nicht erfüllt wären. Insbesondere gibt es keine Rechtsvorschrift, die dem Versicherungsträger die Erhebung der Daten bei der sächsischen Hochschule erlaubte oder der sächsischen Hochschule die Übermittlung an den Versicherungsträger ausdrücklich vorschriebe (§ 67 a Abs. 2 Satz 2 Nr. 2 lit. a SGB X).
Der Versicherungsträger darf also Anwesenheitsnachweise nicht direkt von der sächsischen Hochschule anfordern.

Auf diese unbefriedigende Rechtslage habe ich den Versicherungsträger hingewiesen.

11 Landwirtschaft, Ernährung und Forsten

11.1 Entwurf eines Erlasses des SMUL zur Regelung der Datenübermittlung in Flurbereinigungsverfahren

Bei der Durchführung von Flurbereinigungsverfahren sind neben den Eigentümern der zum Flurbereinigungsgebiet gehörenden Grundstücke u. a. auch die Pächter dieser Grundstücke gemäß § 10 Nr. 2 Buchst. d FlurbG beteiligt.
Die Flurbereinigungsbehörde (Amt für ländliche Neuordnung) hat gemäß § 11 FlurbG die Beteiligten zu ermitteln, wobei die Eintragungen im Grundbuch maßgebend sind (§ 12 Satz 1 FlurbG). Nun ist die Pacht kein eintragungsfähiges Recht; es ist also aus dem Grundbuch nicht ersichtlich, wer Pächter eines bestimmten Grundstückes ist.

Um die Pächter ermitteln zu können, hatte das SMUL vor, die Ämter für Landwirtschaft, bei denen diese Daten vorhanden sind, durch Erlass anzuweisen, den Flurbereinigungsbehörden Namen und Anschriften der im Verfahrensgebiet tätigen landwirtschaftlichen Haupt- und Nebenerwerbsbetriebe sowie die Flurstücksnummern der bewirtschafteten Flächen bei Einleitung eines Flurbereinigungsverfahrens mitzuteilen.
Gestützt hat das SMUL diese Datenübermittlung auf die Amtshilfe-Vorschrift des § 135 FlurbG.

Dem SMUL, das mich um eine datenschutzrechtliche Bewertung gebeten hat, habe ich mitgeteilt, dass die Ermittlung der Beteiligten am Flurbereinigungsverfahren in § 11 i. V. m. §§ 12 bis 14 FlurbG abschließend geregelt ist. Eine Datenübermittlung durch die Ämter für Landwirtschaft an die Ämter für ländliche Neuordnung ist dort nicht vorgesehen. Eine solche Datenübermittlung wäre deshalb rechtswidrig.

Gemäß § 11 FlurbG hat die Flurbereinigungsbehörde die Beteiligten nach Maßgabe der §§ 12 bis 14 FlurbG zu ermitteln. Die Pächter von Grundstücken sind nach § 12 und § 13 FlurbG nicht zu ermitteln. Für sie gilt § 14 FlurbG, d. h. sie sind durch öffentliche Bekanntmachung aufzufordern, innerhalb von drei Monaten ihre Rechte bei der Flurbereinigungsbehörde anzumelden.
§ 135 Abs. 1 Satz 1 FlurbG wird durch die in § 11 i. V. m. §§ 12 bis 14 FlurbG getroffene abschließende Regelung verdrängt. Im Übrigen genügt § 135 Abs. 1 Satz 1 FlurbG auch nicht den Anforderungen an eine hinreichend bestimmte Datenverarbeitungsnorm.

Die Sorge, die das SMUL ausgedrückt hat, dass nicht berücksichtigte Nebenbeteiligte ihre Rechte später im Planstreitverfahren nach § 59 FlurbG geltend machen könnten, ist unbegründet. Meldet ein Pächter sein Recht nicht innerhalb von drei Monaten bei der Flurbereinigungsbehörde an, ist er nicht mehr zu beteiligen (§ 14 Abs. 1 Satz 3 FlurbG). Jedoch nur die Beteiligten am Flurbereinigungsverfahren dürfen gemäß § 59 Abs. 2 FlurbG Widerspruch gegen den Flurbereinigungsplan einlegen.

11.2 Mitteilung durch die Ämter für Landwirtschaft an landwirtschaftliche Betriebe über Schlachthöfe, die für die Schlacht-Prämiengewährung „gesperrt“ sind

Gemäß Art. 11 der Verordnung (EG) Nr. 1254/1999 wird unter bestimmten Voraussetzungen dem Erzeuger von Rindfleisch eine Schlachtprämie gewährt. Art. 35 der VO (EG) Nr. 2342/1999 regelt, welche Angaben in dem Antrag auf Prämiengewährung zu machen sind. Diese Angaben ergeben sich aus einer vom Schlachthof auszustellenden Bescheinigung, die der Antragsteller mit seinem Prämienantrag an die zuständige Behörde (in Sachsen das Amt für Landwirtschaft) weiterzugeben hat.
Unter den Voraussetzungen des Artikel 10 e Abs. 2 der VO (EG) Nr. 2801/1999 entzieht die zuständige Behörde dem Schlachthof das Recht, Bescheinigungen für Prämienzwecke zu erteilen, für eine bestimmte Zeit. Der Rindfleischerzeuger, der sein Tier in einem solchen Schlachthof schlachten lässt, erhält in diesem Fall nicht die für die Prämiengewährung notwendige Bescheinigung. Er hat demnach ein Interesse daran zu erfahren, von welchem Schlachthof er die Bescheinigung erhalten wird, wo er also sein Tier „prämienunschädlich“ schlachten lassen soll.

Das Amt für Landwirtschaft darf dem Rindfleischerzeuger, der glaubhaft die Absicht bekundet, seine Tiere in dem betreffenden Schlachthof schlachten und sich entsprechende Bescheinigungen ausstellen zu lassen, mitteilen, ob diesem Schlachthof das Recht zur Ausstellung von Bescheinigungen entzogen worden ist. Die Befugnis zur Datenübermittlung ergibt sich aus § 15 Abs. 1 Nr. 2 SächsDSG.

Der Betroffene, also der Betreiber des Schlachthofes, hat kein schutzwürdiges Interesse am Unterbleiben der Übermittlung. Er wäre sogar verpflichtet, bereits im Vorfeld des zwischen ihm und dem Rindfleischerzeuger abzuschließenden Werkvertrages über die Schlachtung bestimmter Tiere den Rindfleischerzeuger darauf hinzuwei-

sen, dass ihm das Recht auf Erteilung von Bescheinigungen entzogen worden sei. Ansonsten haftet er nach dem BGB (culpa in contrahendo).
Die in § 15 Abs. 3 SächsDSG vorgeschriebene Anhörungspflicht besteht nicht. Dieser Anhörungspflicht stehen schwerwiegende private Belange entgegen. Und zwar ist es dem einzelnen Rindfleischerzeuger nicht zuzumuten, mit der Schlachtung seiner Tiere so lange zu warten, bis die zuständige Behörde (das Amt für Landwirtschaft) den Betreiber des Schlachthofes angehört hat, zumal nicht ersichtlich ist, welche der Übermittlung entgegenstehenden Gründe der Schlachthof anbringen könnte.

Da die Entziehung („Sperrung“) zeitbezogen ist, bezieht sich die Übermittlungserlaubnis auch auf die Angabe, für wie lange sie gilt (gegebenenfalls: „unbefristet“).

Aushänge in den jeweiligen Prämienbehörden, wie sie das SMUL in Betracht gezogen hat, sind nicht zulässig, da die Übermittlung zweckgebunden ist. Nicht ein unbestimmter Kreis von Adressaten, nämlich alle, die das Amt für Landwirtschaft betreten, sondern lediglich die Landwirte, die ihre Tiere in einem bestimmten Schlachthof schlachten lassen wollen, sollen Kenntnis davon erhalten, ob dieser Schlachthof Bescheinigungen ausstellen darf oder nicht. Alle anderen geht das nichts an; das gilt auch für die Schlachtbetriebe, deren Träger eine Kapitalgesellschaft ist: Auch in diesen Fällen besteht ein datenschutzrechtlich relevanter Bezug auf natürliche Personen (gem. § 3 Abs. 1 SächsDSG).

12 Umwelt

Luftaufnahmen der bebauten und befestigten Flächen zur Berechnung des Niederschlagswasserentgeltes

Eine Abwasser-GmbH hat zur Berechnung des Niederschlagswasserentgeltes Luftaufnahmen der an die öffentliche Entwässerungsanlage angeschlossenen Grundstükke angefertigt.

Diese besondere Form der Erhebung personenbezogener Daten ist zulässig gemäß § 11 Abs. 1 SächsDSG.
Aufgabe der GmbH ist die Abwasserbeseitigung. Hierfür darf sie ein Entgelt erheben. Wie dieses Entgelt zu berechnen ist, bestimmen die Allgemeinen Geschäftsbedingungen der GmbH, die Inhalt der privatrechtlichen Verträge sind, die die GmbH mit den Grundstückseigentümern, die dem Anschluss- und Benutzungszwang unterliegen, abschließt.
Die Höhe des Entwässerungsentgeltes richtet sich nach der Größe der bebauten und befestigten Flächen des Grundstückes. Die Luftbildaufnahmen geben sowohl der GmbH als auch den betreffenden Grundstückseigentümern einen Anhaltspunkt, in welcher Größenordnung sich die Flächen bewegen. Sie dienen damit dazu, die für die Gebührenberechnung nötigen Angaben sozusagen als Zwischenstufe zutreffend zu erheben.
Die Luftbilder wurden zwar ohne Kenntnis der Betroffenen angefertigt, dennoch muss weder ein Gesetz oder eine Rechtsverordnung diese „heimliche“ Datenerhe-

bung erlauben, da die Daten allgemein zugänglich sind (vgl. § 11 Abs. 2 und 3 SächsDSG). Ebenso, wie der Gebrauch der Straßen jedermann unter bestimmten Voraussetzungen gestattet ist (Gemeingebrauch), so ist auch die Benutzung des Luftraumes frei, soweit sie nicht durch das Luftverkehrsgesetz und einige andere Vorschriften beschränkt wird. Die bei Benutzung des Luftraumes durch Betrachten der Erdoberfläche erhobenen Grundstücks-Daten sind daher genauso allgemein zugänglich wie vom öffentlichen Straßenraum aus durch Bildaufnahmen der Außenansichten von Gebäuden bzw. Grundstücken (Einfriedungen, Bepflanzung) gewonnene Daten. Für derartige Bildaufnahmen, die vom öffentlichen Straßenraum aus angefertigt worden sind, haben die Gerichte in letzter Zeit überwiegend entschieden, dass sie das Persönlichkeitsrecht (der Bewohner bzw. Eigentümer) nicht verletzen, weil nämlich nur die Öffentlichkeitssphäre berührt ist, von der jedermann Kenntnis nehmen kann und die daher keinen Schutz gegen Indiskretionen genießt (VG Karlsruhe, Beschl. v. 1. Dezember 1999, AZ 2 K 2911/99, unter Berufung auf ein Urteil des LG Waldshut-Tiengen vom 28. Oktober 1999, 1 O 200/99, sowie OLG Brandenburg NJW 1999, 339, 3340 rSp.). Für Luftbildaufnahmen gilt nichts anderes. Luftaufnahmen bedürfen daher aus gutem Grund seit einiger Zeit nicht mehr einer behördlichen Genehmigung. Gegen die zweckgerichtete und nicht tiefer in das Persönlichkeitsrecht eingreifende Feststellung für jedermann zugänglicher Verhältnisse aus der Luft können deshalb keine grundsätzlichen Bedenken vorgetragen werden.

13 Wissenschaft und Kunst

13.1 Beanstandung einer sächsischen Hochschule wegen Gewährung von Akteneinsicht durch Studenten in einem laufenden Verwaltungsrechtsstreit

Drei Studenten, die Mitglieder des Konzils einer sächsischen Hochschule sind, wurde vom Kanzler der Hochschule Einsicht in Klage und Klageerwiderung in einem rechtshängigen verwaltungsgerichtlichen Verfahren gewährt. Beklagte ist die Universität, Kläger ein Hochschullehrer, der in einer sog. Normergänzungsklage die Hochschule auf Änderung ihrer Satzung verklagt hat. Diese Klage hatte der Professor zum Gegenstand einer Hausarbeit im Rahmen einer Fortgeschrittenen-Übung im öffentlichen Recht gemacht, an der auch die drei Studenten Interesse hatten oder gar teilnehmen wollten.
Gewährt wurde die Akteneinsicht nicht zum Zweck, den Studenten einen Vorteil für ihre Teilnahme an der Fortgeschrittenen-Übung zu verschaffen; dies war nur eine unerwünschte Folge. Der Kanzler hat Einsicht vielmehr aus zwei Gründen gewährt: Zum einen habe der Professor in einer Sitzung des Konzils erklärt, dass er seine Klageschrift an Interessenten herausgeben werde. Zum andern diene die Akteneinsicht der Wahrnehmung der hochschulpolitischen und -internen Belange der Studenten. Rechtsgrundlage sei § 29 VwVfG.
Einer der Studenten selber hat den Professor über die Akteneinsichtnahme informiert, die den Studenten ermöglichte, die rechtlichen Ausführungen des Klägers zu kennen,

bevor diese in einer allen Studenten zugänglichen öffentlichen Verhandlung des Verwaltungsgerichts oder doch zumindest in einer Sitzung des für Satzungsänderungen zuständigen Konzils, dem auch Studenten angehören, erörtert wurden.
Der Hochschullehrer hat sich daraufhin wegen Verletzung seines Rechts auf informationelle Selbstbestimmung durch die Hochschule an mich gewandt.
In der Anhörung nach § 26 SächsDSG hat die Universität zusätzlich vorgebracht, die Akten enthielten keine personenbezogenen Daten, sondern lediglich rechtliche Ausführungen. Jedenfalls seien personenbezogene Daten wie die Adresse des Hochschullehrers öffentlich bekannt. Wie überhaupt der Rechtsstreit mit seinem wesentlichen Inhalt durch die Gremienarbeit der Universität bekannt sei. Darüber hinaus habe der Professor durch die Hausarbeit selbst zu einer Veröffentlichung beigetragen.

Ich habe die Gewährung der Akteneinsicht beanstandet.

Die mit der Akteneinsicht verbundene Übermittlung personenbezogener Daten des Hochschullehrers und weiterer in der Klageschrift genannter Personen war rechtswidrig. Weder lag ein Einverständnis dieser Personen in diese Datenübermittlung vor noch wird sie durch eine Rechtsvorschrift erlaubt.

1. Die Klageschrift enthält personenbezogene Daten des Hochschullehrers, so z. B. wann und mit wem er, den Verfahrensgegenstand betreffend, Kontakt aufgenommen hat und welchen Inhalt die Gespräche hatten.
   Des Weiteren enthält die Klageschrift Mitteilungen über weitere Personen, die den Kläger in seiner Prozessführung unterstützt haben. Deren Recht auf informationelle Selbstbestimmung ist ebenfalls betroffen.
   Entgegen der Auffassung der Universität ist auch die Klageschrift als Ganzes ein personenbezogenes Datum. In den rechtlichen Ausführungen kommt der Gedankengang des Verfassers zum Ausdruck, der mit diesem Inhalt und in dieser Form (Aufbau) seine persönliche geistige Schöpfung ist.

2. Es mag sein, dass der eine oder andere Interessierte, möglicherweise auch eine gewisse begrenzte Öffentlichkeit mit dem Thema des Prozesses bekannt war oder bekannt gemacht wurde, bevor es zur Akteneinsicht kam. Dies berechtigt die Universität als öffentliche Stelle jedoch nicht, eine Datenübermittlung an Private vorzunehmen. Das Datenschutzrecht enthält keine Regel, wonach öffentliche Stellen personenbezogene Daten, die - aus welchen Gründen auch immer - umrisshaft und ungefähr bekannt sind, an Private übermitteln dürfen.
   Die Einzelheiten waren eben nicht bekannt, sonst hätte man nicht die Akten schauen müssen. Im Übrigen enthielten die Akten auch viele noch nicht bekannte Informationen.

3. Ein Einverständnis des Professors in die Weitergabe seiner Daten durch die Hochschule lag nicht vor. Er hat lediglich geäußert, dass *er* die Klageschrift an Interessenten herausgeben werde. Darin liegt kein Einverständnis mit der Herausgabe oder gar Gewährung vollständiger Akteneinsicht durch *Dritte*, nämlich die Hochschule.

4. Die von der Universität genannte Rechtsgrundlage des § 29 VwVfG scheidet aus: Gemäß § 9 VwVfG i. V. m. § 1 SächsVwVfG regeln die Vorschriften nur die Akteneinsicht und die Beteiligtenstellung in einem Verwaltungsverfahren. Dies ist die nach außen wirkende Tätigkeit der Behörden, die auf die Prüfung der Voraussetzungen, die Vorbereitung und den Erlass eines Verwaltungsaktes oder auf den Abschluss eines öffentlich-rechtlichen Vertrages oder - ausnahmsweise - eines Realaktes gerichtet ist. Verfahren, die auf den Erlass von Rechtsverordnungen oder Satzungen gerichtet sind, gehören ebensowenig dazu wie das gerichtliche Verfahren, für das Beteiligtenstatus und Akteneinsicht in §§ 61 f. und § 100 VwGO speziell geregelt sind.

   Geklagt wurde auf Feststellung einer Satzungsergänzungspflicht. Einer solchen Klage geht kein Verwaltungsverfahren voraus, auf das die Vorschriften des Verwaltungsverfahrensgesetzes hätten Anwendung finden können. Die Feststellung eines Normergänzungsanspruchs wird ausschließlich in einem gerichtlichen Verfahren durchgeführt. Die Gewährung von Akteneinsicht ist für das gerichtliche Verfahren in § 100 VwGO abschließend geregelt.

   Das Bundesverwaltungsgericht hat entschieden (BVerwGE 67, 300 [304]): Das Einsichtsrecht beginnt frühestens mit der Einleitung des Verfahrens nach § 22 VwVfG und endet mit seinem Abschluss gemäß § 9 VwVfG. Ein darüber hinaus gehendes allgemeines Akteneinsichtsrecht außerhalb eines Verwaltungsverfahrens besteht nicht (BVerwGE 61, 15 [22]).

5. Gewährt die Hochschule Akteneinsicht in Schriftsätze eines verwaltungsgerichtlichen Verfahrens, umgeht sie § 100 VwGO. Die Akteneinsicht wird vom Gericht, nicht von einer Prozesspartei gewährt. Einsehen können die Akten die am Verfahren Beteiligten. Die drei Mitglieder des Konzils sind dies nicht:

   a) Aus ihrem studentischen Mitgliedschaftsstatus an der Universität folgt nicht, dass sie als künftige mittelbare oder unmittelbare Normadressaten bzw. Normbetroffene ein Recht auf Beteiligung im Verfahren hätten. Denn für die verwaltungsgerichtliche Normenkontrolle nach § 47 VwGO wird dies verneint, da sich eine Rechtsnorm grundsätzlich nicht an einen bestimmten Personenkreis richtet (BVerwGE 65, 131 [137]). Für die Frage der Beiladung im verwaltungsgerichtlichen Verfahren auf Normergänzung ist dies nicht anders zu beurteilen. Deshalb bleiben die Studenten trotz ihrer Mitgliedschaft im Verhältnis zur Universität als einer Körperschaft des öffentlichen Rechts zweifellos Dritte im Sinne des § 3 Abs. 4 SächsDSG mit der Folge, dass § 15 SächsDSG einschlägig ist. Die bereichsspezifische Datenschutzregelung des § 106 Sächsisches Hochschulgesetz bestätigt diesen Drittstatus der Studenten. Es steht außer Frage, dass den rund 25.000 Studenten der Hochschule nicht ein persönliches Recht auf Akteneinsicht zusteht.

   b) Auch soweit es um die Wahrnehmung der organschaftlichen Aufgaben der drei betroffenen Studenten als Konzilsmitglieder bzw. Fachschaftsbeiräte geht, kommt deren Beteiligung am verwaltungsgerichtlichen Rechtsstreit un-

ter keinem rechtlichen Gesichtspunkt in Betracht. In einem gegen eine juristische Person des öffentlichen Rechts gerichteten verwaltungsgerichtlichen Klageverfahren (Außenrechtsstreit) kommt Organen und Organteilen der juristischen Person grundsätzlich keine eigene Beteiligtenfähigkeit zu (vgl. Kopp/ Schenke, VwGO, 12. Auflage 2000, § 61 Rdnrn. 5, 11). Deshalb können die studentischen Konzilsmitglieder als solche selbst dann nicht beigeladen werden, wenn man in dem Klageverfahren die Anwendung von § 65 VwGO für prinzipiell möglich erachten würde.

Auch soweit die Studenten in ihrer organschaftlichen Funktion am hochschulinternen Willensbildungs- und Entscheidungsprozess beteiligt sein könnten, gilt für dieses Verfahren nicht das Verwaltungsverfahrensgesetz, denn es handelt sich nicht um eine nach außen wirkende Tätigkeit der Universität (siehe oben).

Die Informationsrechte und Informationspflichten der innerhalb der Universität Beteiligten richten sich vielmehr nach der körperschaftsinternen Kompetenzverteilung, wie sie das Sächsische Hochschulgesetz für die einzelnen Hochschulorgane, deren Mitglieder und den jeweiligen organschaftlichen Willensbildungs- und Entscheidungsprozess vorsieht (siehe §§ 67 f. Sächsisches Hochschulgesetz). Das Nähere über die Rechte und Pflichten der Mitglieder wird in der Grundordnung geregelt. An die daraus resultierende Kompetenzverteilung ist der Kanzler der Universität gebunden; er darf sie nicht durch eine „freihändige“ oder gar selektive Informationspolitik unterlaufen.

Wenn also die Kompetenz des Konzils zur Änderung der Grundordnung durch die Klage berührt ist, folgt aus den vorgenannten gesetzlichen Vorschriften, dass sich das Konzil von der Verwaltung der Universität über den Stand des gerichtlichen Verfahrens informieren lassen kann und dass der Kanzler als Leiter der Verwaltung auch zur Information des Konzils verpflichtet ist (§§ 96 Abs. 4 Satz 2, 65 Abs. 4 Satz 1 Nr. 1 SächsHG).

Auskunfts- und Akteneinsichtsrechte einzelner Konzilsmitglieder gegen die Hochschulverwaltung resultieren daraus jedoch gerade nicht. Solche Rechte sind weder im Sächsischen Hochschulgesetz noch in der Grundordnung der Universität vorgesehen. Dies wäre verfahrensökonomisch auch unsinnig, da das Konzil der Universität Hunderte von Mitgliedern umfasst und es kaum überschaubar wäre, wenn jedem einzelnen von ihnen ein eigenes, persönliches Informationsrecht gegenüber der Verwaltung zustünde.

Ob, wann und wie intensiv sich das Konzil als zuständiges Kollegialorgan sich mit einem Gegenstand zu befassen gedenkt, hat das Konzil (nach Beratung) zu entscheiden. Das einzelne Konzilsmitglied ist demgemäß rechtlich darauf beschränkt, seine Informations- und Befassungswünsche an das Konzil heranzutragen, das dann anschließend als Kollegialorgan über diesen Antrag entscheidet und sodann gegebenenfalls ein entsprechendes Auskunftsbegehren gegenüber der Verwaltung geltend macht.

Es wäre also richtig gewesen, die Konzilsmitglieder mit ihrem Akteneinsichtsbegehren auf die Beachtung der hochschulinternen Kompetenzordnung hinzuweisen und den zuvor geschilderten Weg über das Konzil anheim zu stellen.

Datenschutzrechtlich dürfte klar sein, dass die einzelnen Konzilsmitglieder keine öffentliche Stelle sind und daher keinen Anspruch auf Datenübermittlung im Sinne des § 13 SächsDSG geltend machen können. Öffentliche Stelle ist vielmehr ausschließlich das Konzil als Kollegialorgan, das als solches zu entscheiden und sodann auch mit Informationen „zu bedienen“ ist.

c) Gleiches gilt sinngemäß für die Mitgliedschaft im Fachschaftsrat; auch dort können die einzelnen Mitglieder nicht die Rechtsstellung einer öffentlichen Stelle für sich beanspruchen; es ist vielmehr der Fachschaftsrat, der als Kollegialorgan zur Entscheidung und zur Datenanforderung befugt sein könnte.

6. Auch § 15 SächsDSG bietet keine ausreichende Rechtsgrundlage für eine Akteneinsicht:
   Soweit die Universität die Auffassung vertritt, die Mitglieder des Konzils seien Mitglieder der Hochschule, deshalb liege kein Übermitteln an eine Person außerhalb der datenverarbeitenden Stelle vor, wird damit der Begriff der öffentlichen Stelle verkannt: Dies ist jede verwaltungsorganisatorische Einheit, die für sich bestimmte gesetzliche Aufgaben mit Hilfe personenbezogener Daten durchführt. Die Universität besteht ihrerseits also aus einer Vielzahl öffentlicher Stellen. So sind die zentralen Gremien jeweils öffentliche Stellen ebenso wie die organisatorisch zur Wahrnehmung bestimmter gesetzlicher Aufgaben bestimmten Organisationseinheiten der Verwaltung jeweils für sich öffentliche Stellen sind. Jeder Datenfluss von einer dieser Stellen zu einer anderen ist als Datenübermittlung anzusehen.
   Die Datenübermittlung von öffentlichen Stellen an nicht-öffentliche Stellen (die Studenten) regelt § 15 SächsDSG. Selbst wenn die Studenten ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft darlegen und der Betroffene kein schutzwürdiges Interesse am Unterbleiben der Übermittlung haben würde (Anmerkung: Beide Voraussetzungen liegen im vorliegenden Fall nicht vor), so müsste das Verfahren des § 15 Abs. 3 SächsDSG eingehalten werden: Der betroffene Hochschullehrer hätte vor der Übermittlung angehört werden müssen. Dies ist nicht geschehen.

Sowohl die Universität als auch das SMWK, dem ich die Beanstandung als Aufsichtsbehörde zur Unterrichtung zugeleitet habe, haben die Beanstandung „zurückgewiesen“. Sie meinen, die Rechtslage sei anders, den einzelnen Mitgliedern des Konzils stünde die Akteneinsicht zu, weil sie durch die angestrebte Satzungsänderung in ihrer Rechtsstellung betroffen würden, eine Behauptung, für die ich keine sachlichen Gründe finde, zumal nicht jedem (mittelbar) Betroffenen Akteneinsicht zusteht. Eine solche Rechtsvorschrift gibt es nicht.

13.2 Übermittlung personenbezogener Daten von Zahnärzten durch die Zahnärztekammer Sachsen an eine außersächsische Universität zu Forschungszwecken

Im Rahmen eines durch eine außersächsische Universität durchgeführten Forschungsvorhabens war geplant, dass Zahnärzte, die Mitglieder der Zahnärztekammer Sachsen sind, zu ihrer Tätigkeit befragt werden. Hierzu benötigte die Universität personenbezogene Daten dieser Zahnärzte, nämlich Namen und Vornamen, Titel, Geschlecht, Geburtsdatum, Adresse des jeweiligen Zahnarztes sowie den Status als niedergelassener Arzt oder als bei einem Krankenhaus oder einer öffentlichen Stelle des Freistaates Sachsen angestellter Arzt. Diese Daten sollte die Zahnärztekammer Sachsen an die Universität übermitteln.

Ich habe der Zahnärztekammer Folgendes mitgeteilt:

Die Landeszahnärztekammer Sachsen ist gemäß § 13 Abs. 1 i. V. m. § 12 Abs. 2 Nr. 4 SächsDSG befugt, die oben genannten Daten ihrer Mitglieder an die Universität zu übermitteln.
Die Übermittlung dient der Durchführung eines Forschungsvorhabens. Im Rahmen dieses Forschungsvorhabens sollen Zahnärzte zu ihrer Tätigkeit befragt werden. Der Kreis der zu Befragenden soll eine repräsentative Stichprobe darstellen, und zwar hinsichtlich Alter, Geschlecht und Status des Zahnarztes als Selbständiger. Um eine repräsentative Stichprobe ziehen zu können, werden die genannten Daten sämtlicher Mitglieder der Landeszahnärztekammer Sachsen benötigt.
Die Zahnärztekammer verfügt nicht über das nötige statistische Fachwissen, um die Stichprobe in der gebotenen Weise selbst ziehen zu können; auch ist die statistisch richtige Ziehung von Stichproben notwendiger Bestandteil der Forschungstätigkeit. Daher ist es für die Durchführung des Forschungsvorhabens erforderlich, dass die Zahnärztekammer den Datensatz für sämtliche Mitglieder übermittelt. Gemäß § 30 Abs. 3 SächsDSG muss sich aber die Universität gegenüber der Zahnärztekammer Sachsen verpflichten, die Daten der nicht in die Stichprobe aufgenommenen Zahnärzte zu anonymisieren (Wegfall mindestens von Name und Anschrift), nachdem die Stichprobe gezogen und ihre Repräsentativität überprüft worden ist.

Solche Forschungsvorhaben zu ermöglichen und zu fördern gehört nicht zu den in § 5 Sächsisches Heilberufekammergesetz genannten Aufgaben der Zahnärztekammer. Mit der Übermittlung der Daten ist also eine Zweckänderung hinsichtlich des ursprünglichen Erhebungs- und Speicherungszweckes der Daten der Mitarbeiter verbunden. Diese Zweckänderung bedarf einer besonderen gesetzlichen Begründung. Die Voraussetzungen der Zulässigkeit einer solchen Zweckänderung nennt § 12 Abs. 2 Nr. 4 SächsDSG. Danach ist die Übermittlung zulässig, soweit sie zur Durchführung wissenschaftlicher Forschung erforderlich ist und das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen am Unterbleiben der Zweckänderung erheblich überwiegt. Eine Abwägung der beiden Interessen fällt hier zugunsten der Forschung aus. Der Eingriff in das Recht auf informationelle Selbstbestimmung des einzelnen Zahnarztes ist relativ gering. Es

handelt sich um Daten, die er selbst durch seine Tätigkeit als Zahnarzt, abgesehen vom Geburtsdatum, allgemein zugänglich macht.
Dabei ist die Angabe des Geburtsdatums nicht für das Forschungsvorhaben erforderlich: Soweit erkennbar, reicht für die Gewährleistung der Repräsentativität der Statistik das Geburtsjahr (oder Alter in Jahren) aus. Der von der Kammer zu übermittelnde Datensatz ist insoweit zu beschränken.

14 Technischer und organisatorischer Datenschutz

14.1 Private Nutzung von E-Mail und Internet in öffentlichen Stellen

1. Rechtliche Rahmenbedingungen
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 TKG). Dazu gehört zum Beispiel auch der TK-Anlagenverbund der Ministerien oder der „InfoHighway Sachsen“, 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 jedoch für das geschäftsmäßige Erbringen von Telekommunikationsdiensten, „das nachhaltige Angebot von Telekommunikation einschließlich des Angebots von Übertragungswegen für Dritte mit oder ohne Gewinnerzielungsabsicht“ (§ 3 Nr. 5 TKG). 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[1].

Gleiches gilt für Tele- und Mediendienste, deren Regelungen bei der Definition des „Anbieters“ nur auf das Bereithalten zur Nutzung oder die Zugangsvermittlung von Diensten abstellen.

[1] „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.“

Die *private* Internet- und E-Mail-Nutzung ist also ein Tele- bzw. Mediendienst; bei E-Mail-Inhalten kommt noch die Beachtung des Fernmeldegeheimnisses hinzu. Insofern sind hier insbesondere die datenschutzrechtlichen Bestimmungen zu beachten (TDSV, TDDSG, MDStV). Die *dienstliche* Nutzung dagegen unterliegt nicht den Bestimmungen des Telekommunikationsrechtes. Hier ist nur der Arbeitnehmerdatenschutz einschlägig. Allerdings ist hier darauf hinzuweisen, dass es nach der Rechtsprechung des BAG[2] in der Telekommunikation „Privatgespräche aus dienstlichem Anlass" gibt, die auch bei ausschließlich dienstlich gestatteter Nutzung geführt werden dürfen – die Gespräche müssen „in der Sphäre des Arbeitgebers liegen" oder durch die Fürsorgepflicht gestattet sein. Der Arbeitnehmer muss sich jedoch in diesen Fällen einer möglichen Kontrolle des Arbeitgebers unterwerfen, wobei zwischen Verbindungs- und Inhaltsdaten zu differenzieren ist.

2. Privater Internetzugang von Bediensteten

Wird ein privater Zugang von Bediensteten zum Internet gestattet, so hat der Arbeitgeber die Verpflichtungen des TDDSG/MDStV zu beachten:

- Nutzungsdaten sind frühestmöglich, spätestens unmittelbar nach Ende der jeweiligen Nutzung zu löschen (soweit es sich nicht um Abrechnungsdaten handelt; § 6 Abs. 2 TDDSG bzw. § 15 Abs. 2 MDStV).
- Die Prinzipien der Datenvermeidung und der Datensparsamkeit sind zu beachten (§ 3 Abs. 4 TDDSG bzw. §12 Abs. 5 MDStV).
- Der Anbieter hat dem Nutzer die Inanspruchnahme von Diensten anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist. Der Nutzer ist über diese Möglichkeit zu informieren (§ 4 Abs. 1 TDDSG bzw. § 13 Abs. 1 MDStV).
- Nutzungsprofile sind nur bei Verwendung von Pseudonymen zulässig (§ 4 Abs. 4 TDDSG bzw. § 13 Abs. 4 MDStV).

Der Arbeitgeber kann den Datenverkehr zur Gewährleistung der Datensicherheit und aus betriebstechnischen Gründen überwachen. Damit ist jedoch keine Überwachung der abgerufenen Inhalte möglich. Eine freiwillige Unterwerfung unter weitergehende Kontrollmaßnahmen ist nicht möglich, da nach § 3 Abs. 3 TDDSG/§ 12 Abs. 4 MDStV eine Erbringung von Diensten nicht von einer Einwilligung des Nutzers in eine Verarbeitung für andere Zwecke abhängig gemacht werden darf. Unberührt davon bleibt natürlich die Datenübermittlung an die Strafverfolgungsbehörden im Rahmen der Strafprozessordnung.

Die einzige Regulierungsmöglichkeit für den Arbeitgeber besteht hier in einer restriktiven Gewährung der privaten Internetnutzung (z. B. nur auf Antrag bei Vorliegen besonderer Gründe) und einer zeitlichen Begrenzung (pauschale Obergrenze, z. B. eine Stunde pro Tag, und/oder nur bei Bestehen der besonderen Gründe, nach Dienstzeit usw.). Dies wäre wohl vom Vertragsrecht her gedeckt. Zu Überdenken wäre auch eine inhaltliche Begrenzung des Angebots (z. B. Wort- und Seitenfilter). Zu Regeln wären die allgemeinen Kriterien und Modalitäten in einer Dienstvereinbarung.

[2] BAG EzA § 87 BetrVG 1972 Kontrolleinrichtung Nr.16, S.159, s.a. Anlage.

Technisch realisieren ließe sich das m. E. nur über zwei Accounts – dienstlich und privat. Für den Nutzer ist dies zumutbar; ggf. ändert sich nur die Nutzerkennung. Auf der Serverseite gestaltet sich die Konfiguration etwas schwieriger.

3. E-Mail-Nutzung
Im Gegensatz zur Sprachtelefonie und zur Internetnutzung ist eine Erfassung der Zeitdauer der Kommunikation bei E-Mail nutzlos. Der eigentliche Kommunikationsvorgang ist nur von kurzer Dauer, die Vor- oder Nacharbeiten des Nutzers sind nicht erfassbar. Das Proprium dieser Kommunikation ist gerade die Zeitversetzung. Denkbar wäre allenfalls einer Bestimmung der versendeten Datenmenge. Aber auch diese hängt von den verwendeten Formaten und nicht von der eigentlichen Information ab.

3.1 Eingehende E-Mail
Bei einer Veröffentlichung von dienstlichen E-Mail-Adressen kann nicht gesichert werden, dass der Empfänger ausschließlich dienstlich begründete E-Mails erhält. In der Regel wird auch private Kommunikation stattfinden. Von daher halte ich – da für private E-Mail-Inhalte das Fernmeldegeheimnis zu wahren ist – eine Kontrolle eingehender E-Mail generell für unzulässig (im Übrigen werden eingehende Telefongespräche auch nicht erfasst und ausgewertet).

3.2 Ausgehende private E-Mail
Für ausgehende E-Mail gilt das zur privaten Internet-Nutzung Gesagte. Allerdings kommt hier ein pauschales Zeitkontingent nicht in Frage, allenfalls eine Nutzung außerhalb einer vorgegebenen Dienstzeit. Für die Kostenabrechnung gilt gleiches. Dem Internet-Account entspricht die private E-Mail-Adresse.

14.2 Risiken und Empfehlungen bei der Nutzung von E-Mail

Sächsische Behörden versenden ihre elektronisch erstellten Schriftstücke zunehmend mit elektronischen Kommunikationsmitteln, z. B. mit E-Mail. Das ermöglicht, multimediale Daten schnell und ohne Medienbruch auszutauschen. Allerdings birgt dies Risiken hinsichtlich Sicherheit und Datenschutz. Dies ist besonders beim Versand von E-Mails mit personenbezogenen Daten und anderen Datenarten mit hohem Gefährdungsgrad zu berücksichtigen.

1. Verwendung von E-Mail
E-Mail (Electronic Mail) dient dem elektronischen Daten- und Nachrichtenaustausch zwischen mehreren Computerbenutzern über ein örtlich begrenztes Intranet oder weltweit über das Internet. Ein Intranet ist dabei ein auf Internet-Techniken (TCP/IP-Protokoll, Browser) basierendes verwaltungsinternes Informations- und Kommunikationsnetz. Dieses Netz stellt nur ihren Beschäftigten Dienste und Anwendungsprogramme (E-Mail, Aufgaben- und Dokumentenverwaltung, interne Daten ...) für dienstliche Zwecke zur Verfügung. Das Internet dagegen ist der weltweite Verbund von lokalen Netzwerken und Servern, die Dienste und Informationen (E-Mail, WWW, FTP, Telnet, Newsgroups ...) für alle Nutzer anbieten. Der Vorteil der E-Mail liegt in der weitgehend software- und hardwareunabhängigen Übermittlungs-

möglichkeit, der Schnelligkeit sowie der Fähigkeit, unterschiedlichste Dateien in elektronischer Form anzuhängen, die sofort weiterverarbeitet werden können.

Eine E-Mail besteht im allgemeinen aus Adressangaben (Empfänger, Absender), Betreff, Textkörper und eventuell aus einem oder mehreren Anhängen (Attachments). Die Nachrichten können aus Texten, Programmen, Grafiken oder sogar aus Tönen bestehen. Die elektronische Post dient damit nicht nur zur Weitergabe von kurzen Nachrichten, sondern auch zur Weiterleitung von Vorgängen oder Schreiben der Behörde an andere Behörden oder externe Empfänger. Überdies kann E-Mail auch zur Weitergabe von Dateien genutzt werden, die ohne Umwandlung von Programmen des Empfänger-PC´s verwendet werden.

Bevor Beschäftigte Nachrichten austauschen können, müssen ihre Computer vernetzt, E-Mail-Programme installiert und für jeden eine eindeutige E-Mail-Adresse (z. B. in der Form: Vorname.Name @Behörde.de) eingerichtet sein. Für jeden Beschäftigten wird ein Postfach oder eine Mailbox auf dem Mail-Server eingerichtet. Jedes Postfach ist durch ein Passwort geschützt, dass nur dem Benutzer bekannt ist.

Von den Beschäftigten gesendete Nachrichten werden an den Mail-Server weitergeleitet, der mit anderen Mail-Systemen kommuniziert und die Nachrichten an den Mail-Server des Empfängers übermittelt.

Der Übertragungsweg einer E-Mail ist variabel und im Vorfeld nicht bestimmbar, da eine E-Mail vom Mail-Server mittels „Store-and-Forward“ (zwischenspeichern und weiterschicken) an den nächst günstigen (kürzester Weg, ausreichende Bandbreite, Verfügbarkeit ...) Mail-Server weitergeschickt wird. Von dort wird eine E-Mail solange von einem Mail-Server zum nächsten übertragen, bis der Mail-Server des Empfängers erreicht ist. Der Empfänger kann dann die Nachricht mit seinem Mailprogramm aus seiner Mailbox herunterladen, lesen, eventuell ausdrucken oder anders weiterverarbeiten.

2. Risiken bei der Nutzung von E-Mail
Aufgrund der technischen Gegebenheiten bei der Übermittlung von E-Mails ergeben sich folgende Sicherheits- und Datenschutzrisiken:

- Mitlesen, Aufzeichnen oder Verändern von E-Mails während der Übertragung
Die E-Mail wird im Normalfall im Klartext übertragen. Daher könnte die Nachricht auf allen Mail-Servern, die auf dem Übertragungsweg liegen, unbefugt mitgelesen, kopiert oder sogar unbemerkt verändert werden. Eine ungesicherte E-Mail ist mit einer maschinengeschriebenen Postkarte vergleichbar. Eine vertrauliche Kommunikation ist so mittels E-Mail nicht möglich. Die Übertragung personenbezogener Daten ist deshalb ohne zusätzliche Maßnahmen nicht zulässig.

Wenn Behörden anstelle ihres Intranets das weltweite Internet zur E-Mail-Übermittlung nutzen, erhöhen sich die Risiken, weil sehr viele unbekannte (unkontrollierbare) Mail-Server zum Zwischenspeichern und Weiterleiten genutzt werden. Zu beachten ist ferner, dass aufgrund temporärer Überlastung regionaler Netze auch Mail-Server

des Auslandes zur Weiterleitung genutzt werden könnten, obwohl E-Mail-Absender und -Empfänger ihren Wohnsitz im Inland haben.

- *Vortäuschen einer falschen Absenderadresse*
Bei den meisten E-Mail-Programmen können die Absenderangaben manipuliert werden, weil die für den Versand zuständigen Protokolle (z. B. Simple Mail Transfer Protocol [SMTP]) die Angaben des Absenders nicht überprüfen. Eine Nachricht kann also problemlos unter einer falschen Absenderadresse verschickt werden. Damit besteht ein erhebliches Missbrauchsrisiko, denn der Empfänger sieht die Nachricht als authentisch und verbindlich an.

- *Zugriff auf Nachrichten im Postfach*
Alle auf einem Mail-Server eingehenden, ausgehenden und eventuell auch nicht gelöschten älteren E-Mails werden in den Postfächern des Mail-Servers gespeichert. Die Systemadministratoren des Mail-Servers oder das Personal des Internet-Providers könnten unbefugt auf die Nachrichteninhalte in den Postfächern zugreifen.

- *Nichtzustellen einer E-Mail*
Die Kommunikation per E-Mail ist im Allgemeinen schnell und komfortabel, aber nicht immer zuverlässig. Durch Störungen auf dem Übertragungsweg kann es zu Nachrichtenverlusten oder zu gänzlichem Ausfall kommen. Auch Hard- oder Softwarefehler beteiligter Kommunikationssysteme oder falsche Empfängeradressen könnten zu einer Fehl- oder Nichtzustellung einer E-Mail führen. Meist wird der Absender darüber nicht informiert. Obwohl bei einigen Mailprogrammen Optionen wie „Lesebestätigung angefordert“ oder „Übermittlungsbestätigung angefordert“ eingestellt werden können, erfolgt nicht immer eine korrekte Antwort. Entweder unterstützt die Empfängerseite diese Option nicht oder es wird nur das Eintreffen der E-Mail auf dem Mail-Server angezeigt, nicht aber das Herunterladen und Lesen der Nachricht beim Empfänger.

- *Vireninfektion durch E-Mail*
Über den elektronischen Postweg können - wie bei einem Transport per Diskette Nachrichten mit Viren ins System gelangen. Selbst ein automatisches Durchsuchen der Nachrichten nach Viren bietet keinen vollständigen Schutz, weil die Virenprogramme nicht ständig auf dem aktuellsten Stand sein können.

Eingehende E-Mails sind das häufigste Einfalltor für Computer-Viren, Trojanische Pferde oder Würmer. Solche Schadprogramme (z. B. der „I LOVE YOU-Virus“) können unkontrolliert über Adressbücher des Mailprogramms weitere mit Viren infizierte E-Mails versenden, wichtige Dateien löschen oder verändern, bzw. durch ihr hohes aufkommen jeden E-Mail-Verkehr lahmlegen.

3. Empfehlungen bei der Nutzung von E-Mail
Das Sächsische Datenschutzgesetz fordert für die Übertragung von personenbezogenen Daten gemäß § 9 Abs. 2 Nr. 9 SächsDSG, dass diese Daten nicht unbefugt gelesen, kopiert, verändert oder gelöscht werden können. Dies gilt auch bei der Nutzung von E-Mail.

- Wegen der aufgeführten Risiken dürfen E-Mails ohne zusätzliche Sicherheitsvorkehrungen nur gesendet werden, wenn sie keine personenbezogenen oder sonstige schützenswerte Informationen enthalten und nicht der Schriftform bedürfen.

- Kryptographische Verfahren, wie symmetrische und asymmetrische Verschlüsselung, sind geeignet, Verletzungen des Datenschutzes bei der Übertragung schutzwürdiger elektronisch gespeicherter Daten per E-Mail zu verhindern. Mit ihrer Hilfe lassen sich Manipulationen und Übertragungsfehler nachweisen und die unberechtigte Kenntnisnahme verhindern. Derartige Verfahren sind heute Stand der Technik und können mit vertretbarem Aufwand eingesetzt werden.

  Zu beachten ist, dass die Verschlüsselung von Daten mit einem hinreichend sicheren Verschlüsselungsverfahren erfolgt. Außerdem muss eine ordnungsgemäße Schlüsselerzeugung, -verwaltung und -verteilung gewährleistet sein. Die Verschlüsselungskomponenten sind durch technische, bauliche und organisatorische Maßnahmen vor unbefugtem Zugriff zu schützen (s. *6/14.2* und *8/14.3).*

  Allerdings können kryptographische Verfahren zur Zeit nur in gegenseitiger Absprache eingesetzt werden, weil landeseinheitliche Vorgaben fehlen.

- Der elektronische Versand von Schriftstücken, die der Schriftform bedürfen, ist ohne digitale Signatur nur vorab zu Informationszwecken zulässig oder wirksam.

- Die Adressierung von E-Mails muss eindeutig erfolgen, um eine fehlerhafte Zustellung zu vermeiden. Durch den Versand von Testnachrichten an eine neue E-Mail-Adresse kann die korrekte Zustellung geprüft werden.

- Aktuelle Anti-Virenprogramme sind sowohl beim Mail-Server als auch beim PC des Nutzers einzusetzen. Bei verschlüsselter Kommunikation muss die Virenprüfung beim PC durchgeführt werden.

- Offensichtlich nicht sinnvolle E-Mails von unbekannten Absendern sind sofort ungeöffnet zu löschen.

- Es sollten nur vertrauenswürdige E-Mail-Anhänge (z. B. nach telefonischer Absprache oder erwartete) geöffnet werden.

- In Anwendungsprogrammen (z. B. WinWord, Excel, PowerPoint) sollte der Makro-Virenschutz aktiviert und Warnmeldungen beachtet werden.

- Der Austausch von Dokumenten in Formaten, die Makros unterstützen, sollte vermieden werden. Statt dessen könnte das RTF-Format, das alle gängigen Textverarbeitungssysteme lesen kann, verwendet werden.

- Innerhalb der Behörde müssen zur Nutzung von E-Mail eindeutige Regelungen (z. B. Vertretungsregelung, Ausdrucken, Registrieren und Löschen von E-Mails,

Zeichnungsregelungen, Zustellnachweise, Absenderangaben in einer E-Mail-Nachricht: Behörde, Anschrift, Bearbeitername, Rufnummer und Angaben zu Anhängen: Dateiname und Format) festgelegt werden.

- Bei der Nutzung von E-Mail werden umfangreiche personenbezogene Daten (Protokoll- und Verbindungsdaten) gespeichert. Ich verweise für diese Problematik auf meinen Artikel zur privaten Nutzung von E-Mail in öffentlichen Stellen (14.1). Protokolldaten dienen nur zum Zweck der Datenschutzkontrolle, Datensicherheit oder zur Sicherstellung eines ordnungsgemäßen Betriebs einer Datenverarbeitungsanlage. Sie dürfen nur für diesen Zweck und hiermit in Zusammenhang stehende Maßnahmen gegenüber Bediensteten genutzt werden (§ 12 Abs. 4 SächsDSG). Weitere Regelungen, wie der Umfang der Protokollierung und eventuelle Stichprobenkontrollen, sollten in einer Dienstvereinbarung mit dem Personalrat unter Beteiligung des Sächsischen Datenschutzbeauftragten (§ 31 Abs. 7 SächsDSG) festgelegt werden.

- Vor jedem Versand von Schriftstücken mit personenbezogenen oder schützenswerten Daten muss der Beschäftigte entscheiden, ob diese per E-Mail mit zusätzlichen Sicherheitsmaßnahmen oder nur auf dem Postweg gesendet werden können.

Der Entwurf einer Dienstvereinbarung zur Nutzung von E-Mail kann beim Sächsischen Datenschutzbeauftragten angefordert werden.

14.3 Übermittlung von Dokumenten an den Petitionsausschuss im Intranet der Staatsregierung

Die Landtagsverwaltung hatte sich mit der Frage an mich gewandt, ob die Ministerien ihre Stellungnahmen an den Petitionsausschuss auch in elektronischer Form an den Landtag übermitteln könnten.

Der Landtag ist an das interne Netz der Ministerien (in Zukunft an den Infohighway) angeschlossen. Damit ist eine technische Übermittlung von Antworten der Staatsregierung an den Petitionsausschuss des Landtages technisch möglich. Da diese Antworten allerdings in der Regel in hohem Grad personenbezogene Daten enthalten werden, ist eine ungeschützte Übermittlung nicht vertretbar. Nach § 9 SächsDSG müssen ausreichende technische, personelle und organisatorische Maßnahmen getroffen werden. Im konkreten Fall müssen insbesondere folgende Maßnahmen realisiert werden:

- Zugriffsregelungen, damit (auf beiden Seiten) nur Berechtigte Zugriff erhalten,
- Verschlüsselung der Daten,
- Integration in die Vorgangsbearbeitung,
- Speicher- und Löschungsregelungen,
- Protokollierung.

Nach Rücksprache mit den Beteiligten ist eine geschlossene Benutzergruppe eingerichtet worden, in der unter Einsatz von PGP die Dokumente verschlüsselt über den InfoHighway von den Ministerien an den Petitionsausschuss verschickt werden.

Von einer Authentifizierung der Teilnehmer mit Hilfe einer digitalen Signatur im Sinne des Signaturgesetzes kann abgesehen werden, wenn die zugriffsberechtigte Gruppe auf beiden Seiten klein bleibt. Sollte der Kreis der Beteiligten größer werden (z.B. alle Abgeordneten des Petitionsausschusses in ihren Bürgerbüros), so sind auch solche Maßnahmen zu ergreifen.

14.4 Verarbeitung personenbezogener Daten und Outsourcing von EDV-Leistungen

Immer mehr öffentliche Stellen betreiben im Bereich der EDV Outsourcing. Dieses Outsourcing kann unterschiedliche Formen haben. Wartungsverträge, Beschaffung, Softwareentwicklung und -betreuung, Drucken, Transport - all das sind Dienstleistungen, die an Fremdfirmen vergeben werden können.

Der klassische Fall des EDV-Outsourcing, der auch seinen Niederschlag in den Texten der Datenschutzgesetze der 80er Jahre gefunden hat, war die Auftragsdatenverarbeitung. Papierne Listen wurden an ein Rechenzentrum übermittelt. Dort wurden die Daten am Terminal eingetippt, in der Anlage verarbeitet und die Ergebnisse ausgedruckt. Diese Druckbögen gingen zurück an den Auftraggeber. Mittlerweile lässt die Technik differenziertere Möglichkeiten des Wechselspiels zwischen Auftraggeber und –nehmer (sowohl bei Vertragsgestaltung als auch bei praktischer Umsetzung) im Rahmen des Outsourcing zu. Zum Beispiel gibt der Auftraggeber die Daten selbst ein und druckt selbst – gerechnet wird im fremden Rechenzentrum; die Geräte gehören einer Fremdfirma, stehen aber in den Räumen der öffentlichen Stelle und werden von ihr bedient; eine Fremdfirma übernimmt das Operating. Vor kurzem hat die Stadt Leipzig den weitestgehendenden Schritt getan: Die Leistungen für den gesamten EDV-Bereich – vom Einzelplatz-PC bis zum Rechenzentrum – wurden an eine Firma vergeben, an der die Stadt zwar beteiligt ist, aber nicht die Mehrheit hält. Ich hatte diesen Fall datenschutzrechtlich zu beurteilen, da es zum einen für bestimmte Datenkategorien (Meldedaten, Sozialdaten) Beschränkungen für eine Auftragsdatenverarbeitung gibt, zum anderen im Rechenzentrum der Stadt Leipzig andere öffentliche Nutzer ebenfalls rechnen ließen.

Dabei ist das Verhältnis von Outsourcing – als eigentlich betriebswirtschaftlichem Begriff - und Auftragsdatenverarbeitung – als datenschutzrechtlichem Begriff – zu untersuchen. In der Regel findet, wenn Datenverarbeitungsvorgänge outgesourct werden, auch – zumindest in Teilbereichen – Auftragsdatenverarbeitung statt. In solchen Fällen sind die Regeln des § 7 SächsDSG zu beachten. Outsourcing kann aber durchaus auch im Gewand des beauftragten Unternehmers einher kommen oder sogar ohne Verarbeitung personenbezogener Daten durch die Fremdfirma stattfinden. Letzterer Fall soll hier in seiner Abgrenzung zur Datenverarbeitung im Auftrag gesondert betrachtet werden, da er auch im Falle der Stadt Leipzig zu einer Lösung der oben beschriebenen Probleme führte.

Auftragsdatenverarbeitung findet statt, wenn der Auftragnehmer personenbezogene Daten verarbeitet. Sowohl für „personenbezogene Daten“ (§ 3 Abs.1 SächsDSG) als

auch für das „Verarbeiten“ (§ 3 Abs.2 SächsDSG) sind dabei die Begriffsbestimmungen des Sächsischen Datenschutzgesetzes zu beachten. Das Vorliegen von Auftragsdatenverarbeitung ist an drei Voraussetzungen gebunden:

1. Es geht um personenbezogene Daten.
2. Sie werden verarbeitet.
3. Handelndes Subjekt ist der Auftragnehmer. Er verarbeitet personenbezogene Daten. Auf seinen Blickwinkel kommt es bei der Bewertung des Sachverhaltes an.

Liegt eine der drei Voraussetzungen nicht vor, so findet keine Auftragsdatenverarbeitung statt.

Zu 1. Bei von vornherein nicht personenbezogenen Daten (z.B. Klimadaten, Kostenberechnungen bei der Beschaffung, Konstruktionsberechnungen o.ä.) liegt natürlich keine Auftragsdatenverarbeitung vor. Gleiches lässt sich z.B. mit einer Verschlüsselung der Daten erreichen, die damit *für den Auftragnehmer* – der zwar noch Daten informationstechnisch verarbeitet - keine personenbeziehbaren Daten mehr sind.

Zu 2. Der Fall ist evident. Wenn zwar ein Vertrag geschlossen wurde, jedoch keine personenbezogenen Daten übermittelt und dann beim Auftragnehmer verarbeitet wurden, fand keine Auftragsdatenverarbeitung statt.

Zu 3. Die öffentliche Stelle vergibt ihre gesamten DV-Leistungen an eine Fremdfirma. Eine Auftragsdatenverarbeitung liegt in diesen Fällen dann noch nicht vor, wenn folgender Grundsatz gilt: *Die logische Verarbeitung findet bei der öffentlichen Stelle statt, auch wenn sie physisch auf Geräten der Fremdfirma und betreut von deren Personal stattfindet.*
Dies ist nur dann erfüllt, wenn:

- die Administration, insbesondere die Rechtevergabe, ausschließlich bei der öffentlichen Stelle liegt,
- Mitarbeiter der Fremdfirma während der Verarbeitung keinen Zugriff auf die personenbezogenen Daten haben,
- die Übertragungswege sicher sind.

Diese Lösung ist auch bei der Stadt Leipzig vertraglich umgesetzt worden. Ich werde ihre Realisierung – sowohl im Fall des ehemaligen Rechenzentrums der Stadt als auch in der Verwaltung – weiter begleiten, da dieses Outsourcing-Modell mittlerweile auch für andere Kommunen als Pilotprojekt interessant geworden ist und die dabei gewonnenen positiven wie negativen Erfahrungen für die zukünftige stärkere Verbreitung dieses Modells von Bedeutung sind.

14.5 Application Service Providing

Mittlerweile tritt - vor allem im kommunalen Bereich - in den Scheinwerfer, wenn auch noch am Rande, eine völlig neue Form der Datenverarbeitung - ASP (Application Service Providing): Ohne großen zusätzlichen technischen und finanziellen Aufwand wird z. B. mit einem Standardbrowser über das Internet eine Verbin-

dung zu dem Application Service Provider aufgebaut, der die Software auf seinem eigenen Rechner hat und die Daten auf Wunsch der Kommune nach dem Programm, wie er es ihr anempfohlen hat, verarbeitet und sodann zurückschickt. Diese Datenbearbeitung soll verschlüsselt vorgenommen werden, so dass auch personenbezogene hochsensible Informationen - auch Informationen aus dem Willensbildungsprozess der Kommunen oder des Staates - über diese Formen verarbeitet werden können. Das Verfahren hat den Vorteil, dass die Dienstleistung sehr schnell abrufbar ist, der Aufwand findet beim Auftragnehmer und eben nicht in der Kommune statt und die Leistung, die erbracht wird, ist relativ gut abrechenbar. Man kauft sozusagen die Dienstleistung eines Datenverarbeiters. Allerdings hat ASP auch gravierende Nachteile. Wie kann man die sechs Schutzprinzipien der Datenverarbeitung - *Vertraulichkeit, Authentizität, Integrität, Verfügbarkeit, Transparenz, Revisionsfähigkeit* – durchhalten? Wie lassen sich die Versprechungen der Anbieter nachprüfen? Auch wenn Vertrauen (Trust) mittlerweile zum Begriff in der Informationstechnik geworden ist – die notwendigen korrespondierenden Kontrollmechanismen bei ASP sind mir bisher noch nicht bekannt. Ein zweites – mittelbar datenschutzrechtliches - Risiko für die Kommune besteht: Was ist bei Vertragsbruch oder bei Ausfall des ASP-Unternehmens? Und was passiert an Kostenexplosion, wenn ein Ausfall tatsächlich vorkommt? Die Kommune ist dann bewegungsunfähig, weil sie für die Datenverarbeitung keine eigenen Ressourcen mehr zur Verfügung hat. Sie müsste den Betrieb auf Handbetrieb umstellen; das ist natürlich - in größeren Gemeinden jedenfalls - kaum noch möglich. Ich rate deshalb zum gegenwärtigen Zeitpunkt – zumindest für den Bereich der Verarbeitung personenbezogener Daten – von Application Service Providing ab, sehe aber nach Beantwortung der offenen Fragen durchaus Entwicklungschancen.

14.6 Telemedizin im Krankenhausbereich

In einem Thesenpapier habe ich folgende erste Grundsätze formuliert, die keinen Anspruch auf Vollständigkeit haben:

1. Bei Anwendung der Telemedizin müssen die bestehenden Patientenrechte gewahrt bleiben. Wünschenswert wäre eine nachhaltige Verbesserung des Schutzes von Patientendaten, auf keinen Fall darf es zu einer Verschlechterung kommen.

2. Für die Übermittlung von Patientendaten gilt in der Telemedizin grundsätzlich nichts anderes als für die herkömmliche Behandlung, d. h. Beachtung der ärztlichen Schweigepflicht (Berufsordnung der Ärzte, § 203 StGB) und Offenbarung von Patientendaten nur mit entsprechender Befugnis, wobei Offenbarungsbefugnis nicht mit Offenbarungspflicht gleichzusetzen ist.

3. Ohne Einwilligung des Patienten ist die Übermittlung seiner Daten durch ein Krankenhaus nur nach Maßgabe der einschlägigen Bestimmungen in den Landeskrankenhausgesetzen zulässig.

4. Eine pauschale und vorab für alle telemedizinischen Behandlungen erklärte Einwilligung des Patienten (z. B. im Behandlungsvertrag des Krankenhauses) erfüllt

nicht die Anforderungen an eine datenschutzgerechte Einwilligung. Der Patient ist vielmehr umfassend aufzuklären, so dass er Umfang und Tragweite seiner Entscheidung zum Zeitpunkt der Erklärung hinreichend übersehen kann.

5. Werden Patientendaten in einer „elektronischen Patientenakte“ dokumentiert, ist sicherzustellen, dass *während der Behandlung* nur das Behandlungsteam im Rahmen des Behandlungsvertrages zugriffsberechtigt ist. *Nach Abschluss der Behandlung* sollte die Dokumentation dem alleinigen Zugriff der Fachabteilung unterliegen. Eine erforderliche Notfallregelung bedarf besonderer Sicherheitsmaßnahmen. Es empfiehlt sich hier wie auch bei 11. der Einsatz der „Health Professional Card“ und der mit ihr verknüpften digitalen Signatur.

6. Nach Maßgabe der Landeskrankenhausgesetze dürfen Patientendaten innerhalb des Krankenhauses auch für Zwecke der Aus- und Fortbildung genutzt werden, ohne dass es dazu der Einwilligung des Patienten bedarf.

7. Bei der Dokumentation von Patientendaten in einer „elektronischen Patientenakte“ müssen die Rechte des Patienten auf Auskunft und Einsicht gewahrt bleiben.

8. Sofern die Verfahrenskonzeption die (Zwischen-)Speicherung bzw. Archivierung von Patientendaten bei Stellen außerhalb des Krankenhauses vorsieht, handelt es sich um eine Auftragsdatenverarbeitung. Ob und unter welcher Voraussetzung sie zulässig ist, richtet sich nach den Landeskrankenhausgesetzen und Art. 8 Abs. 3 der EG-Datenschutzrichtlinie.

9. Für Forschungsvorhaben dürfen Patientendaten, die im Rahmen der Telemedizin gespeichert werden oder „anfallen“ (z. B. bei Bildübertragungen) nach Maßgabe der Landeskrankenhausgesetze genutzt werden, i. d. R. also entweder mit Einwilligung des Patienten oder mit anonymisierten Daten.

10. Soweit die im Rahmen der Telemedizin anfallenden Daten nicht nur in einem Bezug zum Patienten stehen, sondern auch Rückschlüsse auf das Verhalten und die Leistung von Ärzten bzw. des Behandlungsteams zulassen, handelt es sich um Beschäftigtendaten. Sofern personalvertretungsrechtlich vorgesehen, sollten Speicherung und Nutzung dieser Beschäftigtendaten durch Dienstvereinbarung geregelt werden.

11. Authentizität und Vollständigkeit von Patientendaten können durch technische Mängel oder Mängel in der Dokumentation beeinträchtigt werden und damit Leben und Gesundheit eines Patienten gefährden. Die Verantwortungsträger sind im Hinblick auf arbeitsrechtliche, haftungsrechtliche oder strafrechtliche Konsequenzen zu benennen.

12. Da im Rahmen der Telemedizin sensible personenbezogene Daten mit spezifischen Risiken für die Rechte und Freiheiten der Betroffenen verarbeitet werden, verlangt Art. 20 Abs. 1 der EG-Datenschutzrichtlinie, dass vor Beginn der Verarbeitung eine Vorabkontrolle durch den Datenschutzbeauftragten durchgeführt

wird. (Eine entsprechende Regelung enthält § 4d Abs. 5 des BDSG-Entwurfs, Stand: 14. Juni 2000.) Bei der Vorabprüfung ist auch die datenschutzgerechte technisch-organisatorische Ausgestaltung des Verfahrens zu bewerten.

Der Arbeitskreis „Technik" der Konferenz der Datenschutzbeauftragten des Bundes und der Länder wird sich in einer Arbeitsgruppe mit diesem Thema befassen und im nächsten Jahr ein Ergebnis vorlegen.

14.7 Telemedizin - health professional card (HPC)

Der Einsatz moderner Technik in der Medizin bringt die Informationen schneller und besser auswertbar „an den Mann". Da im sächsischen Telemedizinprojekt digitale Bilddokumente und Befunde sowohl zwischen internen als auch externen Partnern übermittelt, gespeichert und verarbeitet werden sollen, ergeben sich neue Anforderungen an die eingesetzte Technik und vor allem an die Organisation. Reichte bisher die papierne schriftliche Dokumentation samt der Unterschrift des Arztes im verschlossenen Umschlag aus, um die Echtheit und die Vollständigkeit einer Patientenakte zu gewährleisten, so ist dies heute auf andere Art und Weise zu sichern. Dieser Schutz vor Verfälschung, der sich nicht nur aus Datenschutz und Haftungsansprüchen ergibt, sondern in erster Linie medizinische Gründe hat, zwingt zum Einsatz einer elektronischen Signatur. Diese soll angewendet werden bei:

- Zugangskontrolle zu den Systemen der beteiligten Krankenhäuser und Praxen,
- Befundfreigabe in der Radiologie,
- Informationsübermittlung zwischen den verschiedenen Standorten der Projektpartner.

Erleichternd für die Entscheidung zum Einsatz der digitalen Signatur war der Umstand, dass im medizinischen Bereich bereits eine ausgearbeitete Spezifikation für eine Karte vorliegt, die die digitale Signatur gewährleistet, die sogenannte „Health Professional Card (HPC)".[3] Die Arbeitsgruppe des wissenschaftlichen Beirates des Telemedizinprojektes, an der auch die Sächsische Landesärztekammer beteiligt ist, optierte von Anfang an für die grundsätzliche Ausrichtung an dieser Spezifikation. Entscheidungskriterium ist allerdings die Erfüllung der Anforderungen des Signaturgesetzes (SigG) - im neuen Signaturgesetz: „qualifizierte Signatur" -, denn nur so ist auch zukünftig die Gleichstellung mit der schriftlichen Dokumentation und damit die von den Ärzten verlangte Rechtssicherheit für elektronische Dokumente gegeben. Da die vorhandene HPC-Spezifikation noch nicht in allen Punkten den Anforderungen des Signaturgesetzes (sowohl alter als auch neuer Form) entspricht und in einigen Bereichen auch nicht mit den derzeitig angebotenen Kartenlösungen der Trust-Center kompatibel ist, haben wir aus den oben genannten rechtlichen Gründen der Erfüllung der Anforderungen des SigG den Vorrang gegeben, wobei jedoch bereits in der

[3] Deutsche HPC Spezifikation - Ärzte -, Gemeinsame AG der Kassenärztlichen Bundesvereinigung und der Bundesärztekammer, Juli 1999, Version 1.0; Spezifikation zur äußeren Gestaltung des elektronischen Arztausweises für Deutschland, Bundesärztekammer (BÄK), Kassenärztliche Bundesvereinigung (KBV), Zentralinstitut für die Kassenärztliche Versorgung in der Bundesrepublik (ZI), Köln, August 2000.

Modell projekt 5	Das Modellprojekt 5 besteht aus zwei unabhängigen Kreiskrankenhäusern der Regelversorgungsstufe. Sie arbeiten medizinisch zusammen in einem virtuellen Verbund, der beispielhaft für die Kooperation der Krankenhäuser der Regelversorgung untereinander in Sachsen stehen kann. Das technologische Konzept zur Umsetzung des HPC-Projekts basiert auf einer modularen Systemarchitektur, in der die Hochrüstung der drei HPC-Anwendungen separat in den jeweils betreffenden Systemen erfolgt. Die Systeme sind mit Standardschnittstellen untereinander verbunden. Dadurch bleibt die unabhängige Nutzbarkeit der hochgerüsteten Systeme erhalten. Die niedrigste Modularitätsebene ist in der Radiologie der PACS Arbeitsplatz. Im PACS werden jeweils die einzelnen Arbeitsplätze zur Befundung und Betrachtung hochgerüstet und bleiben auch nach der Hochrüstung mit den HPC Anwendungen als Einzelsysteme nutzbar.
Modell projekt 6	Das Modellprojekt 6 besteht aus einem Krankenhaus der Schwerpunktversorgung, drei unabhängigen Krankenhäusern der Regelversorgungsstufe und niedergelassenen Ärzten, die in einem virtuellen Verbund medizinisch zusammenarbeiten. Es steht bei spielhaft für die Kooperation von Krankenhäusern der Regel versorgung und Praxen mit einem Kompetenzzentrum. Das technologische Konzept zur Umsetzung des HPC-Projekts basiert auf einer modularen Systemarchitektur, in der die Hochrüstung der drei HPC-Anwendungen separat in den jeweils betreffenden Systemen erfolgt. Die Systeme sind mit Standardschnittstellen unter einander verbunden. Dadurch bleibt die unabhängige Nutzbarkeit der hochgerüsteten Systeme erhalten. Die niedrigste Modularitätsebene ist in der Radiologie das PACS. Die HPC relevanten Hochrüstungen erfolgen auf dem zentralen PACS-Server. In diesem Modellprojekt wird ergänzend zu den 3 HPC-Anwendungen auch noch die HPC gestützte Langzeit-Archivierung eingeführt und in verschiedenen Kooperationsmodellen getestet.
Modell projekt 7	Im Modellprojekt 7 sind zwei Kreiskrankenhäuser eines gemeinsamen Trägers zu einem virtuellen Verbund integriert, das beispielhaft für die Integration von Krankenhäusern eines gemeinsamen Trägers stehen kann. Das technologische Konzept zur Umsetzung des HPC-Projekts basiert auf einer zentralen Systemarchitektur für die Zugangskontrolle, in der die Hochrüstung auf einem speziell dafür eingerichteten Server durchgeführt wird. Dadurch wird erreicht, dass ein Nutzer einmal angemeldet auch gleichzeitig in den anderen Systemen angemeldet ist.

Pilotphase sowohl optisch wie technisch eine weitgehende Annäherung an die HPC-Spezifikation angestrebt wird. Dies mag auf den ersten Blick als Abweichen von der vorgegebenen HPC-Spezifikation erscheinen, relativiert sich aber, wenn man sich vor Augen hält, dass sich auch nach Ansicht der Verfasser diese Spezifikation immer noch in der Entwicklung befindet. Zudem dürfte sich eher die HPC in Richtung Signaturgesetz entwickeln als umgekehrt, denn nur eine Rechtsvorschrift gewährleistet auch die von der HPC angestrebte Rechtssicherheit.

Drei der acht Teilprojekte des sächsischen Telemedizinprogramms werden die HPC einsetzen

Der veranschlagte quantitative Umfang des Karteneinsatzes ergibt sich aus folgender Tabelle:

	HPC Sichtausweis + A+B(1+2)+C	Chipkarte für medizin. Personal (A+B2+C)	Chipkarte für medizin. Personal (A)	Summe Karten
Projekt 5	115	40	80	235
Projekt 6	180	50	140	370
Projekt 7	126	34	31	191
ingesamt	421	124	251	796

(HPC - Sichtausweis mit Bild, Name, Kammerzugehörigkeit; A = Authentifizierung (eindeutige Identifizierung des Arztes im EDV-System); B1 = Digitale Signatur bei Befundfreigabe; B2 = Digitale Signatur zur Unterschrift beliebiger Schreiben; C = Schutz von Patientendaten bei ihrer Übertragung in offenen Systemen (Verschlüsselung))

Der HPC-Einsatz wird am 1. Juni 2001 starten. Der weitere Ablauf gestaltet sich folgendermaßen:

Adaptionen der Anwendungen an Routinetauglichkeit und Anwenderakzeptanz beim Hersteller	Q3 2001
Vollausbau aller Anwendung nach den Adaptionen	Q3 2001
Klinischer Betrieb & Auswertung / Evaluierung	Q3/Q4 2001

Bereits vor dem Start ergaben sich vor allem organisatorische Probleme. Das Signaturgesetz geht in seiner Grundkonzeption davon aus, dass der einzelne Nutzer einen Vertrag mit einem Trustcenter schließt, das ihm eine Karte mit der Funktionalität digitaler Signatur übergibt und – solange der Nutzer zahlt – den Verzeichnisdienst pflegt. Externe Dritte spielen nur dann eine Rolle, wenn es um die Einrichtung und Bestätigung zusätzlicher Attribute geht. Nicht im Blick ist der Umstand, dass beim Einsatz der Karte auch dieser externe Dritte möglicherweise eine rechtsverbindliche Beziehung mit dem Nutzer eingehen will. Dies kann zum einen darin liegen dass der

Einsatz der digitalen Signatur gerade an die Attributeigenschaft gebunden ist (z. B. zur Unterschrift berechtigter Beamter) oder eine zusätzliche Funktionalität hinzukommt (Sichtausweis). Der überwiegende Teil der bisher erkennbaren Einsatzmöglichkeiten der (im neuen SigG qualifizierten) digitalen Signatur sind aber solche Anwendungen (die HPC als Sichtausweis der Ärztekammer, der ministerielle Dienstausweis, die Bürgerkarte einer Kommune). Damit ergeben sich bisher rechtlich noch unbefriedigend gelöste Fragen: Wer gibt die Karte aus? Wer ist über den Verlust zu informieren? Kann die Karte eingezogen werden? Wer bezahlt?
Der derzeit in Sachsen vorgeschlagene Weg für die HPC sieht folgendermaßen aus:

- Der Arzt stellt persönlich unter Vorlage seines Personalausweises einen Antrag zur Ausstellung einer Signaturkarte vom Typ HPC über einen zertifizierten Weg beim Trust Center.
- Die Sächsische Landesärztekammer prüft, ob der Antragsteller Arzt ist und gibt die Herstellung der Signaturkarte vom Typ HPC beim Trust Center frei.
- Das Trust Center generiert die HPC und den PIN-Brief auf zertifizierten Wegen.
- Der Arzt bestätigt den Empfang der HPC dem Trust Center. Das Trust Center informiert die SLÄK.

Ein weiteres – aber besser lösbares – Problem ergibt sich daraus, dass Institutionen Karten mit einem unterschiedlichen Funktionsumfang einsetzen wollen (z. B. Zugangskontrolle), die nicht notwendigerweise mit digitaler Signatur verbunden sind, diese jedoch aber auch umfassen können. Dies führt dazu, dass man im Krankenhaus z. B. drei unterschiedliche Kartentypen einsetzt: die HPC als Sichtausweis mit qualifizierter digitaler Signatur für den Arzt, die Karte mit qualifizierter digitaler Signatur für nichtärztliches Personal mit Unterschriftsberechtigung (z. B. medizinisches Personal oder Buchhaltung) und Karten mit einfacher digitaler Signatur für sonstige Mitarbeiter, bei denen Zugangsberechtigungen überprüft werden müssen. Alle drei sollen möglichst die gleiche Hardware und Software nutzen. Dies stellt hohe Anforderungen an die Organisationskunst der Krankenhausverwaltung und Systembetreuung.

Damit sind schon die ersten Bereiche einer Evaluierung angeschnitten, denn die dabei gewonnenen (positiven wie negativen) Erfahrungen werden Einfluss auf die weitere Einführung dieser Technik haben. Über die Organisationsfragen hinaus werden innerhalb des Projektes auch physische Probleme der Kartennutzung und die Einbindung der digitalen Signatur in die Softwareanwendungen betrachtet werden.

Im Februar 2001 hat der Bundestag dem Entwurf eines Gesetzes über Rahmenbedingungen für elektronische Signaturen zugestimmt. Damit wird es nach der noch zu erfolgenden abschließenden Beteiligung des Bundesrates sehr wahrscheinlich, dass das neue Signaturgesetz zur Jahresmitte 2001 in Kraft treten kann.

Wichtige Begleitmaßnahmen sind die Erneuerung der Signaturverordnung, sowie die Schaffung der gesetzlichen Rahmenbedingungen zur Gleichstellung mit der handschriftlichen Unterschrift im Privat- und öffentlichen Recht. Damit sind dann die Grundlagen – bei entsprechender Wirkung in der Rechtsprechung – für die endgültige

Anerkennung der digitalen Signatur und den Einsatz elektronischer Dokumente gelegt.

15 Vortrags- und Schulungstätigkeit

In diesem Jahr nicht belegt.

16 Materialien

16.1 Entschließungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder

16.1.1 Entschließung der 58. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 7./8. Oktober 1999 in Rostock zur Aufbewahrung des Schriftguts der ordentlichen Gerichtsbarkeit und Staatsanwaltschaften

Die Datenschutzbeauftragten des Bundes und der Länder haben bereits in ihrer Entschließung zu Aufbewahrungsbestimmungen und Dateiregelungen im Justizbereich am 9./10. März 1995 gefordert, dass insbesondere die Dauer der Aufbewahrung von Strafakten nach rechtskräftigem Abschluss eines Strafverfahrens, ihre Aussonderung und Vernichtung einer Regelung durch formelles, den Grundsätzen des Volkszählungsurteils entsprechendes Gesetz bedarf.

Mit Beschluss vom 16. August 1998 hat das Oberlandesgericht Frankfurt am Main festgestellt, dass der derzeitige Zustand zwar für eine Übergangsfrist noch hinzunehmen sei, dass die Schaffung einer gesetzlichen Grundlage für die Aufbewahrung von Akten jedoch nicht als nur mittelfristige Aufgabenstellung des Gesetzgebers betrachtet werden dürfe, sondern alsbald in Angriff zu nehmen sei. In gleicher Weise hat auch das OLG Hamm mit Beschluss vom 17. September 1998 darauf hingewiesen, dass die Aufbewahrung von Strafakten einer gesetzlichen Grundlage bedarf. Auch der Entwurf des Strafverfahrensänderungsgesetzes 1999 enthält insoweit keine Regelung.

Die Datenschutzbeauftragten des Bundes und der Länder halten es daher für dringend geboten, dass unverzüglich mit der Umsetzung dieser Aufgabe begonnen wird. Sie weisen ferner darauf hin, dass auch für die Aufbewahrung von Zivilakten und Akten im Bereich der freiwilligen Gerichtsbarkeit umgehend gesetzliche Regelungen zu schaffen sind, die die Dauer der Aufbewahrung auf das erforderliche Maß festlegen.

16.1.2 Entschließung der 58. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 7./8. Oktober 1999 in Rostock zu „Täter-Ofper-Ausgleich und Datenschutz“

Kernstück datenschutzrechtlicher Überlegungen zum Täter-Opfer-Ausgleich ist die Frage, ob Institutionen zur Durchführung des Ausgleichsverfahrens umfassende In-

formationen insbesondere über Opfer von Straftaten erhalten dürfen, ohne dass diese davon Kenntnis erlangt und eingewilligt haben.

Darin wäre ein unverhältnismäßiger Eingriff in das Recht auf informationelle Selbstbestimmung der Betroffenen zu sehen. Dies ist nach geltendem Recht unzulässig.

Der nunmehr vorliegende Gesetzentwurf der Bundesregierung (BR-Drs. 325/99 vom 28. Mai 1999) sieht in § 155 a Satz 3 StPO-Entwurf vor, dass nur der ausdrücklich geäußerte entgegenstehende Wille der oder des Verletzten dazu führt, dass keine Datenübermittlungen an Schlichtungsstellen erfolgen sollen. Das bedeutet, dass solche im Einzelfall gleichwohl möglich sind. Dies halten die Datenschutzbeauftragten nicht für ausreichend.

Der Bundesrat ist sogar dem Gesetzentwurf der Bundesregierung nicht gefolgt; er hat vielmehr angeregt, im Gesetz klarzustellen, dass es für solche Datenübermittlungen auf den Willen der Opfer nicht ankommen soll. Folgende Argumente werden dafür genannt: Eine vor der Einschaltung von Schlichtungsstellen durch die Justiz einzuholende Einwilligung führe dazu, dass das kriminalpolitisch wichtige Institut des „Täter-Opfer-Ausgleichs“ nicht ausreichend genutzt werde. Erst die professionelle Tätigkeit der Schlichtungsstellen mit ihrem Selbstverständis als „objektive Dritte mit dem Gebot der Unterstützung jeder Partei“ könnte wirksame Überzeugungsarbeit leisten; nur dann könne der Rechtsfriede dauerhafter als bei herkömmlichen Verfahren sichergestellt werden, wenn durch die „fachlich geleitete Auseinandersetzung“ der „am strafrechtlich relevanten Konflikt beteiligten Parteien im Idealfall Verständnis und wechselseitige Toleranz geweckt werden“.

Dieser Argumentation widersprechen die Datenschutzbeauftragten entschieden: Die Achtung und wirksame Unterstützung der Opfer ist ein wesentliches Anliegen des Strafverfahrens. Rechtsfriede und Toleranz können nur verwirklicht werden, wenn die Strafverfolgungsbehörden bei Datenübermittlungen an Schlichtungsstellen (z. B. in der Rechtsform von Vereinen) den Willen und die Eigenverantwortung der Opfer uneingeschränkt respektieren. Auch die Sicht der Beschuldigten, ohne deren Mitwirkung der Täter-Opfer-Ausgleich nicht durchgeführt werden kann, sollte von den Strafverfolgungsbehörden dabei berücksichtigt werden. Die Konferenz der Datenschutzbeauftragten fordert deshalb, dass an der Voraussetzung der unzweifelhaften Einwilligung vor solchen Datenübermittlungen festgehalten wird.

Ferner sollte der Gesetzgeber festlegen, dass die Berichte der Schlichtungsstellen an Staatsanwaltschaft und Gericht nur für Zwecke der Rechtspflege verwendet werden dürfen. Das besondere Vertrauensverhältnis zwischen den Schlichtungsstellen und den am „Täter-Opfer-Ausgleich“ Beteiligten muss gesetzlich geschützt werden.

16.1.3 Entschließung der 58. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 7./8. Oktober 1999 in Rostock zu Eckpunkten der deutschen Kryptopolitik - ein Schritt in die richtige Richtung

Das Brief-, Post und Fernmeldegeheimnis zählt zu den traditionellen und wichtigsten Garantien einer freiheitlichen Verfassung. Art. 10 Grundgesetz gewährleistet deshalb

die freie Entfaltung der Persönlichkeit durch einen privaten, vor Dritten verborgenen Austausch von Nachrichten, Gedanken und Informationen. Deshalb darf nur in Ausnahmefällen im überwiegenden Allgemeininteresse auf gesetzlicher Grundlage in dieses Grundrecht eingegriffen werden.

Im Zuge der Privatisierung der Telekom hat der Staat sein Post- und Fernmeldemonopol verloren, so dass zum Grundrechtsschutz die bloße Abwehr unrechtmäßiger staatlicher Eingriffe nicht mehr genügt. Darüber hinaus bestehen die Möglichkeiten der staatlichen Datenschutzkontrolle in offenen Netzen nur in eingeschränktem Maße. Der Schutz personenbezogener Daten während der Verarbeitung und Übertragung ist häufig nicht ausreichend gewährleistet. Deshalb sind ergänzende staatliche Maßnahmen zum Schutz Aller gegen neugierige Dritte (z. B. Systembetreiber, Unternehmen mit wirtschaftlichen Interessen, Hacker und Hackerinnen, ausländische Geheimdienste) erforderlich.

Die Privatsphäre lässt sich jedoch nur mit Rechtsvorschriften nicht ausreichend schützen. Neben bestehenden Ge- und Verboten sind wirksame technische Vorkehrungen nötig. Systemdatenschutz und datenschutzfreundliche Technologien sind unverzichtbar. Den Bürgerinnen und Bürgern müssen effektive Instrumente zum Selbstschutz an die Hand gegeben werden. Der Datenverschlüsselung kommt deshalb in einem modernen Datenschutzkonzept eine herausragende Bedeutung zu.

Bislang musste befürchtet werden, dass auf Betreiben der staatlichen Sicherheitsbehörden in Deutschland das Recht auf Verschlüsselung eingeschränkt würde. Jetzt jedoch hat die Bundesregierung mit dem Eckpunktepapier vom 2. Juni 1999 die Diskussion auf eine völlig neue Basis gestellt. Richtigerweise wird darin die Kryptographie als „eine entscheidende Voraussetzung für den Datenschutz der Bürger“ besonders hervorgehoben.

Die Position der Bundesregierung, die freie Verfügbarkeit von Verschlüsselungsprodukten nicht einschränken zu wollen, wird von den Datenschutzbeauftragten des Bundes und der Länder ausdrücklich begrüßt. Damit wurde ein erster wichtiger Schritt in die richtige Richtung getan, dem jedoch weitere folgen müssen. Der im Sinne des Art. 10 des Grundgesetzes legitime und grundrechtlich geschützte Anspruch Aller auf unbeobachtete Telekommunikation und auf den Schutz ihrer personenbezogenen Daten sollte von der Bundesregierung noch stärker unterstützt werden. Um der Bedeutung geschützter Telekommunikation unter den Bedingungen der Informationsgesellschaft gerecht zu werden, sind konkrete Maßnahmen notwendig. Vorrangig sind zu nennen:

- Aktive Förderung des Einsatzes von Verschlüsselungstechniken in der öffentlichen Verwaltung, bei Privatpersonen und in Wirtschaftsunternehmen,

- Erbringung von Serviceleistungen, die den Gebrauch von effektiven Verschlüsselungsprogrammen für jedermann erleichtern,

- Maßnahmen zum besonderen Schutz der Telekommunikation von Berufsgruppen,

die besonderen Verschwiegenheitspflichten unterliegen (z. B. Ärzte und Ärztinnen, Anwälte und Anwältinnen, Psychologen und Psychologinnen),

- Unterstützung von Wirtschaftsunternehmen beim Schutz ihrer geschäftlichen Telekommunikation,

- Förderung einer neutralen Bewertung von Verschlüsselungsprodukten mit dem Ziel, den Verbrauchern Empfehlungen für ihren Gebrauch zu geben,
- Förderung der Entwicklung europäischer Verschlüsselungsprodukte mit offen gelegten Algorithmen.

Vor diesem Hintergrund fordern die Datenschutzbeauftragten die öffentlichen Stellen auf, mit gutem Beispiel voranzugehen. Sie sollten vorbehaltlos die technischen Möglichkeiten des Einsatzes kryptographischer Verfahren zum Schutz personenbezogener Daten prüfen und derartige Lösungen häufiger als bisher einsetzen. Künftig muss Kryptographie der Standard in der Informations- und Kommunikationstechnik werden, auf deren Einsatz nur dann verzichtet wird, wenn wichtige Gründe dagegen sprechen.

Hersteller von Produkten der Informations- und Telekommunikationstechnik werden aufgefordert, die guten Voraussetzungen zur Entwicklung von Verschlüsselungsprodukten in Deutschland zu nutzen, um sichere, leicht bedienbare und interoperable Produkte zu entwickeln und den Anwendern kostengünstig anzubieten. Die Datenschutzbeauftragten des Bundes und der Länder bieten hierfür ihre Kooperation an.

16.1.4 Entschließung der 58. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 7./8. Oktober 1999 in Rostock zum Beschluss des Europäischen Rates zur Erarbeitung einer Charta der Grundrechte der Europäischen Union

Der Europäische Rat hat anlässlich seiner Zusammenkunft am 4. Juni 1999 in Köln die Ausarbeitung einer Charta der Grundrechte der Europäischen Union beschlossen. In dem Ratsbeschluss heißt es: „Im gegenwärtigen Entwicklungszustand der Union ist es erforderlich, eine Charta dieser Rechte zu erstellen, um die überragende Bedeutung der Grundrechte und ihre Tragweite für die Unionsbürger sichtbar zu verankern."

Die Datenschutzbeauftragten des Bundes und der Länder unterstützen nachhaltig die Initiative des Europäischen Rates zur Ausarbeitung einer europäischen Grundrechtscharta. Sie fordern Bundesregierung, Bundestag und Bundesrat auf, sich für die Einfügung eines Grundrechts auf Datenschutz in den zu schaffenden Katalog europäischer Grundrechte und dessen Verankerung in den Verträgen der Europäischen Union einzusetzen. Damit würde der herausragenden Bedeutung des Datenschutzes in der Informationsgesellschaft Rechnung getragen.

Die europäische Datenschutzrichtlinie verpflichtet die Mitgliedstaaten zur Gewährleistung des Schutzes der Grundrechte und Grundfreiheiten und insbesondere des

Schutzes der Privatsphäre (Art. 1 Abs. 1). Die Datenschutzbeauftragten weisen darauf hin, dass einige europäische Länder ein Datenschutzgrundrecht in ihre Verfassung aufgenommen haben; in einigen anderen Ländern wurde ihm durch die Rechtsprechung Grundrechtsgeltung zuerkannt. In Deutschland wird das vom Bundesverfassungsgericht aus dem Persönlichkeitsrecht (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG) abgeleitete Grundrecht auf Datenschutz als solches von zahlreichen Landesverfassungen ausdrücklich erwähnt.

16.1.5 Entschließung der 58. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 7./8. Oktober 1999 in Rostock zu Patientenschutz durch Pseudonymisierung

Im Gesundheitsausschuss des Deutschen Bundestages wird derzeit der vom Bundesministerium für Gesundheit vorgelegte Gesetzentwurf zur Gesundheitsreform 2000 dahingehend geändert, dass die Krankenkassen künftig von den Leistungserbringern (z. B. Ärztinnen und Ärzte, Krankenhäuser, Apotheken) die Patientendaten nicht in personenbezogener, sondern in pseudonymisierter Form erhalten. Dieses neue Modell nimmt eine zentrale Forderung der Datenschutzbeauftragten auf, für die Verarbeitung von Patientendaten solche technischen Verfahren zu nutzen, die die Persönlichkeitsrechte der Betroffenen wahren und so die Entstehung des „gläsernen Patienten“ verhindern.

Auch anhand von pseudonymisierten Daten können die Krankenkassen ihre Aufgaben der Prüfung der Richtigkeit der Abrechnungen sowie der Wirtschaftlichkeit und der Qualität der Leistungen erfüllen.

Die Konferenz unterstützt den Bundesbeauftragten für den Datenschutz dabei, dass in den Ausschussberatungen die Wirksamkeit der Pseudonymisierung, die gesetzliche Festlegung von Voraussetzungen für die Identifizierung der Versicherten zu bestimmten Zwecken und die Definition strikter Zweckbindung dieser Daten durchgesetzt werden.

16.1.6 Entschließung der 58. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 7./8. Oktober 1999 in Rostock zu DNA-Analysen zur künftigen Strafverfolgung auf der Grundlage von Einwilligungen

In der Strafprozessordnung ist der Einsatz der DNA-Analyse zur vorbeugenden Verbrechensbekämpfung nur mit richterlicher Anordnung vorgesehen.

In einigen deutschen Ländern werden DNA-Analysen ohne richterliche Anordnung gestützt allein auf die Einwilligung der Betroffenen durchgeführt. Soweit die dabei erhobenen Daten zum Zweck der Identitätsfeststellung in künftigen Strafverfahren genutzt werden sollen, bedürfen DNA-Analysen nach der klaren gesetzlichen Regelung des DNA-Identitätsfeststellungsgesetzes jedoch einer richterlichen Anordnung. Der Richter oder die Richterin hat u. a. die Prognose zu treffen, ob Grund zur Annahme besteht, dass gegen Betroffene künftig erneut Strafverfahren wegen des

Verdachts erheblicher Straftaten zu führen sind. Wenn nunmehr auch DNA-Analysen gespeichert und zum Zweck der zukünftigen Strafverfolgung genutzt werden dürfen, die auf freiwilliger Basis - also ohne richterliche Anordnung - erstellt worden sind, und dies sogar durch die Errichtungsanordnung für die DNA-Analyse-Datei beim BKA festgeschrieben werden soll, werden damit die eindeutigen gesetzlichen Vorgaben des DNA-Identitätsfeststellungsgesetzes unterlaufen.

Die von Strafgefangenen erteilte Einwilligung zur Entnahme, Analyse und Speicherung kann keine Grundlage für einen derartigen Eingriff sein. Eine wirksame Einwilligung setzt voraus, dass sie frei von psychischem Zwang freiwillig erfolgt. Da Strafgefangene annehmen können, dass die Verweigerung der Einwilligung Auswirkungen z. B. auf die Gewährung von Vollzugslockerungen hat, kann hier von Freiwilligkeit keine Rede sein. Ausschlaggebend für die Beurteilung der Freiwilligkeit einer Einwilligung ist die subjektive Einschätzung des Betroffenen. Auch wenn im Einzelfall die Weigerung von Strafgefangenen, sich einer DNA-Analyse zu unterziehen, die Entscheidung über Vollzugslockerungen nicht beeinflusst, ist dennoch davon auszugehen, dass die Befürchtung, die Verweigerung habe negative Folgen, die freie Willensentscheidung beeinträchtigen.

Die Datenschutzbeauftragten des Bundes und der Länder halten deshalb die Praxis einiger Länder, DNA-Analysen - abweichend von den gesetzlich vorgesehenen Verfahren - systematisch auf Grund von Einwilligungen durchzuführen, für eine Umgehung der gesetzlichen Regelung und damit für unzulässig. Die möglicherweise mit der Beantragung richterlicher Anordnungen verbundene Mehrarbeit ist im Interesse der Rechtmäßigkeit der Eingriffsmaßnahmen hinzunehmen. Die Datenschutzbeauftragten fordern daher, DNA-Analysen zum Zweck der Identitätsfeststellung für künftige Strafverfahren nur noch auf der Grundlage richterlicher Anordnungen durchzuführen.

16.1.7 Entschließung der 58. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 7./8. Oktober 1999 in Rostock zum Zugriff der Strafverfolgungsbehörden auf Verbindungsdaten in der Telekommunikation

Die Ausbreitung moderner Telekommunikationsnetze und die Fortentwicklung der Informationstechnologie erfolgen in großen Schritten. Dieser technische Fortschritt hat einerseits zu einer massenhaften Nutzung der neuen Möglichkeiten der Telekommunikation und damit zu einer grundlegenden Veränderung des Kommunikationsverhaltens der Bevölkerung geführt. Andererseits erhalten dadurch die herkömmlichen Befugnisse der Strafverfolgungsbehörden zur Überwachung des Fernmeldeverkehrs eine neue Dimension, weil aufgrund der weitreichenden Digitalisierung immer mehr personenbezogene Daten elektronisch übertragen und gespeichert werden.

Die bei der Telekommunikation anfallenden Daten können mit geringem Aufwand in großem Umfang kontrolliert und ausgewertet werden. Anhand von Verbindungsdaten lässt sich nachvollziehen, wer wann mit wem kommuniziert hat, wer welches Medi-

um genutzt hat und wer welchen weltanschaulichen, religiösen und sonstigen persönlichen Interessen und Neigungen nachgeht. Bereits auf der Ebene der bloßen Verbindungsdaten können so Verhaltensprofile erstellt werden, die die Aussagekraft von Inhaltsdaten erreichen oder im Einzelfall sogar übertreffen. Eine staatliche Überwachung dieser Vorgänge greift daher tief in das Telekommunikationsgeheimnis der Betroffenen ein und berührt auf empfindliche Weise die Informationsfreiheit und den Schutz besonderer Vertrauensverhältnisse.

Die bisherige rechtliche Grundlage für den Zugriff der Strafverfolgungsbehörden auf Verbindungsdaten in § 12 der Fernmeldegesetzes (FAG) stammt noch aus einer Zeit, in der die analoge Vermittlungstechnik vorherrschte, nicht für jedes Gespräch personenbezogene Verbindungsdaten erzeugt wurden und die Telekommunikationsdienste in wesentlich geringerem Maße als heute genutzt wurden. Die Vorschrift erlaubt auch Zugriffe auf Verbindungsdaten wegen unbedeutenden Straftaten, bei denen eine inhaltliche Überwachung der Telekommunikation unzulässig wäre. Unter Berücksichtigung der Digitaltechnik, der vollständigen Datenerfassung und der Möglichkeit zur Bildung von Verhaltensprofilen verstößt § 12 FAG daher gegen den Verhältnismäßigkeitsgrundsatz und ist somit nicht mehr geeignet, Eingriffe in das Telekommunikationsgeheimnis zu rechtfertigen.

In einem früheren Gesetzesentwurf war vorgesehen, den Zugriff auf Verbindungsdaten grundsätzlich auf nicht unerhebliche Straftaten zu beschränken. Beschlossen wurde aber lediglich die unveränderte Fortgeltung des § 12 FAG, zuletzt befristet bis zum 31. Dezember 1999. Nunmehr wollen der Bundesrat und die Justizministerkonferenz die Befristung für die Weitergeltung dieser Vorschrift aufheben und es damit beim bisherigen, verfassungsrechtlich bedenklichen Rechtszustand belassen.

Die Datenschutzbeauftragten des Bundes und der Länder wenden sich entschieden gegen eine Verlängerung der Geltungsdauer des § 12 FAG und fordern stattdessen eine Neufassung der Eingriffsbefugnis unter Beachtung der grundrechtlichen Bindungen und Anforderungen, die sich aus dem von Art. 10 Grundgesetz geschützten Telekommunikationsgeheimnis ergeben.

Die gesetzliche Ermächtigung für den Zugriff auf Verbindungsdaten gehört sachlich in die Strafprozessordnung. Die gesetzlichen Zugriffsvoraussetzungen sollten in Abstimmung mit § 100 a StPO neu geregelt werden.

16.1.8 Entschließung der 60. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 12./13. Oktober 2000 in Braunschweig: Vom Bürgerbüro zum Internet - Empfehlungen zum Datenschutz für eine serviceorientierte Verwaltung

Bei der Modernisierung der öffentlichen Verwaltung soll insbesondere die Dienstleistungs- und Serviceorientierung verbessert werden. Dazu sollen unter anderem Dienstleistungen in multifunktionalen Servicecentern (Bürgeramt, Bürgerbüro, Bürgerladen, Kundencenter) gebündelt und die Möglichkeiten der modernen Informations- und Kommunikations-Technik intensiver genutzt werden (Information,

Kommunikation und Transaktion über das Internet, Einrichtung von Call-Centern). Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder unterstützt alle Bemühungen, den Kontakt von Bürgerinnen und Bürgern mit den Verwaltungen schneller, einfacher, effektiver und insbesondere transparenter zu machen. Die Datenschutzbeauftragten erklären daher ihre ausdrückliche Bereitschaft, solche Entwicklungsprozesse konstruktiv zu begleiten.

Es ist aber unerlässlich, dass bei allen Lösungen eine sichere und vertrauliche Kommunikation zwischen Verwaltung und Bürgern sowie ein angemessener Schutz personenbezogener Daten gewährleistet wird. Nur Serviceangebote, die dem Recht auf informationelle Selbstbestimmung gerecht werden, nützen letztlich sowohl Bürgerinnen und Bürgern als auch der Verwaltung selbst.

Eine Arbeitsgruppe der Konferenz der Datenschutzbeauftragten des Bundes und der Länder erarbeitet deshalb Empfehlungen zum Datenschutz für eine serviceorientierte Verwaltung. Diese Empfehlungen sollen den Verwaltungen helfen, bei der Verbesserung ihrer Dienstleistungs- und Serviceorientierung den Forderungen nach Datenschutz und Datensicherheit gerecht zu werden. Diese Empfehlungen werden demnächst veröffentlicht und entsprechend der rechtlichen und technischen Entwicklung fortgeschrieben.

16.1.9 Entschließung der 60. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 12./13. Oktober 2000 in Braunschweig zur Datensparsamkeit bei der Rundfunkfinanzierung

Die Finanzierung des öffentlich-rechtlichen Rundfunks ist derzeit Gegenstand öffentlicher Diskussion in der Politik und unter den Rundfunkanstalten selbst. Erörtert wird hierbei auch, ob die Erhebung von Rundfunkgebühren, die an das „Bereithalten eines Rundfunkempfangsgerätes“ anknüpfen, im Hinblick auf veränderte Gerätetechniken und bestehende Mängel im Verfahren modifiziert oder durch andere Finanzierungsformen ersetzt bzw. ergänzt werden sollte.

Künftig wird kaum noch überschaubar sein, welche Geräte zum Rundfunkempfang geeignet sind. Über die eigentlichen Fernseh- und Rundfunkgeräte hinaus ist dies bereits heute beispielsweise mit Personalcomputern, die über einen Internetzugang verfügen, oder mit bestimmten Mobiltelefonen möglich. In naher Zukunft werden neue Technologien wie UMTS weitere Empfangsmöglichkeiten eröffnen. Sofern der Besitz derartiger multifunktionaler Geräte zum Kriterium für die Rundfunkgebührenpflicht gemacht wird, würde das zu einer erheblichen Ausweitung von Datenabgleichen führen. Schon das gegenwärtig praktizierte Gebühreneinzugsverfahren erfordert in großem Umfang die Verarbeitung personenbezogener Daten. Nach den Angaben der Rundfunkanstalten meldet ein signifikanter Teil der Rundfunkteilnehmerinnen und -teilnehmer trotz der Verpflichtung hierzu seine Geräte nicht an. Um möglichst alle Gebührenpflichtigen zu erfassen, nutzen die Rundfunkanstalten Daten aus dem Melderegister, vom privaten Adresshandel und setzen vor Ort Rundfunkgebührenbeauftragte ein, die einzelne Haushalte aufsuchen. Damit wird in

unverhältnismäßiger Weise in das Recht auf informationelle Selbstbestimmung vieler gesetzestreuer Bürgerinnen und Bürger eingegriffen.

Die Datenschutzbeauftragten des Bundes und der Länder fordern die Bundesländer auf, einer Neuordnung ein Modell zu Grunde zu legen, das sich stärker als das bestehende System der Rundfunkfinanzierung an den Prinzipien der Datenvermeidung, Datensparsamkeit und Dezentralisierung orientiert. Nach ihrer Überzeugung lässt sich die verfassungsrechtlich gebotene Staatsferne und Funktionsfähigkeit des öffentlich-rechtlichen Rundfunks auch mit anderen, das Recht auf informationelle Selbstbestimmung weniger stark einschränkenden Finanzierungsmodellen als dem derzeit praktizierten gewährleisten.

16.1.10 Entschließung der 60. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 12./13. Oktober 2000 in Braunschweig zu datenschutzrechtlichen Konsequenzen aus der Entschlüsselung des menschlichen Genoms

Bei der Entschlüsselung des menschlichen Genoms sind in den letzten Monaten wohl entscheidende Durchbrüche gelungen. Für mehr als 20, oft vererbliche Krankheiten sind bereits Gentests zu erwerben, mit denen in Labors analysiert werden kann, ob eine Erkrankung vorliegt bzw. in welchem Umfang ein Erkrankungsrisiko besteht. Viele dieser Krankheiten sind allerdings bisher nicht heil- oder behandelbar.

Gentechnische Untersuchungen beim Menschen eröffnen den Zugang zu höchstpersönlichen und hochsensiblen Informationen in einem Maße, das die Intensität bisheriger personenbezogener Informationen ganz erheblich übersteigt. Durch den genetischen Einblick in den Kernbereich der Privatsphäre, etwa in Gesundheitsdisposition, Anlagen der Persönlichkeitsstruktur oder den voraussichtlichen Lebensverlauf, entsteht eine ganz neue Qualität des Wissens und des Offenlegens von persönlichsten Daten. Sowohl für die Betroffenen als auch für dritte Personen, insbesondere Familienangehörige, ist es von entscheidender Bedeutung, ob und inwieweit sie selbst und wer außer ihnen von den Ergebnissen Kenntnis bekommt. Davor steht die Frage, ob und aus welchen Anlässen überhaupt genetische Untersuchungen am Menschen vorgenommen werden dürfen. Zur informationellen Selbstbestimmung gehört auch das Recht auf Nichtwissen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert, dass für die Zulässigkeit gentechnischer Untersuchungen beim Menschen und für den Umgang mit den dabei gewonnenen Informationen sehr schnell klare und verbindliche Prinzipien entwickelt werden, um auch die informationelle Selbstbestimmung in diesem Kernbereich zu sichern und zugleich eine „genetische Diskriminierung“ bei der Gewinnung oder Verwendung genetischer Informationen, etwa im Arbeitsverhältnis oder beim Abschluss von Versicherungsverträgen zu verhindern. Auf der Grundlage dieser und in der „Entschließung über Genomanalyse und informationelle Selbstbestimmung“ vom 26. Oktober 1989 formulierten Grundsätze wird die Konferenz an der Ausgestaltung mitwirken.

Die Datenschutzbeauftragten erinnern an ihre Grundsätze aus der Entschließung von 1989 bezüglich der Genomanalyse:

1. Die Genomanalyse darf grundsätzlich nur auf freiwilliger Basis nach umfassender Aufklärung der Betroffenen vorgenommen werden; ausgenommen sind Straf- und Abstammungsverfahren.

2. Die jederzeit widerrufliche Einwilligung muss sich auch auf die weitere Verwendung der gentechnischen Informationen erstrecken. Im Falle eines Widerrufs sind die gewonnenen Informationen zu löschen oder an den Betroffenen herauszugeben.

3. Jede Genomanalyse muss zweckorientiert vorgenommen werden. Es ist diejenige genomanalytische Methode zu wählen, die keine oder die geringste Menge an Überschussinformationen bringt. Überschussinformationen sind unverzüglich zu vernichten.

4. Es ist zu prüfen, inwieweit genomanalytische Untersuchungsmethoden einer staatlichen Zulassung bedürfen. Für DNA-Sonden ist dies jedenfalls zu bejahen.

5. Die Genomanalyse im gerichtlichen Verfahren muss auf die reine Identitätsfeststellung beschränkt werden; es dürfen keine genomanalytischen Methoden angewandt werden, die Überschussinformationen zur Person liefern. Die Nutzung der Genomanalyse im Strafverfahren setzt eine normenklare gesetzliche Ermächtigung voraus. Präzise Regelungen müssen u.a. sicherstellen, dass genomanalytische Befunde einer strengen Zweckbindung unterworfen werden.

6. Im Arbeitsverhältnis sind die Anordnung von Genomanalysen oder die Verwendung ihrer Ergebnisse grundsätzlich zu verbieten. Ausnahmen bedürfen der gesetzlichen Regelung. Eine bloße Einwilligung des Arbeitnehmers ist wegen der faktischen Zwangssituation, der er im Arbeitsleben häufig unterliegt, nicht ausreichend.

7. Genomanalysen im Versicherungswesen sind grundsätzlich nicht erforderlich und mit dem Prinzip der Versicherungen, Risiken abzudecken und nicht auszuschließen, unvereinbar. Dies sollte durch eine Klarstellung im Versicherungsvertragsgesetz deutlich gemacht werden.

8. Im Rahmen der pränatalen Diagnostik dürfen nur Informationen über das Vorhandensein oder Fehlen von Erbanlagen erhoben werden, bei denen eine Schädigung heilbar ist oder die zu einer so schwerwiegenden Gesundheitsschädigung des Kindes führen würden, dass ein Schwangerschaftsabbruch straffrei bliebe.

   Reihenuntersuchungen an Neugeborenen dürfen sich nur auf solche Erbkrankheiten erstrecken, die bei frühzeitiger Erkennung eines genetischen Defekts geheilt oder zumindest spürbar therapeutisch begleitet werden können.

Die Eltern müssen nach umfassender fachkundiger Beratung in voller Freiheit über die Anwendung genomanalytischer Methoden entscheiden können. Jegliche Beeinflussung, insbesondere jeder individuelle und gesellschaftliche Druck, muss vermieden werden.

Die informationelle Selbstbestimmung Dritter, zu der auch das Recht auf Nichtwissen gehört, muss berücksichtigt werden. Demnächst werden nicht nur – wie bisher – Gensequenzen aufgedeckt und verglichen, sondern auch die mit dem Genom verbundenen Wirkungszusammenhänge für die menschliche Gesundheit und für die Persönlichkeitsstruktur entschlüsselt werden können.

16.1.11 Entschließung der 60. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 12./13. Oktober 2000 in Braunschweig zur Novellierung des BDSG

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert an Bundestag und Bundesrat, das Gesetzgebungsverfahren eines novellierten Bundesdatenschutzgesetzes zügig und ohne Abstriche zum Abschluss zu bringen. Damit wird die längst überfällige Anpassung des deutschen Datenschutzrechts an die Vorgaben der EG-Richtlinie vorgenommen. Die Novelle enthält verschiedene innovative Ansätze, insbesondere das Gebot zur Datenvermeidung und Datensparsamkeit bei der Systemgestaltung (Systemdatenschutz - § 3 a E-BDSG) und die Einführung des Datenschutzaudit (§ 9 a), die von den Datenschutzbeauftragten schon seit langem befürwortet werden.

Sowohl der Systemdatenschutz als auch das Datenschutzaudit werden die Durchsetzung datenschutzfreundlicher Lösungen im Wettbewerb erleichtern und tragen auf diese Weise zur Selbstregulierung des Marktes bei. Das Datenschutzaudit fügt sich in die bewährten Strukturen des betrieblichen Datenschutzes ein und ermöglicht es den Unternehmen, datenschutzkonforme Angebote und Verhaltensweisen nachprüfbar zu dokumentieren und damit einen Wettbewerbsvorsprung zu gewinnen.

Die Konferenz fordert den Bundesrat auf, die Aufnahme des Datenschutzaudit in das BDSG nicht zu blockieren. Sie geht weiter davon aus, dass die angekündigte zweite Stufe der Novellierung des BDSG noch in dieser Legislaturperiode realisiert wird, und erklärt ihre Bereitschaft, hieran konstruktiv mitzuwirken.

16.1.12 Entschließung zwischen der 59. und 60. Konferenz der Datenschutzbeauftragten des Bundes und der Länder zur Auftragsdatenverarbeitung durch das Bundeskriminalamt

Im Rahmen der Neukonzeption des polizeilichen Informationssystems INPOL ist geplant, neben bundesweit verfügbaren Verbunddaten auch Landesdatenbestände im Wege der Auftragsdatenverarbeitung logisch getrennt in der INPOL-Datenbank zu

speichern. Zudem sollen aufgrund bilateraler Absprachen landesspezifische Informationen in bestimmtem Umfang gespeichert werden können und ebenso gegenseitige Zugriffe einzelner Länder auf die Datenbestände ermöglicht werden.

§ 2 Abs. 5 des Bundeskriminalamtgesetzes lässt grundsätzlich eine Unterstützung der Länder bei deren Datenverarbeitung auf Ersuchen, also in Einzelfällen, zu. Diese Vorschrift kann auch herangezogen werden, wenn aufgrund besonderer Dringlichkeit, wie gegenwärtig bei der Realisierung von INPOL-neu, eine zeitlich befristete Auftragsdatenverarbeitung von Landesdaten geplant ist. Hierzu sind Ende vergangenen Jahres entsprechende Beschlüsse des Arbeitskreises II und der Innenministerkonferenz gefasst worden.

Diese Entwicklung birgt aus der Sicht der Datenschutzbeauftragten die Gefahr, dass weitere Beschlüsse folgen werden, die die dauerhafte Speicherung von Landesdaten beim BKA begründen; bereits jetzt sind Tendenzen deutlich, die zentralisierte Speicherung der Daten auch zur Erleichterung der gegenseitigen Zugriffe auf Landesdaten zu nutzen.

Die Notwendigkeit der zentralen Datenspeicherung beim Bundeskriminalamt wird im Wesentlichen mit Kosten- und Zeitargumenten begründet. Diese sind jedoch aus datenschutzrechtlicher Sicht nicht geeignet, eine Erweiterung der zentralen Datenverarbeitung beim Bundeskriminalamt zu begründen.

Die dauerhafte zentrale Datenhaltung beim BKA würde die informationelle Trennung von Landesdaten und Verbunddaten aufweichen; die in § 2 Abs. 1 BKA-Gesetz statuierte Schwelle, dass nur Daten über Straftaten von länderübergreifender, internationaler oder sonst erheblicher Bedeutung beim BKA verarbeitet werden dürfen, würde schleichend umgangen.

Eine dauerhafte zentrale Landesdatenhaltung beim Bundeskriminalamt beinhaltet eine neue, bei der augenblicklichen Rechtslage unakzeptable Qualität polizeilicher Datenverarbeitung.

Die Datenschutzbeauftragten des Bundes und der Länder fordern dazu auf, die für die Datenverarbeitung beim Bundeskriminalamt gesetzlich gezogenen Grenzen strikt zu beachten. Sie appellieren an die Innenminister/-senatoren von Bund und Ländern, an den bisherigen Beschlüssen festzuhalten und die Polizeien der Länder, wie ursprünglich geplant, aufzufordern, unverzüglich eigene Datenverarbeitungsverfahren zu entwickeln. Bis zur Realisierung dieser Verfahren könnte allenfalls eine übergangsweise Lösung als Auftragsdatenverarbeitung unter Wahrung datenschutzrechtlicher Anforderungen ermöglicht werden. Daneben steht das Angebot des Bundeskriminalamtes, kostenlos Software von INPOL-neu zur Verfügung zu stellen. Diese Lösung würde auch das vorgetragene Kostenargument entkräften.

16.1.13 Entschließung zwischen der 59. und 60. Konferenz der Datenschutzbeauftragten des Bundes und der Länder zu effektiver parlamentarischer Kontrolle von Lauschangriffen durch aussagekräftige jährliche Berichte der Bundesregierung

Die Bundesregierung hat den Bundestag jährlich über die nach Art. 13 Abs. 3 GG zur Strafverfolgung eingesetzten „Großen Lauschangriffe“ zu unterrichten. § 100 e StPO konkretisiert die Berichtspflicht dahingehend, dass die Bundesregierung aufgrund von Mitteilungen der Staatsanwaltschaften der Länder den Bundestag über Anlass, Umfang, Dauer, Ergebnis und Kosten der Maßnahmen zu unterrichten hat.
Diese Berichte sollen eine laufenden parlamentarische Kontrolle dieser mit intensiven Grundrechtseingriffen verbundenen Maßnahmen ermöglichen. Der Bundestag soll aufgrund der Berichte in die Lage versetzt werden, die Angemessenheit und Eignung der Maßnahme zu überprüfen.
Diesen Anforderungen wird der erste von der Bundesregierung vorgelegte Bericht nicht in vollem Umfang gerecht. So wurde nur die Gesamtzahl der von der Anordnung Betroffenen erfasst, wobei zwischen Beschuldigten und nicht beschuldigten Wohnungsinhabern unterschieden wird.

Nach § 100 e Abs. 1 StPO muss über den Umfang der Maßnahme berichtet werden. Hierzu zählt die Angabe über die Anzahl aller von der Maßnahme betroffenen Personen, nicht nur der in der gerichtlichen Anordnung genannten. Von dem „Großen Lauschangriff“ ist jeder betroffen, dessen gesprochenes Wort in der Wohnung abgehört wird. Er greift auch in die grundrechtlich geschützten Rechte der am Verfahren Unbeteiligten, wie z.B. unverdächtige Familienangehörige, Bekannte, Besucherinnen und Besucher sowie sonstige Personen, die nicht selbst Wohnungsinhaber sind, ein. Dem wollte der Gesetzgeber mit der Einführung der Berichtspflicht Rechnung tragen.

Die Beschränkung der Berichtspflicht auf Wohnungsinhaber und Beschuldigte gibt nicht den wirklichen Umfang der von der Maßnahme betroffenen Personen wieder. Somit erfüllt sie den Zweck der im Grundgesetz vorgesehenen Berichtspflicht nicht.

Darüber hinaus wäre es wünschenswert, wenn – wie in den „Wire-tap-Reports“ der USA – die Anzahl der abgehörten Gespräche und die Anzahl der Gespräche, die mit dem Ermittlungsverfahren in Zusammenhang stehen, die Art der betroffenen Räume (Geschäftsräume, Wohnung, Restaurant etc.), die Anzahl und Dauer der angeordneten Verlängerungen der Maßnahme, die Zahl der Verhaftungen, Anklageerhebungen und Verurteilungen, zu denen die Maßnahme beigetragen hat, angegeben werden.

Die Länder haben nach Art. 13 Abs. 6 Satz 3 GG eine gleichwertige parlamentarische Kontrolle zu gewährleisten. Die oben genannten Forderungen gelten deshalb gleichermaßen bzw. in entsprechender Weise für die den Landesparlamenten vorzulegenden jährlichen Berichte über die nach § 100 c Abs. 1 Nr. 3 StPO durchgeführten Maßnahmen bzw. über die von der Polizei zur Gefahrenabwehr veranlassten „Großen Lauschangriffe“.

16.1.14 Entschließung der 61. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8./9. März 2001 in Düsseldorf zum Datenschutz beim elektronischen Geschäftsverkehr

Die Konferenz wendet sich mit Entschiedenheit gegen Anträge, die gegenwärtig dem Bundesrat zum Entwurf eines Gesetzes zum elektronischen Geschäftsverkehr (BR-Drs. 136/01) vorliegen. Danach sollen Bestands- und Nutzungsdaten bei Telediensten nicht nur an Strafverfolgungsbehörden, sondern auch an Verwaltungsbehörden zur Verfolgung von Ordnungswidrigkeiten und an Nachrichtendienste übermittelt werden. Darüber hinaus sollen die Anbieterinnen und Anbieter zur Speicherung von Nutzungsdaten auf Vorrat für eine mögliche spätere Strafverfolgung verpflichtet werden.

Die Datenschutzbeauftragten weisen darauf hin, dass sich anhand dieser Daten nachvollziehen lässt, wer wann mit wem kommuniziert hat, wer welches Medium genutzt hat und damit wer welchen weltanschaulichen, religiösen und sonstigen persönlichen Interessen nachgeht. Eine pauschale Registrierung jeder Inanspruchnahme von Telediensten zur staatlichen Überwachung greift tief in das Persönlichkeitsrecht der betroffenen Nutzerinnen und Nutzer ein und berührt auf empfindliche Weise deren Informationsfreiheit. Der Bundesrat wird daher aufgefordert, diese Anträge abzulehnen.

16.1.15 Entschließung der 61. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8./9. März 2001 in Düsseldorf zur Novellierung des G 10-Gesetzes

Die Datenschutzbeauftragten des Bundes und der Länder sehen mit großer Sorge, dass die Empfehlungen des Rechts- und des Innenausschusses des Bundesrates erhebliche Einschränkungen der Persönlichkeitsrechte der Bürgerinnen und Bürger zur Folge hätten, die über den Gesetzentwurf der Bundesregierung teilweise weit hinausgehen. Die Datenschutzbeauftragten wenden sich insbesondere entschieden dagegen, dass

- die Befugnisse der Nachrichtendienste zur Übermittlung und Verwendung von G 10-Daten an Strafverfolgungsbehörden gegenüber dem Gesetzentwurf noch deutlich erweitert werden sollen, indem Erkenntnisse der Nachrichtendienste u.a. zur Strafverfolgung weit über die Schwerkriminalität hinaus genutzt werden dürften,

- der Verzicht auf die Kennzeichnung von G 10-Daten sogar ohne vorherige Zustimmung der G 10-Kommission zulässig sein und

- die Schwelle dafür, endgültig von der Benachrichtigung Betroffener abzusehen, deutlich herabgesetzt werden soll.

Darüber hinaus kritisieren die Datenschutzbeauftragten des Bundes und der Länder, dass die Bundesregierung mit der Gesetzesnovelle über die Vorgaben des BVerfG

hinaus weitere Änderungen im G 10-Bereich erreichen will, die neue grundrechtliche Beschränkungen vorsehen:

- Die Anforderungen an die halbjährlichen Berichte des zuständigen Bundesministers an die PKG müssen so gefasst werden, dass eine wirksame parlamentarische Kontrolle erreicht wird. Dies ist derzeit nicht gewährleistet. Deshalb muss über Anlass, Umfang, Dauer, Ergebnis und Kosten aller Maßnahmen nach dem G 10-Gesetz sowie über die Benachrichtigung der Beteiligten berichtet werden. Die gleichen Anforderungen müssen auch für die Berichte der PKG an den Bundestag gelten.

- Die Neuregelung, nach der auch außerhalb der Staatsschutzdelikte mutmaßliche Einzeltäter und lose Gruppierungen den Maßnahmen nach dem G 10-Gesetz unterliegen sollen, stellt das Trennungsgebot nach Art. 87 Abs. 1 Satz 2 GG weiter infrage. Ermittlungen von der Eingriffsschwelle eines konkreten Anfangsverdachts zu lösen und nach nachrichtendienstlicher Art schon im Vorfeld zur Verdachtsgewinnung durchzuführen, weitet die Gefahr unverhältnismäßig aus, dass auch gegen Unbescholtene strafrechtlich ermittelt wird.

- Alle Neuregelungen wie z.B. zum Parteienverbotsverfahren, zur Verwendung von G 10-Erkenntnissen bei Gefahren für Leib oder Leben einer Person im Ausland und zu Spontanübermittlungen an den BND müssen befristet und einer effizienten Erfolgskontrolle unterzogen werden.

- Bei der internen Datenverarbeitung durch die Nachrichtendienste ist die Zweckbindung so zu formulieren, dass die erhobenen Daten nicht zur Erforschung und Verfolgung anderer als der in § 3 und § 5 G 10-E genannten Straftaten genutzt werden dürfen.

- Die vorgesehenen Ausnahmen von der vom BVerfG geforderten Kennzeichnungspflicht bei der Übermittlung von Daten, die aus G 10-Maßnahmen stammen, begegnen schwerwiegenden datenschutzrechtlichen Bedenken.

- Im Gesetzentwurf fehlt die Regelung, dass eine Weiterübermittlung an andere Stellen und Dritte nicht zulässig ist. Sie darf nur durch die erhebende Stelle erfolgen. Die Weitergabe von G 10-Daten an andere Dienststellen ist bei der übermittelnden Stelle stets zu dokumentieren und zu kennzeichnen.

- Eine dauerhafte Ausnahme von der Benachrichtigungspflicht ist abzulehnen. Sie würde für die Betroffenen zu einem Ausschluss des Rechtsweges führen.

- Dem BND wird nicht mehr nur die „strategische Überwachung“ des nichtleitungsgebundenen, sondern künftig des gesamten internationalen Telekommunikationsverkehrs ermöglicht. Dies setzt den Zugriff deutscher Stellen auf Telekommunikationssysteme in fremden Hoheitsbereichen voraus. Dabei muss sichergestellt werden, dass die Anforderungen des Völkerrechts eingehalten werden.

- Die Überwachung internationaler Telekommunikationsbeziehungen im Falle einer Gefahr für Leib oder Leben einer Person im Ausland (§ 8 G 10-E) ermöglicht sehr intensive Grundrechtseingriffe in großer Zahl und mit einer hohen Dichte, die höher sein kann als bei „strategischen Überwachung“ nach § 5 G 10-E. Dies setzt eine hohe Eingriffsschwelle und enge zeitliche Befristung voraus, die der Entwurf nicht hinreichend vorsieht.

16.1.16 Entschließung der 61. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8./9. März 2001 in Düsseldorf zum Datenschutz bei der Bekämpfung von Datennetzkriminalität

Der Europarat entwirft gegenwärtig zusammen mit anderen Staaten, insbesondere den USA und Japan, eine Konvention über Datennetzkriminalität (Cyber-crime-Konvention), die über ihren Titel hinaus auch die automatisierte Speicherung von Daten im Zusammenhang mit anderen Straftaten regeln soll.[1]

Die Datenschutzbeauftragten des Bundes und der Länder verkennen nicht, dass das Internet – ebenso wie andere technische Hilfsmittel – für Straftaten missbraucht wird. Sie teilen daher die Auffassung des Europarats, dass der Kriminalität auch im Internet wirksam begegnet werden muss. Allerdings ist zu beachten, dass sich die weit überwiegende Anzahl der Nutzenden an die gesetzlichen Vorgaben hält. Insoweit stellt sich die Frage der Verhältnismäßigkeit von Maßnahmen, die alle Nutzenden betreffen.

Die Datenschutzbeauftragten des Bundes und der Länder teilen die Auffassung der Europäischen Kommission, dass zur Schaffung einer sichereren Informationsgesellschaft in erster Linie die Sicherheit der Informationsinfrastruktur verbessert werden und anonyme wie pseudonyme Nutzungsmöglichkeiten erhalten bleiben müssen; über Fragen der Bekämpfung der Datennetzkriminalität sollte ein offener Diskussionsprozess unter Einbeziehung der Betreiberinnen und Betreiber, Bürgerrechtsorganisationen, Verbraucherverbände und Datenschutzbeauftragten geführt werden.[2]

Die Konferenz regt eine entsprechende Debatte auch auf nationaler Ebene an und bittet die Bundesregierung, hierfür den erforderlichen Rahmen zu schaffen.

Die Konferenz der Datenschutzbeauftragten fordert die Bundesregierung auf, sich bei der Schaffung von nationalen und internationalen Regelungen zur Bekämpfung von Datennetzkriminalität dafür einzusetzen, dass

[1] European Committee on Crimes Problems (CDPC), Committee of Experts on Crime in Cyber-Space (PC-CY), Draft Convention on Cyber-crime (PC-CY (2000) Draft No. 25).

[2] Mitteilung der Kommission an den Rat, das Europäische Parlament, den Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen vom 26.01.2001 – KOM (2000) 890 endgültig.

- Maßnahmen zur Identifikation von Internet-Nutzenden, zur Registrierung des Nutzungsverhaltens und Übermittlung der dabei gewonnenen Daten für Zwecke der Strafverfolgung erst dann erfolgen dürfen, wenn ein konkreter Verdacht besteht,

- der Datenschutz und das Fernmeldegeheimnis gewährleistet und Grundrechtseingriffe auf das unabdingbare Maß begrenzt werden,

- der Zugriff und die Nutzung personenbezogener Daten einer strikten und eindeutigen Zweckbindung unterworfen werden,

- Daten von Internet-Nutzenden nur in Länder übermittelt werden dürfen, in denen ein angemessenes Niveau des Datenschutzes, des Fernmeldegeheimnisses und der Informationsfreiheit gewährleistet ist sowie verfahrensmäßige Garantien bei entsprechenden Eingriffen bestehen.

16.1.17 Entschließung der 61. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8./9. März 2001 in Düsseldorf zum Äußerungsrecht der Datenschutzbeauftragten

Die Datenschutzbeauftragten des Bundes und der Länder sind verpflichtet, Einzelne – wie es die Rechtsprechung des Bundesverfassungsgerichts und die Richtlinie der Europäischen Gemeinschaft zum Datenschutz von 1995 vorsehen – vor rechtswidrigem Umgang mit ihren personenbezogenen Daten wirksam zu schützen. Die damit verbundenen Beratungs- und Kontrollaufgaben verleihen den Datenschutzbeauftragten ein öffentliches Wächteramt, das die Befugnis einschließt, Behördenverhalten auch im Detail und, soweit der Bedeutung der Sache angemessen, auch unter Bezeichnung der Amtsträgerinnen und Amtsträger öffentlich zu rügen.

Aus gegebenem Anlass wendet sich die Konferenz der Datenschutzbeauftragten des Bundes und der Länder energisch gegen Versuche im Land Sachsen, durch gesetzgeberische Maßnahmen dieses Recht zu beschneiden und die Arbeit des Sächsischen Datenschutzbeauftragten zu behindern.

16.1.18 Entschließung der 61. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8./9. März 2001 in Düsseldorf zu Informationszugangsgesetzen

Die Konferenz verfolgt mit Interesse die Bestrebungen des Bundes, ein Informationszugangsgesetz zu schaffen und dem Bundesbeauftragten für den Datenschutz die Aufgaben zur Sicherung des Informationszugangs zu übertragen. Die Bundesregierung nimmt damit die Überlegungen auf, die in Artikel 255 EU-Vertrag und Artikel 42 EU-Grundrechte-Charta zum Ausdruck kommen. Die Konferenz betont, dass das Recht auf informationelle Selbstbestimmung der Einzelnen dem freien

Zugang zu behördeninternen, amtlichen Informationen nicht entgegen steht, wenn die Privatsphäre der Betroffenen sowie Betriebsgeheimnisse gesetzlich geschützt bleiben. Die Berichte aus den Ländern Berlin, Brandenburg und Schleswig-Holstein zeigen, dass die datenschutzrechtlichen Gewährleistungen für die informationelle Selbstbestimmung sich mit dem erweiterten Zugangsrecht zu den Informationen öffentlicher Stellen unter der Voraussetzung entsprechender Schutzmechanismen vereinbaren lassen. Die Zusammenführung von Datenschutz- und Informationszugangskontrolle kann diese Gewährleistung institutionell absichern.

16.1.19 Entschließung der 61. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8./9. März 2001 in Düsseldorf zur Novellierung des Melderechtsrahmengesetzes

Die Datenschutzbeauftragten des Bundes und der Länder begrüßen die Absicht der Bundesregierung, das Melderechtsrahmengesetz im Hinblick auf die neuen Informations- und Kommunikationstechnologien zu modernisieren und einzelne unnötige Meldepflichten abzuschaffen.

1. Allerdings sind aus dem vorliegenden Gesetzentwurf Tendenzen zu erkennen, dass durch den Zusammenschluss mehrerer Melderegister übergreifende Dateien entstehen können, die letztlich sogar zu einem zentralen Melderegister führen würden. Eine solche Entwicklung wäre aus datenschutzrechtlicher Sicht nicht hinnehmbar, weil damit das Recht auf informationelle Selbstbestimmung der Bürgerinnen und Bürger unverhältnismäßig eingeschränkt werden würde.

2. Bereits die bisherige Rechtslage, nach der nahezu jedermann eine einfache Melderegisterauskunft von der Meldebehörde erhalten kann, ist äußerst unbefriedigend. Dies wird dadurch verschärft, dass der Gesetzentwurf - wie in seiner Begründung ausdrücklich betont wird – nunmehr vorsieht, einfache Melderegisterauskünfte mit Hilfe des Internet durch jedermann auch elektronisch abrufen zu können. Um sich gegen eine unkontrollierte Weitergabe solcher über das Internet zum Abruf bereitgehaltener Daten schützen zu können und weil beim Internet-gestützten Abruf die gesetzlich vorgeschriebene Berücksichtigung der schutzwürdigen Belange Betroffener nicht möglich ist, sollte für die Bürgerin oder den Bürger in diesen Fällen ein ausdrückliches Einwilligungsrecht oder mindestens ein Widerspruchsrecht geschaffen werden. Es handelt sich hier um personenbezogene Daten, die auf der Grundlage einer gesetzlichen Auskunftspflicht erhoben wurden.

3. Auch für öffentliche Stellen sollte in das Gesetz eine Bestimmung aufgenommen werden, wonach bei elektronischen Abrufverfahren über das Internet zur Wahrung der schutzwürdigen Interessen der Betroffenen zumindest Verfahren der fortgeschrittenen elektronischen Signatur gemäß den Regelungen des Signaturgesetzes einzusetzen sind.

4. Nach geltendem Recht ist jede Melderegisterauskunft unzulässig, wenn eine Gefahr für Leben, Gesundheit, persönliche Freiheit oder ähnliche schutzwürdige Belange glaubhaft gemacht wird. Diese Regelung hat sich bewährt. Die Datenschutzbeauftragten treten angesichts des in diesen Fällen bestehenden hohen Schutzbedarfs dem Vorhaben entschieden entgegen, diese Regelung durch eine Risikoabwägung im Einzelfall aufzuweichen.

5. Bislang dürfen Meldebehörden an Parteien, Wählergruppen und andere Träger von Wahlvorschlägen Auskunft über Daten von Gruppen von Wahlberechtigten erteilen, sofern die Wahlberechtigten dieser Auskunftserteilung nicht widersprochen haben. Die Datenschutzbeauftragten bekräftigen ihre bereits in der Vergangenheit erhobene Forderung, gesetzlich zu regeln, dass eine Einwilligung der Betroffenen Voraussetzung für solche Datenweitergaben sein muss. Die bisherige Widerspruchslösung ist in weiten Kreisen der Bevölkerung unbekannt.

6. Außerdem fordern die Datenschutzbeauftragten, die Hotelmeldepflicht abzuschaffen, da die hiermit verbundene millionenfache Datenerhebung auf Vorrat unverhältnismäßig ist.

Bei Enthaltung Thüringens zu Ziffer 6.

16.2 Sonstiges

Vordruck „Inanspruchnahme von Elternzeit nach § 16 Abs. 1 BErzGG für Arbeitnehmerinnen und Arbeitnehmer

Familienname, Vorname
Anschrift
Ort, Datum[1]

Inanspruchnahme von Elternzeit nach § 16 Abs. 1 BErzGG
für Arbeitnehmerinnen und Arbeitnehmer

An Dienststelle: _____

Ich beanspruche Elternzeit für das Kind

Familienname, Vorname _____ Geburtsdatum: _____

Angaben zum Kind:

☐ Personensorge steht mir zu

☐ leibliches Kind, für das mir die Personensorge nicht zusteht

☐ Kind des Ehegatten

☐ in meine Adoptionspflege aufgenommenes Kind seit _____

☐ Es liegt ein besonderer Härtefall gem. § 1 Abs. 5 BErzGG vor. Vormundschaftsverhältnis zum Kind: _____

☐ das Kind lebt in meinem Haushalt

☐ es wird von mir selbst betreut und erzogen[2]

Eine beglaubigte Kopie der Geburtsurkunde ☐ habe ich bereits zugesandt ☐ füge ich bei

Zeitraum / Zeiträume der Elternzeit[3]

☐ Meine Elternzeit

☐ Der erste Teil meiner Elternzeit soll **beginnen** am _____, d. h.

☐ im Anschluss an die Mutterschutzfrist nach der Entbindung,

☐ nach Beendigung des / der zurzeit laufenden Erziehungsurlaubs / Elternzeit für ein früher geborenes Kind,

☐ ab dem Zeitpunkt der Inobhutnahme des Kindes,

☐ nach Beendigung des Zeitraums der Elternzeit, die mein Ehegatte in Anspruch genommen hat,

☐ _____

☐ Meine Elternzeit soll **enden** mit Ablauf der

☐ vollen Elternzeit (Tag, an dem das Kind 36[4] Monate alt wird) _____

☐ - verkürzten Elternzeit - _____

☐ Das Ende meiner Elternzeit steht noch nicht fest, weil ich einen Anteil von _____ Monaten mit Ihrer Zustimmung auf einen späteren Zeitpunkt, allerdings vor Vollendung des achten Lebensjahres des Kindes übertragen möchte[5].

☐ Der **erste** Zeitraum der Elternzeit soll **enden** mit Ablauf des _____

☐ Der **zweite** Zeitraum der Elternzeit soll **dauern** von _____ bis einschl. _____

☐ Der **dritte** Zeitraum der Elternzeit soll **dauern** von _____ bis einschl. _____

☐ Der **vierte** Zeitraum der Elternzeit soll **dauern** von _____ bis einschl. _____

Meine Erwerbstätigkeit während der Elternzeit:

☐ Ich werde von _____ bis _____ und von _____ bis _____ nicht erwerbstätig sein.

☐ Ich beabsichtige von _____ bis _____ und von _____ bis _____ im Umfang von _____ Wochenstunden teilzeitbeschäftigt

☐ zu werden ☐ zu bleiben[6].

☐ Ich beabsichtige, weiterhin nur für denselben Arbeitgeber zu arbeiten.

☐ Ich beantrage Ihre Zustimmung, im zulässigen Rahmen[7]

☐ bei einem anderen Arbeitgeber tätig zu werden ☐ als Selbständige/r tätig zu werden.

Falls sich die Verhältnisse ändern, werde ich Sie unverzüglich benachrichtigen.

_____

Unterschrift des Antragstellers

Anlagen:

☐ Geburtsurkunde oder Abstammungsurkunde

☐ Gerichtsentscheidung

☐ Zustimmung des anderen Elternteils (nur bei leiblichem Kind, für das dem Antragsteller die Personensorge nicht zusteht)

---

[1] Der Antrag muss spätestens 6 Wochen vor Beginn des Urlaubs gestellt werden, wenn die Elternzeit unmittelbar nach der Geburt des Kindes oder nach der Mutterschutzfrist begonnen werden soll, in anderen Fällen 8 Wochen früher.

[2] Die Betreuung durch andere Personen während der Zeit einer erlaubten Erwerbstätigkeit ist unschädlich, ebenso eine vorübergehende Unmöglichkeit der Betreuung (z. B. wegen Erkrankung des Betreuenden).

[3] Die Elternzeit von max. 3 Jahren pro Kind darf von den Elternteilen allein oder gemeinsam genommen und auf bis zu vier Zeitabschnitte verteilt werden. Arbeitnehmer/innen müssen die Elternzeit schriftlich verlangen und gleichzeitig erklären, für welche Zeiträume sie innerhalb von 2 Jahren ab Geburt bzw. Inobhutnahme des Kindes Elternzeit in Anspruch nehmen wollen (§ 16 Abs. 1 Satz 4 BErzGG).

[4] Für angenommene oder in Adoptionspflege genommene Kinder beginnt sie frühestens ab Inobhutnahme und dauert längstens bis zum 8. Geburtstag des Kindes.

[5] Ein Anteil der Elternzeit von bis zu 12 Monaten kann mit Zustimmung des Arbeitgebers auf die Zeit bis zur Vollendung des 8. Lebensjahres des Kindes übertragen werden.

[6] Grenze der zulässigen Erwerbstätigkeit nach § 15 Abs. 4 Satz 1 BErzGG: 30 Wochenstunden.

[7] § 15 Abs. 4 Satz 2 BErzGG.