Sächsischer Landtag
4. Wahlperiode

DRUCKSACHE 4/10370

Schutz des Persönlichkeitsrechts im öffentlichen Bereich

13. Tätigkeitsbericht

des

Sächsischen Datenschutzbeauftragten

Dem Sächsischen Landtag

vorgelegt zum 31. März 2007

gemäß § 30 des Sächsischen Datenschutzgesetzes

Eingegangen am: 14. Dezember 2007 Ausgegeben am: 14. Dezember 2007

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; sie erleichtert das Verständnis von Texten und hilft, sich auf das Wesentliche zu konzentrieren. 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.)

Herausgeber: Der Sächsische Datenschutzbeauftragte
Andreas Schurig
Bernhard-von-Lindenau-Platz 1 Postfach 12 07 05
01067 Dresden 01008 Dresden
Telefon: 0351/4935401
Fax : 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.

AGG	Allgemeines Gleichbehandlungsgesetz vom 14. August 2006 (BGBl. I S. 1897), zuletzt geändert durch Artikel 8 Abs. 1 des Gesetzes vom 2. Dezember 2006 (BGBl. I S. 2742)
AO	Abgabenordnung in der Fassung der Bekanntmachung vom 1. Oktober 2002 (BGBl. I S. 3866; 2003 I S. 61), zuletzt geändert durch Art. 5 des Gesetzes vom 10. Oktober 2007 (BGBl. I S. 2332)
AufentV	Aufenthaltsverordnung vom 25. November 2004 (BGBl. I S. 2945), zuletzt geändert durch Artikel 7 Abs. 4 des Gesetzes vom 19. August 2007 (BGBl. I S. 1970)
AufenthG	Aufenthaltsgesetz vom 30. Juli 2004 (BGBl. I S. 1950), zuletzt geändert durch Art. 1 des Gesetzes vom 19. August 2007 (BGBl. I S. 1970)
BaföG	Bundesausbildungsförderungsgesetz in der Fassung der Bekanntmachung vom 6. Juni 1983 (BGBl. I S. 645, 1680), zuletzt geändert durch Art. 4 Abs. 9 des Gesetzes vom 22. September 2005 (BGBl. I S. 2809)
BAT-O	Bundesangestelltentarifvertrag vom 23. Februar 1961 (GMBl. S. 137) Inkrafttreten am: 1. April 1961 (vgl. § 74 Abs. 1 BAT) Außerkrafttreten: 1. Oktober 2005; wurde am 1. Oktober 2005 durch einheitlichen Tarifvertrag öffentlicher Dienst (TVöD) für die Bundes- und Kommunalangestellten bzw. am 1. November 2006 durch den Tarifvertrag öffentlicher Dienst - Länderbereich (TV-L) ersetzt.
BDSG	Bundesdatenschutzgesetz in der Fassung der Bekanntmachung vom 14. Januar 2003 (BGBl. I S. 66), zuletzt geändert durch Art. 1 des Gesetzes vom 22. August 2006 (BGBl. I S. 1970)

BGB	Bürgerliches Gesetzbuch in der Fassung der Bekanntmachung vom 2. Januar 2002 (BGBl. I S. 42, 2909; 2003, BGBl. I S. 738), zuletzt geändert durch Art. 2 Abs. 16 des Gesetzes vom 19. Februar 2007 (BGBl. I S. 122)
BSHG	Bundessozialhilfegesetz in der Fassung der Bekanntmachung vom 23. März 1994 (BGBl. I S. 646, ber. S. 2975), zuletzt geändert durch Art. 7 des Gesetzes vom 23. Dezember 2002 (BGBl. I S. 4621)
BZRG	Bundeszentralregistergesetz in der Fassung der Bekanntmachung vom 21. September 1984 (BGBl. I S. 1229, 1985 BGBl. I S. 195), zuletzt geändert durch Art. 4 des Gesetzes vom 21. August 2007 (BGBl. I S. 2118)
EG-Datenschutz-Richtlinie	Richtlinie 95/46/EG des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr vom 24. Oktober 1995 (ABl. EG L 281 vom 23. November 1995, S. 31)
EntschG	Entschädigungsgesetz in der Fassung der Bekanntmachung vom 13. Juli 2004 (BGBl. I S. 1658), zuletzt geändert durch Art. 3 Abs. 14 des Gesetzes vom 12. Juli 2006 (BGBl. I S. 1466)
FPersG	Fahrpersonalgesetz in der Fassung der Bekanntmachung vom 19. Februar 1987 (BGBl. I S. 640), zuletzt geändert durch Gesetz vom 6. Juli 2007 (BGBl. I S. 1270)
FrTrSchulG	Gesetz über Schulen in freier Trägerschaft vom 4. Februar 1992 (GVBl. S. 37), zuletzt geändert durch Art. 7 des Gesetzes vom 15. Dezember 2006 (GVBl. S. 515, 519, ber. 2007 S. 25)
GewO	Gewerbeordnung in der Fassung der Bekanntmachung vom 22. Februar 1999 (BGBl. I S. 202), zuletzt geändert durch Art. 9 des Gesetzes vom 7. September 2007 (BGBl. I S. 2246)
GeschoSReg	Geschäftsordnung der Sächsischen Staatsregierung vom 22. März 2005 (SächsABl. S. 271)
GG	Grundgesetz für die Bundesrepublik Deutschland vom 23. Mai 1949, zuletzt geändert durch Gesetz vom 28. August 2006 (BGBl. I S. 2034)
GVGA	VwV des SMJus zu der Geschäftsanweisung für Gerichtsvollzieher und der Gerichtsvollzieherordnung (VwV GVGA, GVO) vom 28. Februar 2002 (SächsJMBl. S. 47)

HmbDSG	Hamburgisches Datenschutzgesetz vom 5. Juli 1990 (HmbGVBl. S. 133, 165, 226), zuletzt geändert am 18. November 2003 (HmbGVBl. S. 5)
HGB	Handelsgesetzbuch in der im Bundesgesetzblatt Teil III, Gliederungsnummer 4100-1, veröffentlichten bereinigten Fassung, zuletzt geändert durch Art. 10 des Gesetzes vom 16. Juli 2007 (BGBl. I S. 1330)
IHKG	Gesetz zur vorläufigen Regelung des Rechts der Industrie- und Handelskammern, bereinigte Fassung, zuletzt geändert durch Art. 7 vom 7. September 2007 (BGBl. I S. 2246)
InsO	Insolvenzordnung vom 5. Oktober 1994 (BGBl. I S. 2866), zuletzt geändert durch Art. 1 des Gesetzes vom 13. April 2007 (BGBl. I S. 509)
InsOBekV	Verordnung zu öffentlichen Bekanntmachungen in Insolvenzverfahren im Internet vom 12. Februar 2002 (BGBl. I S. 677), zuletzt geändert durch Art. 2 des Gesetzes vom 13. April 2007 (BGBl. I S. 509)
JGG	Jugendgerichtsgesetz vom: 4. August 1953 (BGBl. I S. 751), zuletzt geändert am 18. April 2007 (Art. 5 vom 13. April 2007) (BGBl. I S. 513, 517)
KJHG	Kinder und Jugendhilfegesetz - SGB VIII (Art. 1 des Gesetzes vom 26. Juni 1990, BGBl. I S. 1163), zuletzt geändert durch Art. 2 Abs. 23 des Gesetzes vom 19. Februar 2007 (BGBl. I S. 122)
KomPrüfVO	Verordnung über das kommunale Prüfungswesen (Kommunalprüfungsverordnung) vom 17. März 2006 (GVBl. S. 77)
KPS-Richtlinien	Richtlinie des SMI für die Führung kriminalpolizeilicher personenbezogener Sammlungen in den Polizeidienststellen vom 15. Juli 1993 (SächsABl. 43/1993 S. 1094), Geltungsdauer verlängert durch VwV vom 4. Dezember 2003 (SächsABl. 52/2003, S. 1189)
KraftStG	Kraftfahrzeugsteuergesetz in der Fassung der Bekanntmachung vom 26. September 2002 (BGBl. I S. 3818), zuletzt geändert durch Art. 1 des Gesetzes vom 17. August 2007 (BGBl. I S. 1958)
KWG	Kreditwesengesetz in der Fassung der Bekanntmachung vom 9. September 1998 (BGBl. I S. 2776), zuletzt geändert durch Art. 3 des Gesetzes vom 16. Juli 2007 (BGBl. I S. 1330)

KunstUrhG	Gesetz betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie - Kunsturheberrechtsgesetz (BGBl. I S. 266), zuletzt geändert durch Art. 3 § 31 des Gesetzes vom 16. Februar 2001
LAG	Lastenausgleichsgesetz in der Fassung der Bekanntmachung vom 2. Juni 1993 (BGBl. I S. 845; 1995 BGBl. I S. 248), zuletzt geändert durch Art. 1 des Gesetzes vom 21. Juni 2006 (BGBl. I S. 1323)
LuftSiG	Luftsicherheitsgesetz vom 11. Januar 2005 (BGBl. I S. 78), zuletzt geändert durch Art. 9a des Gesetzes vom 5. Januar 2007 (BGBl. I S. 2)
LDSG-SH	Landesdatenschutzgesetz Schleswig-Holstein zum Schutz personenbezogener Informationen vom 9. Februar 2000 (GVOBl. Schl.-H. 4/2000, S. 169), gültig ab 1. Juli 2000
MZulKraftStVO	Verordnung der Sächsischen Staatsregierung über die Mitwirkung der Zulassungsbehörden bei der Verwaltung der Kraftfahrzeugsteuer vom 22. Juni 2006 (GVBl. S. 152)
OWiG	Gesetz über Ordnungswidrigkeiten in der Fassung der Bekanntmachung vom 19. Februar 1987 (BGBl. I S. 602), zuletzt geändert durch Art. 2 des Gesetzes vom 7. August 2007 (BGBl. I S. 1786)
PaßG	Paßgesetz vom 19. April 1986 (BGBl. I S. 537), zuletzt geändert durch Art. 1 des Gesetzes vom 20. Juli 2007 (BGBl. I S. 1566, 2317)
PAuswG	Gesetz über Personalausweise in der Fassung der Bekanntmachung vom 21. April 1986 (BGBl. I S. 548), zuletzt geändert durch Art. 2 des Gesetzes vom 20. Juli 2007 (BGBl. I S. 1566)
PersBefG	Personenbeförderungsgesetz in der Fassung der Bekanntmachung vom 8. August 1990 (BGBl. I S. 1690), zuletzt geändert durch Art. 27 des Gesetzes vom 7. September 2007 (BGBl. I S. 2246)
PStG	Personenstandsgesetz; geändert am 21. August 2002 (BGBl. I S. 3322), zuletzt geändert durch Art. 14 des Gesetzes vom 21. August 2002 (BGBl. I S. 3322, 3330) BGBl. III, Gl. Nr. 211-1, G aufgeh. durch Art. 5 Abs. 2 des PStRG 211-9 vom 19. Februar 2007 (BGBl. I S. 122)

RStV	Staatsvertrag für Rundfunk und Telemedien, kurz: Rundfunkstaatsvertrag, erstmals in Kraft getreten am 31. August 1991, zuletzt geändert durch Art. 1 des Neunten Staatsvertrages zur Änderung rundfunkrechtlicher Staatsverträge vom 31. Juli bis 10. Oktober 2006 (GBl. BW 2007 S. 111), in Kraft getreten am 1. März 2007
SAKDG	Gesetz über die Errichtung der Sächsischen Anstalt für kommunale Datenverarbeitung vom 15. Juli 1994 (GVBl. S. 1432), zuletzt geändert durch Art. 3 des Gestzesvom 16. Februar 2006 (GVBl. S. 58, 65)
SächsArchivG	Archivgesetz für den Freistaat Sachsen vom 17. Mai 1993 (GVBl. S. 449), zuletzt geändert durch Art. 2 des Gesetzes vom 5. Mai 2004 (GVBl. S. 148)
SächsBAG	Gesetz über die Berufsakademie im Freistaat Sachsen (Sächsisches Berufsakademiegesetz) vom 11. Juni 1999 (GVBl. S. 276), zuletzt geändert durch Art. 12 des Gesetzes vom 15. Dezember 2006 (GVBl. S. 515, 521)
SächsBeurtVO	Verordnung der Sächsischen Staatsregierung über die dienstliche Beurteilung der Beamten (Sächsische Beurteilungsverordnung) vom 16. Februar 2006 (GVBl. S. 26)
SächsBG	Beamtengesetz für den Freistaat Sachsen in der Fassung der Bekanntmachung vom 14. Juni 1999 (GVBl. S. 370), zuletzt geändert durch Art. 2 des Gesetzes vom 10. April 2007 (GVBl. S. 54, 77)
SächsBRKG	Sächsisches Gesetz über den Brandschutz, Rettungsdienst und Katastrophenschutz vom 24. Juni 2004 (GVBl. S. 245, ber. S. 647), geändert durch Art. 5 des Gesetzes vom 9. September 2005 (GVBl. S. 266)
SächsDO	Dienstordnung für die Behörden des Freistaates Sachsen, zuletzt geändert am 18. Mai 2005 (SächsABl. S. 458)
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), geändert durch Gesetz vom 25. August 2003 (GVBl. S. 330), zuletzt Neufassung vom 14. Dezember 2006 (GVBl. S. 530)
SächsEigBVO	Sächsische Eigenbetriebsverordnung, zuletzt geändert durch Art. 4 der VO vom 12. Dezember 2001 (GVBl. 2002 S. 3, 4)

SächsFrüh-ErDurchfG	Gesetz über die Durchführung eines Mammographie- Screenings und anderer Früherkennungsmaßnahmen (Sächsisches Früherkennungsdurchführungsgesetz) vom 1. Juni 2006 (GVBl. S. 150)
SächsGemO	Gemeindeordnung für den Freistaat Sachsen vom 21. April 1993 (GVBl. S. 301), zuletzt geändert durch Art. 1 des Gesetzes vom 7. November 2007 (GVBl. S. 478)
SächsHG	Sächsisches Hochschulgesetz vom 11. Juni 1999 (GVBl. S. 294), zuletzt geändert durch Art. 13 des Gesetzes vom 15. Dezember 2006 (GVBl. S. 515, 521)
SäHO	Vorläufige Haushaltsordnung des Freistaates Sachsen vom 19. Dezember 1990 (GVBl. S. 21), zuletzt geändert durch Art. 10 des Gesetzes vom 13. Dezember 2002 (GVBl. S. 333, 352)
SächsLaJuHiG	Landesjugendhilfegesetz vom 4. März 1992 (GVBl. S. 61), zuletzt geändert durch Art. 6 des Gesetzes vom 14. Juli 2005 (GVBl. S. 167, 175)
SächsKAG	Sächsisches Kommunalabgabengesetz vom 16. Juni 1993 (GVBl. S. 502), zuletzt geändert durch Art. 9 des Gesetzes vom 7. November 2007 (GVBl. S. 478, 484)
SächsKHG	Gesetz zur Neuordnung des Krankenhauswesens - Sächsisches Krankenhausgesetz (GVBl. S. 675), zuletzt geändert durch Art. 9 des Gesetzes vom 22. April 2005 (GVBl. S. 121, 125)
SächsKomZG	Sächsisches Gesetz über kommunale Zusammenarbeit vom 19. August 1993 (GVBl. S. 815), zuletzt geändert durch Art. 3 des Gesetzes vom 7. November 2007 (GVBl. S. 478)
SächsLKrO	Landkreisordnung für den Freistaat Sachsen vom 19. Juli 1993 (GVBl. S. 577), zuletzt geändert durch Art. 2 des Gesetzes vom 7. November 2007 (GVBl. S. 478, 482)
SächsLRettDPVO	Verordnung des SMI über die Rettungsdienstplanung (Sächsische Landesrettungsdienstplanverordnung) vom 5. Dezember 2006 (GVBl. S. 532)
SächsMeldVO	Verordnung des SMI zur Durchführung des Sächsischen Meldegesetzes (Sächsische Meldeverordnung) vom 13. Dezember 2006 (GVBl. S. 540), zuletzt geändert durch Art. 2 der Verordnung vom 19. September 2008 (GVBl. S. 413)

SächsMG	Sächsisches Meldegesetz vom 21. April 1993 (GVBl. S. 353), zuletzt geändert durch Art. 1 des Gesetzes vom 16. Februar 2006 (GVBl. S. 58)
SächsPersVG	Sächsisches Personalvertretungsgesetz, zuletzt geändert durch Art. 11 des Gesetzes vom 15. Dezember 2006 (GVBl. S. 515, 521)
SächsPolG	Polizeigesetz des Freistaates Sachsen, Bekanntmachung vom 13. August 1999 (GVBl. S. 466), zuletzt geändert durch Art. 45 des Gesetzes vom 5. Mai 2004 (GVBl. S. 148, 171)
SächsPsychKG	Sächsisches Gesetz über die Hilfen und die Unterbringung bei psychischen Krankheiten vom 16. Juni 1994 (GVBl. S. 1097), zuletzt geändert durch Zweites Gesetz zur Änderung des Gesetzes vom 16. August 2007 (GVBl. S. 390)
SächsStatG	Sächsisches Statistikgesetz vom 17. Mai 1993 (GVBl. S. 453), zuletzt geändert durch Art. 13 des Gesetzes vom 6. Juni 2002 (GVBl. S. 168, 171)
SächsStudDatVO	Verordnung zur Verarbeitung personengebundener 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)
SächsVerfGHG	Gesetz über den Verfassungsgerichtshof des Freistaates Sachsen (Sächsisches Verfassungsgerichtshofgesetz) vom 18. Februar 1993 (GVBl. S. 177, ber. S. 495), zuletzt geändert durch Erstes Gesetz zur Änderung des Gesetzes vom 27. September 1995 (GVBl. S. 321)
SächsVSG	Gesetz über den Verfassungsschutz im Freistaat Sachsen (Sächsisches Verfassungsschutzgesetz) vom 16. Oktober 1992 (GVBl. S. 459), zuletzt geändert durch Zweites Gesetz zur Änderung des Gesetzes vom 28. April 2006 (GVBl. S. 129)
SächsVwVfG	Vorläufiges Verwaltungsverfahrensgesetz für den Freistaat Sachsen vom 21. Januar 1993 (GVBl. S. 74), zuletzt geändert durch Art. 2 des Gesetzes vom 6. Mai 2003 (GVBl. S. 131, 133)
SächsWG	Sächsisches Wassergesetz vom 23. Februar 1993 (GVBl. S. 201), zuletzt geändert durch Art. 2 des Gesetzes vom 9. Juli 2007 (GVBl. S. 310)

SchulG	Schulgesetz für den Freistaat Sachsen vom 3. Juli 1991 (GVBl. S. 213), zuletzt geändert durch Art. 6 des Gesetzes vom 15. Dezember 2006 (GVBl. S. 515)
SGB I	Erstes Buch Sozialgesetzbuch - Allgemeiner Teil - (Art. 1 des Gesetzes vom 11. Dezember 1975, BGBl I S. 3015), zuletzt geändert durch Art. 2 Abs. 15 des Gesetzes vom 5. Dezember 2006 (BGBl. I S. 2748)
SGB II	Zweites Buch Sozialgesetzbuch - Grundsicherung für Arbeitsuchende - (Art. 1 des Gesetzes vom 24. Dezember 2003, BGBl. I S. 2954), zuletzt geändert durch Art. 2 des Gesetzes vom 10. Oktober 2007 (BGBl. I S. 2329)
SGB IV	Viertes Buch Sozialgesetzbuch - Gemeinsame Vorschriften für die Sozialversicherung - (Art. 1 des Gesetzes vom 23. Dezember 1976, BGBl. I S. 3845), zuletzt geändert durch Art. 22 des Gesetzes vom 7. September 2007 (BGBl. I S. 2246)
SGB V	Fünftes Buch Sozialgesetzbuch - Gesetzliche Krankenversiche rung - (Art. 1 des Gesetzes vom 20. Dezember 1988, BGBl. I S. 2477), zuletzt geändert durch Art. 28 Abs. 4 des Gesetzes vom 7. September 2007 (BGBl. I S. 2246)
SGB VI	Sechstes Buch Sozialgesetzbuch - Gesetzliche Rentenversicherung - (Art. 1 des Gesetzes vom 18. Dezember 1989, BGBl. I S. 2261, 1990 BGBl. I S. 1337), zuletzt geändert durch Art. 24 des Gesetzes vom 7. September 2007 (BGBl. I S. 2246)
SGB VIII	Achtes Buch Sozialgesetzbuch - Kinder und Jugendhilfe - (Art. 1 des Gesetzes vom 26. Juni 1990, BGBl. I S. 1163), zuletzt geändert durch Art. 2 Abs. 23 des Gesetzes vom 19. Februar 2007 (BGBl. I S. 122)
SGB X	Zehntes Buch Sozialgesetzbuch - Sozialverwaltungsverfahren und Sozialdatenschutz - (Art. 1 des Gesetzes vom 18. August 1980, BGBl. S. I 1469 und Art. 1 des Gesetzes vom 4. November 1982, BGBl. S. I 1450), zuletzt geändert durch Art. 263 der Verordnung vom 31. Oktober 2006 (BGBl. I S. 2407)
SGB XI	Elftes Buch Sozialgesetzbuch - Soziale Pflegeversicherung - (Art. 1 des Gesetzes vom 26. Mai 1994, BGBl. I S. 1014), zuletzt geändert durch Art. 28 Abs. 5 des Gesetzes vom 7. September 2007 (BGBl. I S. 2246)

SGB XII	Zwölftes Buch Sozialgesetzbuch - Sozialhilfe - (Art. 1 des Gesetzes vom 27. Dezember 2003, BGBl. I S. 3022), zuletzt geändert durch Art. 5 und 6 des Gesetzes vom 20. Juli 2007 (BGBl. I S. 1595)
StAG	Staatsangehörigkeitsgesetz vom, zuletzt geändert durch Art. 5 des Gesetzes vom 19. August 2007 (BGBl. I S. 1970)
StGB	Strafgesetzbuch in der Fassung der Bekanntmachung vom 13. November 1998 (BGBl. I S. 3322), zuletzt geändert durch Gesetz vom 26. Oktober 2007 (BGBl. I S. 2523)
StPO	Strafprozessordnung in der Fassung der Bekanntmachung vom 7. April 1987 (BGBl. I S. 1074, 1319), zuletzt geändert durch Art. 2 des Gesetzes vom 16. Juli 2007 (BGBl. I S. 1327)
StUG	Stasi-Unterlagen-Gesetz in der Fassung der Bekanntmachung vom 18. Februar 2007 (BGBl. I S. 162)
StVollzG	Strafvollzugsgesetz vom 16. März 1976 (BGBl. I S. 581, 2088), zuletzt geändert durch Art. 2 Abs. 11 des Gesetzes vom 19. Februar 2007 (BGBl. I S. 122 mWv 1. Januar 2009)
TDDSG	Gesetz über den Datenschutz bei Telediensten Kurztitel: Teledienstedatenschutzgesetz (BGBl. I S. 1870, 1871) Inkrafttreten am: 1. August 1997; Letzte Änderung durch Art. 3 und 4 Abs. 2 des Gesetzes vom 14. Dezember 2001 (BGBl. I S. 3721) Außerkrafttreten: 1. März 2007 (Art. 5 ElGVG vom 26. Februar 2007); wurde abgelöst durch das TMG ab 1. März 2007
TKG	Telekommunikationsgesetz vom 22. Juni 2004 (BGBl. I S. 1190), zuletzt geändert durch Art. 3 des Gesetzes vom 18. Februar 2007 (BGBl. I S. 106)
TMG	Telemediengesetz vom 26. Februar 2007 (BGBl. I S. 179): ersetzt das TDDSG ab 1. März 2007
TVG	Tarifvertragsgesetz in der Fassung der Bekanntmachung vom 25. August 1969 (BGBl. I S. 1323), zuletzt geändert durch Art. 223 der Verordnung vom 31. Oktober 2006 (BGBl. I S. 2407)
UrhG	Urheberrechtsgesetz vom 9. September 1965 (BGBl. I S. 1273), zuletzt geändert durch Art. 1 des Gesetzes vom 26. Oktober 2007 (BGBl. I S. 2513)
UWG	Gesetz gegen den unlauteren Wettbewerb vom 3. Juli 2004 (BGBl. I S. 1414), zuletzt geändert durch Art. 5 des Gesetzes vom 21. Dezember 2006 (BGBl. I S. 3367)

VermG	Vermögensgesetz in der Fassung der Bekanntmachung vom 9. Februar 2005 (BGBl. I S. 205), zuletzt geändert durch Art. 4 des Gesetzes vom 19. Dezember 2006 (BGBl. I S. 3230)
VerpflG	Verpflichtungsgesetz; Gesetz über die förmliche Verpflichtung nichtbeamteter Personen vom 2. März 1974 (BGBl. I S. 469, 545; III 453-17), zuletzt geändert durch Änderungsgesetz vom 15. August 1974 (BGBl. I S. 1942)
VersammlG	Versammlungsgesetz in der Fassung der Bekanntmachung vom 15. November 1978 (BGBl. I S. 1789), zuletzt geändert durch Art. 1 des Gesetzes vom 24. März 2005 (BGBl. I S. 969)
VwVPersAktenB	Verwaltungsvorschrift des SMI über die Führung und Verwaltung von Personalakten der Beamten in der Fassung der Bekanntmachung vom 16. Juni 1994 (GVBl. S. 1153), zuletzt geändert durch Art. 1 des Gesetzes vom 7. April 1997 (GVBl. S. 53, ber. S. 466)
VwV Rechtsschutz	Verwaltungsvorschrift des SMI über den Rechtsschutz für Bedienstete in Straf- und anderen Verfahren vom 11. Januar 2007 (SächsABl. 5/2007 S. 172)
VwV Schuldatenschutz	Verwaltungsvorschrift des SMK über den Datenschutz beim Umgang mit personenbezogenen Daten an Schulen (MBl. SMK 2007, S. 26), Fassung gültig ab 2. März 2007
VwVfG	Verwaltungsverfahrensgesetz in der Fassung der Bekanntmachung vom 23. Januar 2003 (BGBl. I S. 102), zuletzt geändert durch Art. 4 Abs. 8 des Gesetzes vom 5. Mai 2004 (BGBl. I S. 718)
WoGG	Wohngeldgesetz in der Fassung der Bekanntmachung vom 7. Juli 2005 (BGBl. I S. 2029 (2792)), zuletzt geändert durch Art. 2 Abs. 12 des Gesetzes vom 5. Dezember 2006 (BGBl. I S. 2748)
ZPO	Zivilprozessordnung in der Fassung der Bekanntmachung vom 5. Dezember 2005 (BGBl. I S. 3202; 2006 BGBl. I S. 431; 2007 BGBl. I S. 1781), zuletzt geändert durch Art. 3 Abs. 6 des Gesetzes vom 26. März 2007 (BGBl. I S. 370)

Sonstiges

AG	Aktiengesellschaft
ARGE	Arbeitsgemeinschaft nach SGB II

ARoV	Amt für offene Vermögensfragen
AVS	Akademie für öffentliche Verwaltung des Freistaates Sachsen
BAnz	Bundesanzeiger
BayVGH	Bayerischer Verwaltungsgerichtshof
BfD	Bundesbeauftragter für den Datenschutz und Informationsfreiheit
BfV	Bundesamt für Verfassungsschutz
BGBl.	Bundesgesetzblatt
BGH	Bundesgerichtshof
BGHZ	Amtliche Sammlung der Entscheidungen des Bundesgerichtshofs in Zivilsachen
BKA	Bundeskriminalamt
BMAS	Bundesministerium für Arbeit und Soziales
BMF	Bundesministerium der Finanzen
BMG	Bundesministerium für Gesundheit
BMI	Bundesministerium des Innern
BMJ	Bundesministerium der Justiz
BMWi	Bundesministerium für Wirtschaft und Technologie
BND	Bundesnachrichtendienst
BR-DS	Bundesrats-Drucksache
BSG	Bundessozialgericht
BSI	Bundesamt für Sicherheit in der Informationstechnik
BStU	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
DöV	Die öffentliche Verwaltung
DSF	Die Gesellschaft für Deutsch-Sowjetische Freundschaftwar eine Massenorganisation in der DDR, die den Bürgern Kenntnisse über die Kultur und Gesellschaft der Sowjetunion vermitteln sollte
DSK	Datenschutzkonferenz (halbjährlich stattfindende Konferenz der Datenschutzbeauftragten des Bundes und der Länder)
DTSB	Der Deutsche Turn- und Sportbund war die zentrale für den Sport zuständige Massenorganisation der DDR
DuD	Datenschutz und Datensicherheit
DVBl.	Deutsches Verwaltungsblatt
DVO	Durchführungsverordnung
EG	Europäische Gemeinschaft
eGK	Elektronische Gesundheitskarte
EPA	Elektronische Patientenakte
EU	Europäische Union
e. V.	Eingetragener Verein
FDGB	Der Freie Deutsche Gewerkschaftsbund war der Dachverband der etwa 15 Einzelgewerkschaften in der DDR
FDJ	Die Freie Deutsche Jugend ist ein sozialistischer Jugendverband. In der DDR war sie die einzige staatlich anerkannte und geförderte Jugendorganisation
FEVS	Fürsorgerechtliche Entscheidungen der Verwaltungs- und Sozialgerichte

FIFA	Die Internationale Föderation des Verbandsfußballs ist der Weltfußballverband mit Sitz in Zürich. Er organisiert verschiedene Fußball-Wettbewerbe, darunter die Herren- und die Frauen-Fußballweltmeisterschaft
GEZ	Gebühreneinzugszentrale der öffentlich-rechtlichen Rundfunkanstalten
gGmbH	Die gemeinnützige GmbH ist eine Gesellschaft mit beschränkter Haftung, der besondere Steuervergünstigungen gewährt werden. Sie ist keine eigene Gesellschaftsform und unterliegt den Vorschriften des GmbH-Gesetzes
GmbH	Gesellschaft mit beschränkter Haftung
HStR	Handbuch des Staatsrecht der Bundesrepublik Deutschland
IHK	Industrie- und Handelskammer
INPOL	Polizeiliches Informationssystem des Bundes u. der Länder
JVA	Justizvollzugsanstalt
KMK	Kultusministerkonferenz
KV	Krankenversicherung
LfD	Landesbeauftragte(r) für den Datenschutz
LfF	Landesamt für Finanzen des Freistaates Sachsen
LfV	Landesamt für Verfassungsschutz des Freistaates Sachsen
LG	Landgericht
LKA	Landeskriminalamt Sachsen
LT-DS	Landtags-Drucksache
MAD	Militärischer Abschirmdienst
MDI	das ehemalige Ministerium des Innern der DDR
MDK	Medizinischer Dienst der Krankenversicherung
MDR	Mitteldeutscher Rundfunk

MfS	Ministerium für Staatssicherheit der ehemaligen DDR
MMR	Multimedia und Recht
NJW	Neue Juristische Wochenschrift
NStZ	Neue Zeitschrift für Strafrecht
NVwZ	Neue Zeitschrift für Verwaltungsrecht
NZS	Neue Zeitschrift für Sozialrecht
OLG	Oberlandesgericht
OVG	Sächsisches Oberverwaltungsgericht
PASS	Polizeiliches Auskunftssystem Sachsen
PDA	Personal Digital Assistant (persönlicher digitaler Assistent)
PKK	Parlamentarische Kontrollkommission
SächsABl.	Sächsisches Amtsblatt
GVBl.	Sächsisches Gesetz- und Verordnungsblatt
SächsLRettDP	Sächsischer Landesrettungsdienstplan
SächsMBl. SMF	Ministerialblatt des Sächsischen Staatsministeriums der Finanzen
SächsVerfGH	Verfassungsgerichtshof des Freistaates Sachsen
SBZ	Sowjetische Besatzungszone
sc.	sinngemäß: das heißt
SIS	Schengener Informationssystem
SMF	Sächsisches Staatsministerium der Finanzen
SMI	Sächsisches Staatsministerium des Innern
SMJus	Sächsisches Staatsministerium der Justiz
SMS	Sächsisches Staatsministerium für Soziales
SMUL	Sächsisches Staatsministerium für Umwelt und Landwirtschaft

SMWK	Sächsisches Staatsministerium für Wissenschaft und Kunst
SRH	Sächsischer Rechnungshof
SSG	Sächsischer Städte- und Gemeindetag
VG	Verwaltungsgericht
VwRR	Verwaltungsrechtsreport
WLAN	Wireless Local Area Network; drahtloses lokales Netzwerk
ZBR	Zeitschrift für Beamtenrecht

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

1.1 Respekt vor den Grundwerten

Wir leben in einer Informationsgesellschaft. Im Gegensatz zu der großen Kampagne in der Bürgergesellschaft gegen die befürchtete Überwachung durch den „großen Bruder“, die 1983 zum wegweisenden Volkszählungsurteil des Bundesverfassungsgerichtes führte, ist heute die Preisgabe von persönlichen Informationen zum Alltag geworden. Schon der Blick ins eigene Portemonnaie zeigt, wie allgegenwärtig mittlerweile der Einsatz von mechanischen und elektronischen Hilfsmitteln ist - EC-Karte, Krankenkassenkarte, Kreditkarte, Bahncard, vielleicht Paybackkarte, Mitgliedsausweise in Kartenform, Karten für die Zugangskontrolle bei der Arbeitsstelle. Ein Mobilfunktelefon gehört mittlerweile zum Standard. Andere elektronische Dienstleistungen wie E-Ticket oder Online-Navigationssysteme sind auf dem Vormarsch. Das Nutzerverhalten hat sich angepasst. Ging man früher (in der papiergestützten Zeit) noch mit einem grundsätzlichen Misstrauen an Formulare heran, in denen Daten abgefragt wurden, so ist das heute begrenzt auf direkt negativ wahrgenommene Abfragen. Gerade unter der jüngeren mit den elektronischen Medien aufgewachsenen Generation fallen bei einigen sämtliche Hemmungen, wenn im Internet freizügig Einblick ins eigene Privatleben und das der Bekannten geboten wird. Dies soll keine Kulturschelte sein, sondern klar vor Augen führen, dass hier eine Entwicklung eingesetzt hat, die nicht durch Verbote und künstliche Begrenzungen rückgängig gemacht werden kann. Vielmehr haben sich alle Beteiligten darauf einzustellen, Chancen und Risiken zu erkennen und ihre eigenen Vorstellungen und Konzepte zu hinterfragen und anzupassen.

Erster Schritt ist allerdings, sich bewusst zu machen, auf welchem Fundament man steht. Wird in der politischen Diskussion auf den Datenschutz Bezug genommen, so ist die Reaktion in der Öffentlichkeit und bei den Betroffenen selbst zwiespältig. Ist bei Themen wie GEZ oder Hartz IV die Empörung groß und findet die Position der Datenschützer Unterstützung, so wird in anderen Bereichen, z. B. in der Kriminalitätsbekämpfung oder Kindeswohlgefährdung der Datenschutz als Hindernis wahrgenommen. Häufig kommt dann der Satz „Datenschutz ist Täterschutz“. Abgesehen davon, dass sich viele Illusionen machen, sie könnten überhaupt nicht zum Gegenstand ihnen nicht genehmer Datenverarbeitung durch öffentliche Stellen werden, so ist dieses Herangehen grundsätzlich falsch. Das Recht auf informationelle Selbstbestimmung ist kein „Schönwetterrecht“. Es gilt für „Gute“ wie für „Böse“. Grundrechte haben ihren Sinn nicht nur in konfliktfreien Lagen, im Gegenteil: Gerade dann, wenn es stört, sind Grundrechte notwendig. Gerade beim Grundrecht auf informa-

tionelle Selbstbestimmung wird dies exemplarisch deutlich. Weil man gemeinhin denkt, dass die Verarbeitung von ein paar Informationen über einen Menschen im Gegensatz zur körperlichen Verletzung ja nicht weiter weh tut, ist die Versuchung groß, sich schnell über die vom Recht aufgestellten Schranken hinwegzusetzen. Erst langsam beginnt die Erkenntnis zu dämmern, dass eine Rufschädigung im Internet, ein Identitätsdiebstahl oder nachlässige Bekanntgabe von eigenen Informationen ebenfalls einschneidende Konsequenzen für die persönliche Lebensführung haben kann. Je stärker unsere Gesellschaft auf Informationsverarbeitung basiert, umso größer wird das Risiko, dass der Einzelne von eben dieser Verarbeitung beeinflusst und bestimmt wird. Das Resultat muss nicht unbedingt vordergründig als negativ erfahren werden (z. B. bei personenbezogener Werbung), allerdings sollten wir uns fragen, ob wir grundsätzlich eine Gesellschaft wollen, die es in Kauf nimmt, dass der Mensch fremd bestimmt wird, oder eine, die versucht, einen Freiraum für den Einzelnen zu sichern. Die Väter und Mütter des Grundgesetzes hatten aus gutem Grund eindeutig letztere Zielrichtung im Auge. Wer sieht, was Diktaturen bewirken und bewirkt haben (und vielleicht dies persönlich erlebt hat), kann dies nachvollziehen. Die von ihnen formulierten Grundwerte sind von uns zu sichern - nicht etwa trotz, sondern gerade wegen der oft beschworenen aktuellen Gefahren für unsere freiheitliche und demokratische Grundordnung.

Das stellt klare Anforderungen an die, die in Exekutive, Legislative und Judikative arbeiten, insbesondere an die, die Verantwortung tragen. Achtung gegenüber den Wertentscheidungen des Grundgesetzes und Sorgfalt in der täglichen Arbeit ist von Nöten bei denen, die Recht schaffen und durchsetzen. Leider vermisse ich das verstärkt. Zwei Beobachtungen unterstützen das:

In den letzten Jahren findet eine Senkung der Handlungs- und Respektschwellen innerhalb der Exekutive statt. Selbst von den Ministerien, die von Geschäftswegen her für Verfassungsfragen zuständig sind, werden Gesetze oder Vorhaben vorgeschlagen, denen die Verfassungswidrigkeit auf die Stirn geschrieben steht. Die vom Sächsischen Innenminister ins Spiel gebrachte öffentlich zugängliche Sexualstraftäterdatei ist ein solches Beispiel. An anderen Stellen wird bewusst eine Reihe von Maßnahmen vorgeschlagen, obwohl man um verfassungsrechtliche Bedenken weiß. Beispiel ist hier wieder der Innenbereich in Bund und Ländern mit den Polizeigesetzen. Man kann sich des Eindrucks nicht erwehren, hier wird abgestimmt ausgetestet, was die Verfassungsgerichte durchgehen lassen - in der Hoffnung, dass diese sich nur auf bestimmte Punkte konzentrieren. Überlegungen zur Verfassungsmäßigkeit werden dem Verfassungsgericht überlassen. Art. 20 Abs. 3 GG „Die Gesetzgebung ist an die verfassungsmäßige Ordnung, die vollziehende Gewalt und die

Rechtsprechung sind an Gesetz und Recht gebunden“ meint jedoch nicht, dass die vollziehende Gewalt, wenn sie an der Gesetzgebung beteiligt ist, nicht an die verfassungsmäßige Ordnung gebunden ist. Wer, wenn ihm die Verfassung Grenzen setzt, denkt und sagt, dann könne man mal schnell die Verfassung ändern, hat das ihm übertragene Amt nicht verstanden. Respekt - „Rücksicht“ - gegenüber den in der Verfassung niedergelegten Grundwerten wird von dem verlangt, der ein politisches Amt innehat, nicht forsche Gleichgültigkeit.

Bereits in meinem letzten Tätigkeitsbericht habe ich darauf hingewiesen, dass das technische Potential eines Verfahrens für seine spätere Nutzung entscheidend ist. Juristische Schranken können leicht aufgehoben werden. Sind die Daten erst einmal da, so kommt mit Sicherheit später ein Anlass, bei dem der bisher noch rechtlich unzulässige Zugriff auf diese Daten gefordert wird. Beispiele, bei denen dies umgesetzt worden ist oder immer wieder thematisiert wird, gibt es genug: Kontodatenspeicherung, Telefon- und Internetverbindungsdaten, Mautdaten. Dies lässt für andere Großprojekte wie Gesundheitskarte, biometrische Daten in Ausweisen oder Steueridentifikationsnummer Schlimmes befürchten.

Letztes Bollwerk sind oft die Verfassungsgerichte. Waren sie früher eher auf Grundsatzentscheidungen begrenzt, sind sie mittlerweile die „Wellenbrecher“ für die Begehrlichkeiten der Politik. Ihre Entscheidungen mögen nicht immer allen schmecken; sie sind aber unentbehrlich bei der Gewährleistung einer freiheitlichen und demokratischen Gesellschaft in unserem Land. Für mich ist das Anlass genug, mit besonderem Augenmerk dorthin zu schauen, wo es um die Beachtung solcher Urteile geht - insbesondere, wenn es sich um Bereiche handelt, die per sé nicht transparent sind (vgl. 5.10.1). Ich werde das auch in Zukunft konsequent tun.

Das Fazit für den Datenschutz in Sachsen ist in diesem Berichtszeitraum durchwachsen. Auf der einen Seite stehen Hörbereitschaft und Aufmerksamkeit bei weiten Teilen der Staatsregierung und der Kommunen. Besonders herausragend möchte ich hier auf die deutliche Haltung des SMK bei dem Thema Schülerstatistik hinweisen, die die Diskussion in der KMK offen gehalten und verhindert hat, dass bundesweit vollendete Tatsachen geschaffen wurden (vgl. 5.7.1). Im Parlament erlebe ich eine dem Datenschutz gegenüber aufgeschlossene Atmosphäre. Die Abgeordneten befassen sich intensiv mit von mir gemachten Vorschlägen; häufig fließen sie mit in die verabschiedeten Gesetze ein. Dies ist in unserem föderalen System nicht selbstverständlich. Ich bedanke mich dafür.

Leider ist auf der anderen Seite negativ zu vermerken, dass die oben erwähnten Entwicklungen auch um Sachsen keinen Bogen machen. Da es häufig um bundesrechtlich zu regelnde Materie geht, ist der eigenständige Handlungsspielraum in Sachsen über das bloße Artikulieren hinaus jedoch gering. Allerdings verhindert das doch im Einzelfall nicht gravierende datenschutzrechtliche Verstöße. In meiner mittlerweile vierzehnjährigen Tätigkeit beim Datenschutz habe ich noch nicht so eklatante Rechtsverstöße wie bei der Affäre um den Verfassungsschutz erlebt. Ich hoffe, dass die noch ausstehenden Konsequenzen gezogen werden.

Auch kann ich zwar häufig, aber nicht immer etwas für diejenigen erreichen, die sich an mich wenden. So hat sich im Berichtszeitraum für den im letzten Tätigkeitsbericht angedeuteten Fall (12/1.8) trotz meiner Bemühungen keine befriedigende Lösung ergeben. Auch wenn hier - wie in den meisten Fällen - die datenschutzrechtlichen Verstöße nicht der Kern des Problems, sondern „Begleitmusik“ waren, hätte ich mich gefreut, wenn ihre Behandlung sich auf eine den Petenten befriedigende Lösung ausgewirkt hätte.

Last but not least möchte ich mich beim Präsidenten des Sächsischen Landtages und der Landtagsverwaltung bedanken. Ohne ihre Unterstützung wäre die Arbeit meiner Behörde unmöglich. Wer die Anforderungen kennt, vor denen eine kontrollierende Stelle steht, kann nachempfinden, welchen technischen, organisatorischen, personellen und auch ideellen Rückhalt sie braucht. Dieser ist immer vorhanden.

1.2 Datenschutz aus einer Hand - Änderung des Sächsischen Datenschutzgesetzes zum 1. Januar 2007

Im Berichtszeitraum wurde das Sächsische Datenschutzgesetz vom 25. August 2003 geändert. Die regierungstragenden Parteien CDU und SPD hatten zuvor in ihrer Koalitionsvereinbarung für die 4. Wahlperiode vom 8. November 2004 Folgendes festgestellt:

„Dem Datenschutz kommt in unserer zunehmend vernetzten Gesellschaft große Bedeutung zu. Das Recht auf informationelle Selbstbestimmung erfordert den Schutz der Daten von Privatpersonen und Unternehmen. Die Koalitionspartner betonen die wichtige Rolle, die der Datenschutzbeauftragte hat. Um den Datenschutz effizienter zu gestalten, wird geprüft, ob die Kontrolle Privater vom Datenschutzbeauftragten wahrgenommen werden kann.“

Infolge dieser Prüfung legten die Koalitionsfraktionen des Sächsischen Landtages am 2. Mai 2006 den Entwurf eines Gesetzes zur Änderung des Sächsischen Datenschutz-

gesetzes (LT-DS 4/5121) vor. Dieser wurde nach einem intensiven parlamentarischen Beratungsverfahren einschließlich einer öffentlichen Anhörung vom 7. September 2006 am 14. Dezember 2006 beschlossen (GVBl. 2006, S. 530) und trat zum 1. Januar 2007 in Kraft.

Wichtigste Änderung ist die durch die Einfügung eines neuen § 30a in das Sächsische Datenschutzgesetz mir übertragene Aufgabe der Aufsichtbehörde für den nicht-öffentlichen Bereich. Diese bisher den Regierungspräsidien zugewiesene Aufgabe tritt mithin künftig neben meine herkömmliche Aufgabe der Kontrolle öffentlicher Stellen nach Art. 57 SächsVerf (Stichwort: „Datenschutz aus einer Hand“). Damit entspricht die Datenschutz-Organisation in Sachsen seit dem 1. Januar 2007 derjenigen in Berlin, Bremen, Hamburg, Mecklenburg-Vorpommern, Nordrhein-Westfalen, neuerdings wieder Niedersachsen sowie Schleswig-Holstein.

Mit der Übertragung der Zuständigkeit als Aufsichtsbehörde nach § 38 BDSG habe ich eine neue und schwierige Aufgabe erhalten. Der Gesetzgeber verfolgte ausweislich der Begründung zum Gesetzentwurf „Synergie- und Kosteneinspareffekte“. Außerdem gewönnen „technische Fragen im Datenschutz zunehmend an Bedeutung“. Hierfür bestehe „Bedarf an qualifiziertem Personal, welches bei einer Stelle dann sowohl für die technischen Fragen im öffentlichen als auch im nicht-öffentlichen Bereich zuständig wäre“.

Meine neuen Kontrollbefugnisse im nicht-öffentlichen Bereich werde ich mit Augenmaß wahrnehmen. Ich werde sie stets eingedenk der Tatsache ausüben, dass nicht-öffentliche Stellen personenbezogene Daten in Ausübung ihrer Grundrechte, namentlich der freien Berufsausübung, Art. 12 GG, und der allgemeinen Handlungsfreiheit, Art. 2 Abs. 1 GG, verarbeiten dürfen. Auch habe ich selbstverständlich das für alles staatliche Handeln gegenüber rechtsunterworfenen Privaten geltende Verhältnismäßigkeitsprinzip zu beachten.

Weitere Änderungen betreffen den Anwendungsbereich des Sächsischen Datenschutzgesetzes im Hinblick auf öffentlich beherrschte Stellen in privater Rechtsform nach § 2 Abs. 2 SächsDSG sowie im Hinblick auf öffentliche Stellen, die am Wettbewerb teilnehmen (z. B. kommunale Wohnungsvermietungsgesellschaften) nach § 2 Abs. 3 SächsDSG.

Als praktisch bedeutsam wird sich auch die wesentliche Erweiterung der Befugnisse der Datenschutzbeauftragten öffentlicher Stellen nach § 11 SächsDSG erweisen. Ihnen wird nunmehr mit § 11 Abs. 3 SächsDSG erstmals die Befugnis erteilt, „zur Aufgabenerfüllung Einsicht in die gespeicherten Daten und die Datenverarbeitungs-

programme“ zu nehmen. Die sächsische Rechtslage ist damit an die anderer Länder, in denen den Datenschutzbeauftragten öffentlicher Stellen ebenfalls die Befugnis zur Einsicht „in alle Unterlagen und Akten und die automatisierte Datenverarbeitung“ zugewiesen ist (z. B. § 10a Abs. 5 Satz 4 HmbDSG, § 10 Abs. 3 Satz 5 LDSG-SH), angepasst worden. § 11 Abs. 3 SächsDSG entspricht damit derzeit voll der aus Art. 18 Abs. 2, 2. Spiegelstrich EG-DSRiLi folgenden Verpflichtung des Freistaates Sachsen, „die unabhängige Überwachung der Anwendung der zur Umsetzung dieser Richtlinie erlassenen einzelstaatlichen Bestimmungen“ zumindest im Hinblick auf die Meldepflicht nach § 10 Abs. 3 SächsDSG. Ferner darf künftig ein stellvertretender Datenschutzbeauftragter als Abwesenheitsvertreter bestellt werden, dessen Rechtsstellung und Bestellung sich nach den Vorschriften über den Datenschutzbeauftragten nach § 11 SächsDSG richten.

Mit § 9 Abs. 1 Satz 2 SächsDSG ist der Grundsatz der Datenvermeidung und Datensparsamkeit, der seit 2001 als Element des modernisierten Datenschutzes in das Bundesdatenschutzgesetz aufgenommen worden war, auch im Sächsischen Datenschutzgesetz erstmals gesetzlich verankert worden. Ziel der außerordentlich wichtigen Regelung ist es, durch den gezielten Einsatz datenschutzfreundlicher Technik die Gefahren für das Recht auf informationelle Selbstbestimmung der Betroffenen zu reduzieren. Die Vorschrift soll die Grundnorm für das Konzept „Datenschutz durch Technik“, d. h. den Datenschutz nicht gegen, sondern mit und durch die Technik zu gewährleisten, sein. Letztlich soll mit der Regelung die öffentliche Hand dazu angehalten werden, diejenige Technik einzusetzen, die keine andere als die im Sinne des verfassungsrechtlichen Verhältnismäßigkeitsgrundsatzes erforderliche Datenverarbeitung zulässt. Damit soll angesichts der zunehmenden Überwachbarkeit des Verhaltens des Einzelnen (z. B. durch RFID, biometrische Verfahren, Vorratsdatenspeicherung, Mautdatenverarbeitung etc.) in der Datenverarbeitung der Gedanke der Datensparsamkeit so gefördert werden, wie der Gedanke der Energiesparsamkeit im Umweltschutz. Dieser Grundsatz soll in eine Präferenzregel zur Auswahl und beim Einsatz von Datenverarbeitungssystemen umgesetzt werden.

Ferner sind zu beachtende Änderungen in § 3 SächsDSG (Begriffsbestimmungen), § 7 SächsDSG (Datenverarbeitung im Auftrag), § 10 SächsDSG (Verfahrensverzeichnisse, Vorabkontrolle), § 30 SächsDSG (Tätigkeitsbericht), § 31 SächsDSG (Datenschutzregister) und § 38 SächsDSG (Ordnungswidrigkeiten) vorgenommen worden.

Mit dem Änderungsgesetz wurde der in § 3 Abs. 3 SächsDSG seit 1991 unveränderte Begriff der Daten verarbeitenden Stelle auf diejenigen Stellen reduziert, die Daten für

sich selbst verarbeiten oder durch andere im Auftrag verarbeiten lassen. Nicht mehr als Daten verarbeitende Stelle gilt seitdem die Stelle, die Daten „für andere verarbeitet“, d. h. der Auftragnehmer. Damit wurde dem Umstand Rechnung getragen, dass der Auftragnehmer keine funktional eigenständige Stelle, sondern lediglich „verlängerter Arm“ des Auftraggebers ist. Der Auftraggeber ist und bleibt die datenschutzrechtlich verantwortliche Stelle.

Mit der in § 10 Abs. 1 Satz 2 Nr. 9 SächsDSG (wieder) aufgenommenen Pflicht zur Angabe von Regelfristen für die Löschung von Daten in das Verfahrensverzeichnis wurde ein redaktionelles Versehen des Gesetzgebers von 2003 beseitigt. Die Pflicht war zuvor in § 10 Abs. 1 Satz 2 Nr. 6 SächsDSG 1991 enthalten. Die Bestimmung geht über den in Art. 19 Abs. 1 der EG-DSRiLi festgelegten Mindestinhalt der Meldung hinaus, die Festlegung zusätzlicher Inhalte durch die Mitgliedstaaten ist jedoch zulässig. Regelfristen zur Löschung der verarbeiteten Daten sollten bereits aus datenschutzorganisatorischen Gründen im Verfahrensverzeichnis nachvollzogen werden können. Das Bundesdatenschutzgesetz und die Datenschutzgesetze anderer Bundesländer enthalten entsprechende Vorschriften. Mit dem neuen § 10 Abs. 4 Satz 6 SächsDSG wird bewirkt, dass sich der Datenschutzbeauftragte einer nachgeordneten Stelle auf das Ergebnis einer Vorabkontrolle durch die übergeordnete Stelle beziehen kann. Damit können die Vorabkontrollen der nachgeordneten Behörden und Gerichte im Sinne eines gebotenen Bürokratieabbaus erheblich vereinfacht und beschleunigt werden. Zugleich sind die datenschutzrechtlich relevanten Vorgangsverwaltungsverfahren, die nach § 10 Abs. 4 Nr. 2 SächsDSG a. F. vom Anwendungsbereich der Vorabkontrolle systematisch und vom Wortlaut her ausgenommen waren, wieder in diesen Anwendungsbereich einbezogen worden. Künftig ist in allen Fällen, in denen kein Verfahrensverzeichnis zu erstellen ist, auch keine Vorabkontrolle durchzuführen.

Mit der Änderung von § 30 Abs. 1 Satz 2 SächsDSG ist klargestellt worden, dass ich mich jederzeit zur Unterrichtung über wesentliche Entwicklungen des Datenschutzes an den Sächsischen Landtag und die Öffentlichkeit wenden darf. Die Änderung ist auch vor dem Hintergrund der Entscheidung des Bundesgerichtshofes in der Strafsache gegen den ehemaligen Sächsischen Datenschutzbeauftragten, Dr. Thomas Giesen, wegen Verletzung des Dienstgeheimnisses (BGH, Urteil vom 9. Dezember 2002, - 5 StR 276/02) von Belang. Wörtlich hatte der BGH als Revisionsinstanz ausgeführt:

„Ein Amtsträger, der wie der Angeklagte zur Kontrolle der Gesetzestreue eines anderen Amtsträgers berufen ist, kann wichtige öffentliche Interessen nicht durch die

Offenbarung eines Gesetzesverstoßes gefährden, wenn er die Öffentlichkeit - wie ersichtlich hier - auch als Verbündeten gewinnen will, um auf ein gesetzmäßiges Verhalten hinzuwirken."

Mit dem Änderungsgesetz sind drei neue Ordnungswidrigkeitentatbestände in § 38 SächsDSG eingefügt worden. Zugleich hat der Gesetzgeber dem Sächsischen Datenschutzbeauftragten die Aufgabe der Verfolgung und Ahndung von Ordnungswidrigkeiten nach dem Sächsischen Datenschutzgesetz übertragen.

Künftig begeht derjenige eine Ordnungswidrigkeit, der das Verfahrensverzeichnis nach § 10 Abs. 1 dem Sächsischen Datenschutzbeauftragten oder, falls ein Datenschutzbeauftragter nach § 11 bestellt ist, diesem, nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig zuleitet. Ist kein Datenschutzbeauftragter nach § 11 SächsDSG bestellt, trifft den Dienststellenleiter diese Pflicht. Des Weiteren verhält sich künftig ordnungswidrig, wer mir mangelhaft Auskünfte erteilt oder ungenügend an Kontrollen mitwirkt.

Fazit: Die Änderungen des Sächsischen Datenschutzgesetzes zum 1. Januar 2007 werden im Allgemeinen eine Anhebung des rechtlichen Datenschutzniveaus für die Betroffenen im öffentlichen wie im nicht-öffentlichen Bereich bewirken. Insbesondere hoffe ich, dass die Tätigkeit der Aufsichtsbehörde für den nicht-öffentlichen Bereich dort effektiver spürbar wird. Auch die den jüngsten Änderungen des Bundesdatenschutzgesetzes entsprechenden Erweiterungen der Befugnisse der Datenschutzbeauftragten nach § 11 SächsDSG erlauben eine intensivere Kontrolltätigkeit in diesem Bereich. Zugleich sind aber mit der Gesetzesänderung neue Fragen aufgeworfen worden, etwa zum Anwendungsbereich des Sächsischen Datenschutzgesetzes bei öffentlich beherrschten Stellen in privater Rechtsform, die „am Wettbewerb teilnehmen", oder im Hinblick auf die Rechtsaufsicht durch die Staatsregierung.

1.3 Öffentliche Stellen nach dem neuen Sächsischen Datenschutzgesetz

In 12/1.7 hatte ich mich mit Abgrenzungsfragen zum Begriff der *öffentlichen Stelle* nach dem Sächsischen Datenschutzgesetz auseinandergesetzt. Auch wenn ich die erläuternden Ausführungen anlässlich der Novellierung des Sächsischen Datenschutzgesetzes, die 2003 wirksam geworden ist, aufgrund eingehender Anfragen gemacht habe, so sind diese Ausführungen weiterhin aktuell. Ich halte an ihnen fest. § 2 Abs. 2 und Abs. 3 SächsDSG gehören zu den Bestimmungen, die mit die meisten Streitfragen aufwerfen. Gerade die für die Anwender schwierigen und wichtigen

Bestimmungen sind mit der erneuten Gesetzesänderung, die 2007 in Kraft getreten ist, nochmals modifiziert worden, so dass ich mich veranlasst sehe, weitere Hinweise zur Gesetzesauslegung zu geben.

Eine entscheidende Änderung hat Absatz 3 erfahren. Der Wettbewerbsbegriff, der bisher nur für juristische Personen des öffentlichen Rechts gegolten hat und an den die Anwendung des Bundesdatenschutzgesetzes geknüpft war, ist nunmehr auf juristische Personen des Privatrechts, die von öffentlichen Stellen beherrscht werden, erweitert worden. Die Bestimmung ist damit insbesondere für die Kommunalwirtschaft von Bedeutung. In der Rechtspraxis wird man nämlich bei Unternehmen in Privatrechtsform von Wettbewerbsunternehmen auszugehen haben, soweit nicht ein rechtliches Monopol das in Absatz 3 gesetzlich geforderte „am Wettbewerb teilnehmen“ hindert. Eine *Teilnahme am Wettbewerb* liegt bereits dann vor, wenn eine wirtschaftliche, aber nicht zwingend gewinnorientierte Betätigung vorgenommen wird. Ein *rechtliches Monopol*, das eine Teilnahme am Wettbewerb ausschließt, kann zum Beispiel bei gesetzlich - auch per Satzung - festgelegtem Anschluss- und Benutzungszwang vorliegen, etwa im Versorgungsbereich zugunsten von Stadtwerks-, Wasser- und Abwasserunternehmen. Derartige Unternehmen unterfallen dann (als Nicht-Wettbewerbsunternehmen) weiterhin dem Sächsischen Datenschutzgesetz. Für die Annahme eines Monopols reicht ein *faktisches Monopol* aber nicht aus. So sind insbesondere kommunale in Privatrechtsform organisierte Verkehrsunternehmen, die dem Bereich des öffentlichen Personennahverkehrs zuzurechnen sind, auch Wettbewerbsunternehmen. Bei Verkehrsunternehmen ergibt sich dies zudem gesetzlich, nämlich aus dem Personenbeförderungsgesetz, das unter Bezugnahme auf das *Gesetz gegen Wettbewerbsbeschränkungen* (UWG) von wettbewerblichem Handeln ausgeht (vgl. § 8 Abs. 3 PersBefG). Auch gemeinnützige Gesellschaften mit beschränkter Haftung (gGmbH) sind Wettbewerbsunternehmen, da sie auch regelmäßig eine wettbewerbliche Geschäftstätigkeit ausüben. Soweit Privatrechtsunternehmen im Sinne von § 2 Abs. 2 SächsDSG sowohl Wettbewerbs- als auch Monopolbereiche unter einem Dach vereinigen, ist im Regelfall von einer Anwendbarkeit des § 2 Abs. 3 SächsDSG auszugehen, es sei denn, der Wettbewerbsanteil würde eine vernachlässigbare Rolle spielen. Vorstellbar wäre dies insbesondere bei Stadtwerken in Privatrechtsform, die z. B. Wasser (im Monopolbereich), aber auch Strom (als Wettbewerber) anbieten.

Im Ergebnis wird also der weit überwiegende Teil der Stellen nach § 2 Abs. 2 SächsDSG nach Bundesdatenschutzgesetz Daten verarbeiten, ausgenommen die Stellen, die ausschließlich rechtliche Monopole innehaben. Nicht rechtlich ver-

selbständigte - nicht rechtsfähige - Eigenbetriebe allerdings fallen weder unter § 2 Abs. 2 noch unter § 2 Abs. 3 SächsDSG (vgl. 12/1.7 Nr. 1).

1.4 Übersendung von Beteiligungsberichten an den Sächsischen Datenschutzbeauftragten durch die kommunalen Gebietskörperschaften

Im letzten Berichtszeitraum habe ich Gemeinden (mit einer Einwohnerzahl über 10.000) und Landkreise gebeten, mir ihre Beteiligungsberichte regelmäßig zu übersenden. Ich benötige diese zur Aufgabenerfüllung, um einordnen zu können, ob es sich bei den juristischen Personen des Privatrechts, die unterhalten werden, um öffentliche Stellen (vgl. § 2 Abs. 2 Satz 1 SächsDSG) handelt und ob diese nach Sächsischem Datenschutzgesetz oder nach dem Bundesdatenschutzgesetz (vgl. § 2 Abs. 3 SächsDSG) Daten verarbeiten. Die Beteiligungsberichte waren im Besonderen nach der alten Gesetzeslage in vielen Fällen eine wertvolle Zusatzinformation, manchmal auch von entscheidender Bedeutung. Ich habe diesbezüglich von den Kommunen und Landkreisen viel Unterstützung erfahren und möchte hierfür danken.

Vereinzelt gab es allerdings Missverständnisse beziehungsweise Unverständnis für meine Forderung, mir die Beteiligungsberichte zur Verfügung zu stellen. Meinen Mitarbeitern wurde entgegengehalten, dass der Druck und die Versendung von Beteiligungsberichten Geld koste und dies nur gegen Kostenerstattung möglich sei, in einem Einzelfall weigerte sich eine Kommune sogar prinzipiell, mir den Beteiligungsbericht zu übermitteln. Einzelne Kommunen wandten sich an die kommunalen Verbände. Das SMI hat mich in meiner Auffassung gestützt.

Auch nach der Änderung des Sächsischen Datenschutzgesetzes benötige ich zur Wahrnehmung meiner Kontrollfunktionen die Beteiligungsberichte der Gebietskörperschaften. Weiterhin ist es für mich wesentlich, zu erfahren, welche Daten verarbeitenden Stellen es - insbesondere im Bereich der Kommunalwirtschaft - überhaupt gibt. Nur mit Hilfe der Berichte kann ich feststellen, ob die mir übersandten Verzeichnisse automatisierter Verarbeitungsverfahren und die mir gemeldeten Datenschutzbeauftragten vollständig sind. Darüber hinaus können die Beteiligungsberichte - auch nach der Gesetzesänderung - in Bezug auf die Frage, ob nach Sächsischem Datenschutzgesetz oder nach Bundesdatenschutzgesetz Daten verarbeitet werden, entscheidend sein.

Ich bitte daher die Kommunen und Landkreise, mir ihre Beteiligungsberichte weiterhin regelmäßig zuzustellen.

1.5 Der Dienstweg für Datenschutzbeauftragte nach § 11 SächsDSG

In 12/1.6 hatte ich mich bereits zu Fragen der Verschwiegenheit und zum Dienstweg im Zusammenhang mit Hinweisen an den Sächsischen Datenschutzbeauftragten geäußert.

Was die Stellung des Datenschutzbeauftragten nach § 11 SächsDSG angeht, so besteht zum Teil Unsicherheit darüber, ob sich der behördliche Datenschutzbeauftragte an einen Dienstweg zu halten hat, um mit dem Sächsischen Datenschutzbeauftragten in Kontakt zu treten und zu kommunizieren.

Mit der Änderung des Sächsischen Datenschutzgesetzes zum 1. Januar 2007 ist auch die gesetzliche Stellung des behördlichen Datenschutzbeauftragten gestärkt worden. Bereits nach der alten Fassung konnte der behördliche Datenschutzbeauftragte weisungsfrei seine Datenschutzaufgaben wahrnehmen, § 11 Abs. 2 Satz 2 SächsDSG. Er durfte wegen der Erfüllung seiner Aufgaben auch nicht benachteiligt werden, § 11 Abs. 2 Satz 3 SächsDSG. Da ihm nach der Bestimmung des § 11 Abs. 4 SächsDSG auch Verschwiegenheit auferlegt ist, verfügt der Datenschutzbeauftragte über eine gesetzliche Stellung als Vertrauensperson, als Ombudsmann. Dies wäre mit einer Verpflichtung, herkömmliche Dienstwege einzuhalten, nicht zu vereinbaren. Der Datenschutzbeauftragte nach § 11 SächsDSG hat eben kraft Gesetzes die Möglichkeit, sich weisungsfrei an andere zuständige Behörden zu wenden und um Unterstützung zu bitten oder diesem Hinweise zu dessen Aufgabenerfüllung zu geben. Mit der Gesetzesänderung ist die Befugnis des Datenschutzbeauftragten hinzugekommen, auch personenbezogene Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen, zu erheben, § 11 Abs. 3 SächsDSG. Müsste sich der behördliche Datenschutzbeauftragte bei Vorgängen dieser Art an einen Dienstweg halten, so würde er unbefugt Umstände und Verhältnisse offenbaren, die ihm nach Gesetz in seiner Dienststelle nur persönlich zugänglich sein sollen. Eine Verschwiegenheitspflicht besteht lediglich nicht gegenüber gesetzlich befugten Behörden, wie dem Sächsischen Datenschutzbeauftragten.

Als Ergebnis bleibt somit festzuhalten, dass der behördliche Datenschutzbeauftragte sich in Datenschutzfragen weisungsfrei z. B. an den Sächsischen Datenschutzbeauftragten wenden kann. Auch einen Erfahrungsaustausch mit Kollegen (Datenschutzbeauftragten) unter Berücksichtigung der jeweiligen Persönlichkeitsrechte halte ich von den Aufgaben des behördlichen Datenschutzbeauftragten her noch für zulässig.

1.6 Verwaltungsmodernisierung - E-Government

Wie bei allem Verwaltungshandeln erfordern auch E-Government-Projekte eine gesetzliche Legitimation, sofern die öffentliche Hand hierbei den Anspruch erhebt, personenbezogene Daten zu verarbeiten. Das Projekt „amt24“, das gegenwärtig noch von der Staatskanzlei verantwortet wird, ist ein ehrgeiziges Unternehmen, eine Internetplattform zu betreiben, auf der vielfältige Verfahren und Dienstleistungen der staatlichen und kommunalen Behörden gebündelt angeboten werden sollen. Perspektivisch ist u. a. vorgesehen, dass Profildaten von Nutzern der Internetpräsenz eingetragen werden - mithin auf Vorrat gespeichert werden dürfen - und für konkrete Anwendungen dem Nutzer wieder zur Verfügung gestellt werden können. Je stärker E-Government-Verfahren ein Interaktionsstadium erreichen, bzw. mehr als nur ein bloßes Formular-Portal darstellen, auf dem Dateien und Anträge durch den Bürger heruntergeladen werden können, desto mehr wird die die Internetpräsenz betreibende Stelle *Daten verarbeitende Stelle*. Derartige Entwicklungen muss man als Datenschützer nicht bedauern oder kritisieren. Konzentrationen, Zusammenarbeit und Zusammenschlüsse werden bei der Datenverarbeitung der öffentlichen Hand zunehmen, aus Kostengründen und auch weil der Bürger übersichtlichere Verfahren fordert. Auch bieten sich gerade anhand neuartiger Informationsflüsse Chancen. Insbesondere wird E-Government nach meiner Überzeugung auch dazu führen, dass viele Datenverarbeitungsprozesse geordneter und transparenter vonstatten gehen können. Datenschutzrechtlich entscheidend wird immer sein, dass sich die Rechte der Betroffenen gegenüber der herkömmlichen Datenverarbeitung nicht verschlechtern. Die innovative Verwaltung in Sachsen ist hierbei auf einem guten Weg. Dabei darf aber der eingangs erwähnte Rechtssatz nicht ins Hintertreffen geraten. Die Verwaltung bekommt Aufgaben und Zuständigkeiten nur durch Gesetz übertragen, vgl. Art. 83 Abs. 1 Satz 1 SächsVerf. Der Freistaat hätte die Möglichkeit durch ein entsprechendes Gesetz, ein „E-Government-Gesetz“, diesbezügliche Aufgaben - wie „amt24“ und die damit einhergehende Datenverarbeitung auf eine solide Grundlage zu stellen, als erstes Bundesland übrigens. Dies habe ich auch so empfohlen und werde gerne hierbei beraten.

Vgl. auch 14.1 zur Protokolldatenverarbeitung des Web-Auftritts der Staatsregierung.

1.7 Verfahrensverzeichnisse/Datenschutzbeauftragte

Bereits in 12/1.3 habe ich darauf hingewiesen, dass zahlreiche öffentliche Stellen des Freistaates Sachsen weder ihrer Verpflichtung zur Vorabkontrolle nach § 10 Abs. 4 SächsDSG noch der Verpflichtung zur Übersendung ihrer Verfahrensverzeichnisse

nach § 10 Abs. 3 SächsDSG nachkommen. Dies stellt sich zwar mittlerweile etwas anders dar, dennoch bestehen nach wie vor erhebliche Defizite. Wie ich bei Routinekontrollen in Stadtverwaltungen feststellen musste, ist manchen öffentlichen Stellen diese Pflicht bis zur Ankündigung meines Besuchs nicht einmal bekannt gewesen.

Ich weise daher erneut darauf hin, dass alle Daten verarbeitenden Stellen verpflichtet sind, mir sowohl vor dem erstmaligen Einsatz eines automatisierten Verarbeitungsverfahrens als auch regelmäßig zum 1. März das entsprechende Verfahrensverzeichnis zuzuleiten. Sofern sich gegenüber dem ursprünglich gemeldeten Verfahren keine Änderungen ergeben haben, ist es ausreichend, mir dies jährlich zum 1. März mitzuteilen.

Ein Verstoß gegen diese Pflicht zur Zuleitung stellt seit dem Inkrafttreten des novellierten Sächsischen Datenschutzgesetzes gemäß § 38 Abs. 1 Nr. 3a SächsDSG eine Ordnungswidrigkeit dar und kann mit einer Geldbuße bis zu 25.000 € geahndet werden.

Sowohl die Verpflichtung zur Vorabkontrolle als auch die zur Zuleitung der Verfahrensverzeichnisse entfallen nur bei der Bestellung eines behördlichen Datenschutzbeauftragten nach § 11 SächsDSG. Aus gegebenem Anlass weise ich darauf hin, dass dieser gemäß § 11 Abs. 2 Satz 1 SächsDSG durch die Bestellung keinem Interessenkonflikt mit seinen sonstigen beruflichen Aufgaben ausgesetzt werden darf. In meiner Bekanntmachung zu Datenschutzbeauftragten öffentlicher Stellen (vgl. 16.1.2) weise ich unter 1.4 darauf hin, dass sich insbesondere bei Bediensteten aus dem Bereich der Personalverwaltung, des Organisationswesens, der Datenverarbeitung oder des Personalrats regelmäßig Spannungsverhältnisse zur eigentlichen Hauptaufgabe ergeben. Unzulässig ist weiterhin die Bestellung von Mitarbeitern in leitenden Funktionen, die in einem besonderen dienstlichen Näheverhältnis zum Leiter der Stelle/Behördenleiter stehen und deren Bestellung regelmäßig im Übermaß Interessenkonflikte hervorrufen würde (z. B. bei Stellvertretern des Leiters, Personalamtsleitern usw.).

Einige Behörden teilten mir dennoch mit, dass sie insbesondere an der Bestellung von Mitarbeitern aus dem Bereich der Datenverarbeitung festhalten, da nur diese überhaupt in der Lage wären, den Interessen des Datenschutzes wirksam Geltung zu verschaffen. Hierbei wird aber offensichtlich übersehen, dass der zu Kontrollierende nicht selbst der Kontrolleur sein darf. Nach meiner, bereits im 12. Tätigkeitsbericht geäußerten Auffassung, bietet sich insbesondere die Bestellung von Mitarbeitern aus

dem Rechnungswesen, der Rechnungsprüfung, dem Controlling oder der Organisation an.

Das SMI hat dankenswerterweise ebenfalls entsprechende Hinweise zur Bestellung von Datenschutzbeauftragten öffentlicher Stellen im Freistaat Sachsen veröffentlicht. Sie sind im Internet unter http://www.sachsen.de/de/bf/staatsregierung/ministerien/smi/smi/upload/Hinweise_DSB.pdf zu finden. Nachdem auch diese nicht alle Kommunen überzeugten, habe ich gegenüber dem SMI angeregt, im Wege der Kommunalaufsicht tätig zu werden. Dies hat das SMI zunächst zum Anlass genommen, in einem Rundschreiben noch einmal ausdrücklich darauf hinzuweisen, dass der Prüfung eines möglichen Interessenkonflikts besondere Aufmerksamkeit zu widmen ist.

Sofern sich kein geeigneter Mitarbeiter findet, steht es jeder Behörde frei, einen Mitarbeiter z. B. aus dem Bereich der Datenverarbeitung *intern* mit der Koordinierung des Datenschutzes zu beauftragen. Dieser kann die Koordinierung der an mich zu übersendenden Verfahrensverzeichnisse sowie Vorabkontrollen übernehmen. Er ist jedoch kein Datenschutzbeauftragter i. S. d. § 11 SächsDSG.

In diesem Zusammenhang weise ich auf die Aktualisierungen meiner Bekanntmachungen (einschließlich der jeweiligen Formulare) zum Verzeichnis automatisierter Verarbeitungsverfahren, zur Vorabkontrolle und zu Datenschutzbeauftragten öffentlicher Stellen hin, die durch das am 1. Januar 2007 in Kraft getretene Gesetz zur Änderung des Sächsischen Datenschutzgesetzes vom 14. Dezember 2006 notwendig wurden. Diese sind sowohl in diesem Tätigkeitsbericht als auch unter www.datenschutz.sachsen.de veröffentlicht.

2 Parlament

2.1 Kleine Anfrage zu den Namen von Anmeldern einer Gegendemonstration

Ein Mitglied des Sächsischen Landtages fragte im Rahmen einer Kleinen Anfrage nach den Namen der „Anmelder“ einer Demonstration politischer Gegner. Die durch die Staatsregierung um Auskunft gebetene Versammlungsbehörde, ein Landratsamt, erkundigte sich bei mir, ob es die Namen der Personen, die die Versammlung angemeldet hatten, nennen dürfe.

Ich habe wie folgt geantwortet:

Das Versammlungsgesetz kennt den Begriff des „Anmelders“ nicht. Vielmehr kennt § 2 Abs. 1 VersammlG nur die „Anmeldung“, die durch den Veranstalter zu erfolgen hat. § 14 Abs. 2 VersammlG kennt noch den Begriff des Versammlungsleiters, der zumeist nicht mit der Person identisch ist, die die Versammlung gegenüber der Versammlungsbehörde angemeldet hat. Veranstalter ist in der Regel eine Untergliederung einer politischen Partei, einer Gewerkschaft, einer sonstigen Gruppierung und ausnahmsweise auch ein einzelner Mensch. Die Frage nach dem „Namen des Anmelders“ kann also nur als Frage nach dem „Namen der Veranstalters“ oder allenfalls nach dem „Namen des Versammlungsleiters“ ausgelegt werden.

Hinzu kommt: Für das parlamentarische Informationsinteresse des anfragenden Abgeordneten kann nicht von Interesse sein, welche konkrete Person gegenüber der Versammlungsbehörde eine Demonstration angemeldet hat, sondern nur, welche andersdenkende Organisation als Veranstalter einer Gegendemonstration aufgetreten ist.

Im Übrigen weise ich auf meine Ausführungen unter 11/5.9.3 hin.

2.2 Einsicht in Unterlagen des Petitionsausschusses

Ein Bürger fragte mich, ob er in „seine“ Petitionsakte beim Petitionsausschuss des Sächsischen Landtages unmittelbar Einsicht nehmen dürfe. Er streite sich darüber mit der Landtagsverwaltung, die ihm wegen seines früheren Verhaltens in dieser Angelegenheit lediglich Kopien übersenden wolle.

Gegenüber dem Petitionsausschuss, einem Organ der ersten Gewalt, nehme ich aus verfassungsrechtlichen Gründen nur beratend Stellung. Dem Petenten habe ich meine beratende Äußerung gegenüber dem Parlament sinngemäß mitgeteilt.

Danach steht einem Petenten nach § 18 Abs. 3 SächsDSG - eine bereichsspezifische Rechtsvorschrift existiert nicht - grundsätzlich ein Recht auf Einsicht in die zu seiner Person beim Petitionsausschuss des Sächsischen Landtages geführten Petitionsakte zu. Der Einsichtsanspruch nach § 18 Abs. 3 SächsDSG - eine sächsische Besonderheit - ist ein Mehr gegenüber der Auskunft und gewährt dem Betroffenen oder seinem Bevollmächtigten ein Recht auf die unmittelbare Einsichtnahme in die Originalakte.

Die Einsicht kann unterbleiben, soweit Teile der Akte den internen Willensbildungsprozess im Petitionsausschuss abbilden oder wegen überwiegender berechtigter Interessen eines Dritten oder wegen einer Rechtsvorschrift geheim gehalten werden

müssen, § 18 Abs. 3, 5 SächsDSG. Vom Einsichtsrecht sind daher nicht erfasst die Teile der Petitionsakte, die die ausschussinterne Willensbildung der Abgeordneten abbilden. Dabei kann es sich z. B. um Sitzungsprotokolle und Notizen des Petitionsausschusses handeln. Als entgegenstehendes Recht Dritter kommt insbesondere das Grundrecht auf Datenschutz in Betracht. Die Rechte nach § 18 SächsDSG sollen dem Betroffenen ermöglichen, sich Kenntnis von *der zu seiner Person* gespeicherten Daten zu verschaffen. Sie schaffen kein Recht auf Kenntnisnahme (bis auf ganz wenige Ausnahmen) auch der Daten Dritter.

Praktisch sollte die Landtagsverwaltung vor der Einsichtnahme die Aktenteile entfernen, die den ausschussinternen Willensbildungsprozess abbilden oder deren Kenntnisnahme mit dem Grundrecht auf informationelle Selbstbestimmung Dritter oder mit Rechtsvorschriften über die Geheimhaltung nicht vereinbar ist. Ist dies unmöglich, da Daten untrennbar miteinander verbunden sind, müssen die betreffenden Seiten kopiert, geschwärzt und wieder kopiert werden.

Bestehen tatsächliche Anhaltspunkte für die Annahme, dass die Einsichtnahme zu einer Störung der öffentlichen Ordnung und Sicherheit im Sächsischen Landtag führen wird, müssen geeignete technisch-organisatorische Vorkehrungen für eine möglichst störungsfreie Einsichtnahme (z. B. separater Raum, Aufsicht durch Polizei etc.) getroffen werden. Ausnahmsweise kommen auch andere geeignete Wege zur Wahrung des Grundrechts des Betroffenen auf Kenntnis der in den Akten zu seiner Person enthaltenen Daten in Betracht, etwa die Übersendung von Kopien.

Sinnvoll wäre eine bereichsspezifische Regelung des Auskunfts- und Einsichtsrechts des Betroffenen im Petitionsausschussgesetz.

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 Einbehalten privater Telefongebühren im Gehaltsabzugsverfahren

In 4/5.1.26 habe ich die Auffassung vertreten, dass der Einzug von Gebühren für Privatgespräche im Gehaltsabzugsverfahren datenschutzrechtlich unzulässig sei.

Begründet habe ich dies damit, dass die Einwilligung in das Gehaltsabzugsverfahren nicht § 4 Abs. 1 Nr. 2 SächsDSG entspräche, da sie nicht völlig frei von jedwedem Zwang erteilt würde. Die Alternative „entweder Sie geben uns die Einwilligung oder Sie erhalten keine PIN, dürfen also keine Privatgespräche führen“ stelle die Betroffenen vor eine Zwangssituation, die mit „Freiwilligkeit“ nichts mehr zu tun habe.

Dies stellt nicht mehr meine Auffassung dar. Mittlerweile bieten zahlreiche Mobilfunkanbieter eine (zum Teil sogar kostengünstigere) Möglichkeit, Privatgespräche von der Dienststelle zu führen. Es ist daher davon auszugehen, dass die Einwilligung in das Gehaltsabzugsverfahren auch dann freiwillig erfolgt, wenn anderenfalls die Möglichkeit, Privatgespräche vom Dienstapparat führen zu können, entfallen würde.

Der Einzug von Gebühren für Privatgespräche im Gehaltsabzugsverfahren ist daher datenschutzrechtlich nicht mehr zu beanstanden.

5.1.2 Ressortübergreifende Personalvermittlungsplattform

Das SMF setzte mich darüber in Kenntnis, dass zur Unterstützung eines ressortübergreifenden Personalaustauschs (zur Unterstützung des Stellenabbaukonzepts und wegen des damit verbundenen Einstellungsstopps) die Einrichtung einer virtuellen datenbankgestützten Personalvermittlungsplattform (PVP) geplant sei. Diese soll aus den Datenbankbereichen „Ausschreibungen“ und „Personalprofile“ bestehen.

Im ersten Bereich sollen alle ressortübergreifenden und öffentlichen Ausschreibungen eingestellt werden und für alle Beschäftigten des Freistaates Sachsen über das „Landesweb“ einsehbar sein. In dieser Datenbank werden keine personenbezogenen Daten verarbeitet, es bestehen insoweit keine datenschutzrechtlichen Bedenken.

Im Bereich „Personalprofile“ sollen hingegen ausgewählte Personaldaten („Stammdaten“) von Beschäftigten eingestellt werden, die sich entweder eigenständig für einen ressortübergreifenden Einsatz bewerben oder die „auf der Grundlage von Organisationsentscheidungen und aufgabenkritischer Betrachtung der Arbeitsbereiche zur ressortübergreifenden Verwendung zur Verfügung stehen“. Hier ist ein lesender

Zugriff für die Personal verwaltenden Stellen aller obersten Dienstbehörden, jedoch nur für diese, vorgesehen. Im Rahmen von konkreten Stellenbesetzungsverfahren sollen über die Stammdaten hinausgehende Personaldaten übermittelt werden.

In einer ersten Stufe sollten die eigenständigen Bewerbungen durch eine Verwaltungsvorschrift (VwV PVP) geregelt werden. Ein Sächsisches Personalvermittlungsplattformgesetz wurde erst für die zweite Stufe vorgesehen, in der auch ohne Einwilligung des Beschäftigten seine Personaldaten in die PVP eingestellt werden sollen.

Zunächst hatte ich zu prüfen, ob das SMF für die Einrichtung der PVP zuständig war. Art. 83 Abs. 1 SächsVerf bestimmt, dass Aufbau, räumliche Gliederung und Zuständigkeiten der Landesverwaltung durch Gesetz geregelt werden müssen. Lediglich die Einrichtung der Behörden im Einzelnen obliegt gemäß Art. 83 Abs. 2 SächsVerf der Staatsregierung. Dazu führt das OVG im Urteil vom 24. September 1998 (SächsVBl. 1999 S. 18) aus: „*Demzufolge kann die Staatsregierung aufgrund ihrer Organisationskompetenz zur Einrichtung von staatlichen Behörden zwar deren konkrete Einrichtung, nicht aber deren Aufbau, räumliche Gliederung und Zuständigkeit bestimmen*."

Eine derartige gesetzliche Grundlage war vorliegend aber gegeben. Nach § 8 SächsHG 2007/2008 sollen die im Haushaltsplan ausgewiesenen Planstellen und Stellen des Personalsolls A bis 2010 auf 80.000 Planstellen und Stellen zurückgeführt werden. Zur Durchführung des Sächsischen Haushaltsgesetzes 2007/2008 kann das SMF als zuständige Behörde Verwaltungsvorschriften erlassen (vgl. § 14 SächsHG 2007/2008).

Die im Rahmen dieser Zuständigkeit geplante Verarbeitung personenbezogener Daten muss dabei weiterhin den datenschutzrechtlichen Regelungen, insbesondere dem Sächsischen Beamtengesetz entsprechen.

§ 124 Abs. 1 Satz 3 SächsBG bestimmt, dass andere Behörden nur Zugang zu Personalaktendaten im Wege automatisierter Datenabrufe auf Grundlage besonderer Rechtsvorschrift haben dürfen. Die Konzeption zur PVP sieht vor, dass andere Geschäftsbereiche, d. h. andere oberste Dienstbehörden des Freistaates im Wege des automatisierten Abrufs Zugang zu Personalaktendaten bekommen können sollen, was eine gesetzliche Regelung letztendlich notwendig macht. Es handelt sich dabei auch um ein automatisiertes Abrufverfahren im Sinne von § 8 SächsDSG. Vorabkontrolle und Beteiligung der Personalräte sind erforderlich, § 10 Abs. 4 SächsDSG.

Im Hinblick auf einen Gesetzentwurf bat ich daher das SMF, mich weiter zu unterrichten.

5.1.3 Das neue Stasi-Unterlagen-Gesetz - Überprüfung von Mitarbeitern und Mandatsträgern

Mit Wirkung zum Ende des Jahres 2006 ist eine vom Bundestag verabschiedete Novellierung des Stasi-Unterlagen-Gesetzes in Kraft getreten. Nach der alten Fassung des Gesetzes sollte die Überprüfung von Mandatsträgern und Beschäftigten im öffentlichen Dienst zum Ende des Jahres 2006 - nach 15 Jahren - wegen eines durch Zeitablauf begründeten Resozialisierungsinteresses auslaufen, § 20 Abs. 3, § 21 Abs. 3 StUG a. F. So hatte es der Gesetzgeber damals vorgesehen. Mit Herannahen dieses Zeitpunktes setzte noch einmal ein erneuter politischer Diskurs und intensive Bemühungen ein, um eine Verlängerung der Überprüfungspraxis zu erreichen. Dies mündete in einer modifizierten Fassung der Vorschriften des § 20 und des § 21 StUG, die im Wesentlichen für die (Personal-)aktenführung des öffentlichen Dienstes und die Kommunen von Bedeutung ist.

In Sachsen sind die Unterlagen im Zusammenhang mit Überprüfungen nach dem Stasi-Unterlagen-Gesetz, soweit es Beschäftigte des öffentlichen Dienstes betroffen hat, regelmäßig in den Personalakten geführt worden. Dabei sind die Überprüfungsakten innerhalb des Personalakts zumeist besonders gesichert worden, zum Beispiel durch das Verschließen der Unterlagen in einem gesicherten Umschlag. Die Überprüfungsakten von Mandatsträgern hingegen sind in jedem Fall als personenbezogene Sachakten zu führen gewesen. Zum Umgang mit BStU-Unterlagen, vgl. 2/5.1.3 und 10/5.1.5 (für viele Bestimmungen auch *VwVPersAktenB* A I.5.), auch 7/5.1.16, 7/5.1.17 sowie 9/5.1.14.

Mit der Gesetzesänderung ist nur noch ein eingegrenzter Teil von Beschäftigten überprüfbar, § 20 Abs. 1 Nr. 6, § 21 Abs. 1 Nr. 6 StUG. Für den Freistaat Sachsen sind insbesondere die kommunalen Wahlbeamten (Absatz 6b), Beamte, die jederzeit in den einstweiligen Ruhestand versetzt werden können (auch Angestellte in entsprechender Funktion) (Absatz 6c), Beamte und Angestellte, die eine Behörde leiten oder eine vergleichbar verantwortungsvolle Aufgabe wahrnehmen (Absatz 6d), Berufsrichter (Absatz 6e) sowie Personen, die sich um derartige Ämter bemühen, zu nennen. Damit kann eine Überprüfung in der bisher erfolgten Breite, was Beamte und Angestellte angeht, nicht mehr fortgesetzt werden. Erwähnenswert ist an dieser Stelle auch, dass herausgehobene Vertreter und Beschäftigte juristischer Personen des Privatrechts nach neuer Gesetzeslage nicht mehr überprüft werden können. Dies gilt

somit u. a. auch für Betriebe der Kommunalwirtschaft, wie Stadtwerke und Personennahverkehrsgesellschaften, die als juristische Personen des Privatrechts von öffentlichen Stellen im Sinne des Sächsischen Datenschutzgesetzes beherrscht werden (vgl. § 2 Abs. 2 SächsDSG). Nach Absatz 7 können darüber hinaus Personen, die beruflich mit Stasi-Unterlagen, Rehabilitierungsangelegenheiten und mit Aufarbeitungsfragen in Bezug auf Herrschaftsmechanismen der ehemaligen DDR oder der sowjetischen Besatzungszone befasst sind bzw. sich um eine diesbezügliche Einstellung bewerben, überprüft werden. Eine Überprüfung bleibt auch weiterhin im Zusammenhang mit Sicherheitsüberprüfungen nach dem Sächsischen Sicherheitsüberprüfungsgesetz - und auch dies betrifft Beschäftigte des öffentlichen Dienstes - möglich, § 20 Abs. 1 Nr. 11, § 21 Abs. 1 Nr. 8 StUG.

Abgesehen von den Beschäftigten sind die Überprüfungen von Abgeordneten, Angehörigen kommunaler Vertretungskörperschaften und ehrenamtlichen Richtern (diese sind neu aufgeführt) zu nennen, Abs. 1 Nr. 6b bzw. e. Im kommunalen Bereich bleibt daher weiterhin eine Überprüfung von Gemeinderäten und Kreisräten möglich. Gegenüber dem bisherigen Anwendungsbereich ist die sachfremde Überprüfung von Vertretern aus dem Sportbereich nach Absatz 1 Nr. 6g hinzugekommen. Neu sind u. a. auch Überprüfungen nach dem Luftsicherheitsgesetz und dem Atomgesetz, § 20 Abs. 1 Nr. 12, § 21 Abs. 1 Nr. 9 StUG, die, da u. a. auch die Zuverlässigkeit nach dem Waffengesetz oder dem Bundesjagdgesetz mit Hilfe von Überprüfungen nach dem Stasi-Unterlagen-Gesetz weiterhin bestehen bleiben soll, insofern konsequent sind.

Nach § 20 Abs. 3, § 21 Abs. 3 StUG ist eine Verwendung für die in Absatz 1 Nr. 6 genannten Zwecke nach dem 31. Dezember 2011 unzulässig. Akten bei den Behörden, die im Zusammenhang mit Alt-Überprüfungen angefallen sind, sollen nach Absatz 3 Satz 2 dem Bundes- oder dem zuständigen Landesarchiv angeboten werden. Für die staatlichen Stellen bedeutet dies, dass Personalaktenteile im Zusammenhang mit einer Überprüfung nach dem Stasi-Unterlagen-Gesetz zusammengeführt, von der Hauptakte separiert und zunächst gesichert aufbewahrt werden können. Nach Absatz 3 Satz 1 ergibt sich gleichwohl weiterhin, dass die Aktenteile, soweit es erforderlich ist, noch genutzt werden können. Soweit eine Nutzung aber nicht mehr erforderlich ist, kann bereits jetzt sukzessive mit einer Anbietung an das Landesarchiv begonnen werden. Wegen der fortwirkenden Zweckbindung des Stasi-Unterlagen-Gesetzes begegnet eine solche Vorgehensweise keinen datenschutzrechtlichen Einwänden, auch nicht im Hinblick auf den Grundsatz der Vollständigkeit der Personalakte (bei personenbezogenen Sachakten greift diese Problematik ohnehin nicht) - im Gegenteil. Soweit die Überprüfungsvorgänge in den Personalakten geführt

worden sind, erstreckt sich der Regelungsbereich des Stasi-Unterlagen-Gesetzes - und der weite Verwendungsbegriff (vgl. § 6 Abs. 9 StUG) - nämlich auch auf diese Aktenteile. Insbesondere ist es nach der klaren spezialgesetzlichen Fassung von Absatz 3 Satz 1 nicht möglich abzuwarten, bis die Personalakte als Ganzes abgeschlossen wird bzw. dem Staatsarchiv anzubieten ist. Die Überprüfungsvorgänge sind somit auch bei der Personalaktenführung gesondert zu behandeln. Pflichtig bis spätestens zum Ende der Frist zum Ende des Jahres 2011 tätig zu werden, sind nicht nur die Personalverwaltungen selbst, sondern auch alle anderen Stellen, die Überprüfungsvorgänge geführt haben, wie zum Beispiel die im staatlichen Bereich eingerichteten Personalkommissionen oder, was die Abgeordneten und Mandatsträger betrifft, die Stellen, die Unterlagen über diese geführt haben, Kommunen und Kommunalaufsichtsbehörden. Zur Einordnung der Unterlagen der Personal- und Fachkommissionen in die Personalakten, vgl. 1/5.1.6.

In der Gesetzesfassung bleiben die kommunalen Archive als Stellen, an die anzubieten wäre, unerwähnt. Da öffentlichen Stellen der Zugang zu den Unterlagen und die Verwendung nur im Rahmen des Stasi-Unterlagen-Gesetzes selbst gestattet ist - so bestimmt es § 4 Abs. 1 StUG - findet eine Archivierung bzw. eine Übermittlung zur Archivierung in Kommunalarchiven keine gesetzliche Stütze. Vorstellbar wäre noch, dass Aktenteile im Zusammenhang mit Alt-Überprüfungen der Kommunen oder Kommunalbehörden der BStU zurückgegeben werden. Eigene Bewertungen oder selbst erstellte Aktenstücke der Kommunen innerhalb der Überprüfungsvorgänge könnten ggf. vernichtet werden, soweit sich keine Zuständigkeit der BStU hierfür begründen lässt.

Nach dem Sächsischen Beamtengesetz besteht die Möglichkeit für die Beamten, dass Unterlagen, die für den Beamten ungünstig sind oder ihm nachteilig werden können, auf seinen Antrag hin nach Fristablauf zu entfernen bzw. zu vernichten sind, § 122 Abs. 1 Nr. 2 SächsBG. Vom Wortlaut her betrifft das auch die Meinungen enthaltenden Einschätzungen und Bewertungen der Dienststellen, die diese anhand der ihnen von der BStU zur Verfügung gestellten Unterlagen getroffen haben. Inwieweit neben der Archivierungsanbietungs-Bestimmung des Absatzes 3 die beamtenrechtlichen Berichtigungs- und Tilgungsansprüche Bestand haben und inwieweit sie mit der Neufassung des Stasi-Unterlagen-Gesetzes kollidieren, wäre gemeinsam mit den staatlichen Stellen genauer zu betrachten. Was den Angestelltenbereich angeht, wird man ggf., soweit keine Regelungen des Beamtengesetzes anwendbar gemacht worden sind, den Einzelfall zu betrachten haben.

Soweit Überprüfungsvorgänge zu Beschäftigten, Mandatsträgern oder anderen Personen sowohl als Alt-Überprüfungen vorliegen, als auch nach neuer Gesetzeslage durchgeführt werden können, können bereits zu diesen Personen angelegte Akten fortgeführt werden. Bei Personen, die Absatz 1 Nr. 6 unterfallen, allerdings nur bis Ende des Jahres 2011.

5.1.4 Personalaktenführung: Aktenstücke, die nicht in die Personalakte gehören

Bei meinen Kontrollen stelle ich immer wieder fest, dass sich in den Personalakten Kopien von Unterlagen befinden, die nicht in die formelle Akte gehören. Der öffentliche Dienst - auch in der Personalverwaltung - neigt nicht selten dazu, sich abzusichern. Man sammelt z. T. Unterlagen nach dem Motto „Vielleicht braucht man es ja doch noch einmal“.

Bei fast jeder meiner Kontrollen, insbesondere im kommunalen Bereich, stelle ich Kopien von Ausweisdokumenten fest. In der Regel handelt es sich dabei um Personalausweiskopien, selten Ablichtungen von Reisepässen. Kopien von derartigen Ausweisdokumenten sind regelmäßig für eine Personalaktenführung nicht erforderlich. Selbst wenn man davon auszugehen hat, dass zum Nachweis der Staatsangehörigkeit Ausweisdokumente vorzulegen sind, so bedeutet dies nicht, dass diese Dokumente abzulichten und in den Personalakt aufzunehmen sind. Die Verwaltung soll sich der Staatsangehörigkeit versichern. Das ist der Sinn der Vorlage. Sie genügt hierfür in der Regel auch zum Nachweis (vgl. 1.2 der Verwaltungsvorschrift des SMI zur Begründung und Beendigung eines Beamtenverhältnisses vom 11. August 1997). Soweit eine bloße Vorlage doch nicht der Erforderlichkeit genügt, so können hierfür vorgesehene entsprechende Staatsbürgerschaftsurkunden verlangt werden, so etwa im Fall einer anstehenden Verbeamtung. Die Speicherung der Ausweisdaten mit ihren überschießenden Informationen betrachte ich hingegen als nicht datenschutzgerecht. Die Ausweisdaten, beziehungsweise die Kopien der Ausweise sind aus den Personalakten zu entfernen. Auch bei EU-Staatsbürgern wird in der Regel ebenso eine Vorlage der Ausweisdokumente genügen. Bei Fragestellungen zur Arbeitserlaubnis bei Angestellten oder Arbeitern aus EU-Drittstaaten ergeben sich die entscheidenden Angaben bereits gesetzlich aus den im Reisepass vermerkten Aufenthaltstiteln. Auch dann genügt eine Vorlage.

Personenstandsurkunden, die für die Bezügerechnung noch entscheidend sein mögen, sollten ebenfalls nur bei Erforderlichkeit vorgelegt bzw. in den Personalakten geführt werden. Für den Fall, dass die Bezügerechnung - wie bei der Staatsverwaltung -

getrennt erfolgt, können weitergehende Angaben zu Beschäftigten und zu den Kindern der Beschäftigten ausschließlich bei der Organisationseinheit verarbeitet werden, die die Bezügerechnungen vornimmt. In diesen Fällen, bei der aufgeteilten Verwahrung der Personalakte, sollte der Grundsatz der Datensparsamkeit Beachtung finden. Es genügt, wenn in der Grundakte die Anzahl der Kinder und deren Geburtsjahre im Personalbogen vermerkt sind.

Neben Ausweisdokumenten befinden sich in den Personalakten nicht selten auch noch andere Unterlagen, die sachlich nicht in die Personalakten gehören. Andere Unterlagen, die als Aktenstücke in gleicher Weise - wie die Ausweiskopien - auszusondern sind bzw. bereits im Vorfeld von der Personalakten führenden Stelle als nicht aktenrelevant abzuweisen wären, können sein: Glückwunschschreiben von Dienstherrn (soweit nicht, wie bei Dienstjubiläen oder bei Leistungsstufen- und Leistungsprämien gesetzlich begründet), private Dankschreiben, vorbereitende Notizen (auch in Bezug auf die Leistung von Beschäftigten), inhaltliche Aufzeichnungen aus den Bewerbungsgesprächen oder Vorgesetzten-Mitarbeiter-Gesprächen, bis hin zum Scheidungsurteil mit seinen Gründen. Es gibt natürlich auch Grenzfälle. Im Einzelfall zu prüfen wären weiterhin etwa Nachweise zu privaten Fortbildungsmaßnahmen mit dienstlichem Bezug oder Unterlagen, aus denen sich die Verleihung eines staatlichen Ordens oder eines Ehrenzeichens ergibt.

Personalaktenstücke im Zusammenhang mit einer Überprüfung nach dem Stasi-Unterlagen-Gesetz sind im Regelfall wegen der neuen Gesetzeslage zusammenzuführen, zu separieren und gesichert aufzubewahren (mind. in einem geschlossenen Umschlag oder einem extra hierfür eingerichteten Schrank, vgl. hierzu die Ausführungen unter 5.1.3).

5.1.5 Zur Verwendung von Daten aus DDR-Personal-Altakten, insbesondere Personalbögen

In 9/5.1.4 hatte ich mich dafür eingesetzt, dass die alten (zum Teil noch aus DDR-Zeiten stammenden), sowie die in neuerer Zeit verwendeten, jedoch nicht datenschutzgerechten, Personalbögen ausgetauscht und in einem verschlossenen Umschlag zur Personalakte genommen werden. Weiterhin halte ich daran fest, dass alte Personalbögen, die zusätzliche, d. h. überschießende Daten, wie Partei- und Gewerkschaftszugehörigkeit enthalten können, nicht als Personalbogen Weiterverwendung finden dürfen. In DDR-Personalbögen habe ich Angaben gefunden wie „Soziale Herkunft - Intelligenz“, Angaben zur Scheidung, Daten zu einer Einstellung oder Bewerbung beim „MDI“ und Gründe, weshalb keine Einstellung erfolgt ist, Angaben zu

Teilnahmen an Veranstaltungen von Parteien oder Massenorganisationen, zu Wehrmachtszugehörigkeit bzw. „bewaffneten Organen der DDR“, zur „Mitarbeit bei gesellschaftlichen Kommissionen bzw. dem Aktiv“, tiefer gehende Angaben zu Ehepartnern (auch dessen Berufstätigkeit) und Kindern, sämtliche bisherigen Wohnanschriften, zu Verwandten in der „BRD“, „anderen Staaten“ oder „Berlin-West“, Angaben über „Belobigungen und Prämierungen“ sowie ein handschriftlicher Lebenslauf.

Bisher habe ich die Auffassung vertreten, dass alte Personalbögen nicht an die Beschäftigten zurückgegeben oder vernichtet werden dürfen. Begründet habe ich dies mit dem Grundsatz der Vollständigkeit der Personalakte, d. h., dass Unterlagen nur unter den Voraussetzungen des § 122 SächsBG aus dieser entfernt werden dürfen. Datenschutzgerecht sei es, die überholten Personalbögen in einem verschlossenen, entsprechend gekennzeichneten Umschlag bei der jeweiligen Personalakte - oder auch gesondert, so z. B. wie die Unterlagen der BStU - aufzubewahren. Zur neuen Rechtslage nach dem Stasi-Unterlagen-Gesetz (vgl. 5.1.3).

Zutreffend ist, dass grundsätzlich von einer einheitlichen, also durchgehend zu führenden Personalakte auszugehen ist, die das Beschäftigungsverhältnis sowohl vor als auch nach der Wiedervereinigung umfasst, denn nach dem Einigungsvertrag endete ein Beschäftigungsverhältnis mit der bundesstaatlichen Neuordnung nicht automatisch. Die Personalunterlagen dienen dazu, den gesamten beruflichen Werdegang eines Mitarbeiters aufzuzeichnen, was in dem zu beachtenden personalaktenrechtlichen Grundsatz der „Vollständigkeit und Richtigkeit der Personalakten“ zum Ausdruck kommt.

Eine Zulässigkeit der Speicherung von Unterlagen aus den Vorgängerpersonalakten oder aus Alt-Sachakten kann aufgrund der Erforderlichkeit für die Dokumentation des unmittelbaren Zusammenhangs mit dem Dienstverhältnis gemäß § 117 SächsBG aber nur für die Urkunden gesehen werden, die zum Nachweis eines lückenlosen Lebenslaufs dienen können (Abschlusszeugnisse u. ä.) oder für die Übernahme in die Dienstlaufbahn relevant waren. Alle übrigen Altunterlagen sind umgehend aus der Hauptpersonalakte zu entfernen, da sie nach den beamtenrechtlichen Bestimmungen nicht in die Personalakte hätten aufgenommen werden dürfen.

Insofern sind im Ergebnis generell alle öffentlichen Stellen von Amts wegen gehalten, Personalbögen mit sachfremdem Inhalt und andere nicht zweckbestimmte, den Beschäftigten betreffende Unterlagen, unabhängig von antragsabhängigen Berichtigungs- und Tilgungsbestimmungen aus den Personalakten zu entfernen. Der-

artige Dokumente sind den Beschäftigten dabei vorzugsweise - auch wenn der Betroffene nach dem Gesetz keinen Anspruch haben mag, diese Unterlagen zu erhalten - anzubieten, d. h. auszuhändigen oder mit deren Kenntnis zu vernichten.

Durchaus problematisch kann auch die Verbindung von das Dienstverhältnis unmittelbar betreffenden Angaben, mit z. T. sachfremden Angaben sein, wie z. B. bei Abschlusszeugnissen aus der DDR-Zeit, die neben eignungsbegründenden Bewertungen u. a. Angaben über politische Einstellungen und die gesellschaftliche Eignung enthalten können. Hier wird man einzelfallbezogen abzuwägen haben. In der Rechtspraxis werden die Zeugnisse regelmäßig ohne Schwärzungen in den Personalakten aufbewahrt. Einstellungsvorschläge oder andere Schriftstücke, die mit dem aktuellen Dienstverhältnis in keinem Zusammenhang stehen, sollten zumindest gesperrt in einem geschlossenen Umschlag verwahrt bzw. auf vollständige Entfernung aus den Akten geprüft werden. In derartigen Unterlagen sind z. T. Einzelangaben zu finden, die nicht vertretbar offen in den Personalakten verwahrt werden können, wie z. B. „Genosse … ist Mitglied der Partei und weiter in der FDJ, DSF, FDGB und DTSB organisiert.“, „Seine 3-jährige Dienstzeit im Wachregiment trug wesentlich zur Formung seiner Persönlichkeit bei und schuf die Grundlage dazu, dass er seine Kraft weiterhin zum bewaffneten Schutz unseres Staates zur Verfügung stellt.“, „Von Seiten der Familie … gibt es keinerlei Westkontakte.“. Zwischeneineinschätzungen, „Attestationen“, „Beurteilungen“ und Vorschlagsblätter können wiederum Angaben zu Parteiaktivitäten und zur Beschäftigung mit „polit-aktuellen Themen“, die Verleihung von Auszeichnungen und Einzelangaben zu höchstpersönlichen Lebensbereichen enthalten. Die Beispiele ließen sich beinahe endlos fortsetzen, anhand von ihnen lässt sich aber abschätzen, um welche tiefgehende Datenverarbeitungsvorgänge es gehen kann. Auch innerhalb des informationell abgeschotteten Bereichs der Personalverwaltung sollte dem Rechnung getragen werden. Zu anderen auszusondernden Unterlagen (vgl. 5.1.4).

Die aufgestellten Grundsätze aus den vorstehenden Überlegungen haben bei der Staatsverwaltung gemäß 2.1 VwV Personalakten für die Personalaktenführung von Arbeitern und Angestellten in gleichem Maße zu gelten.

Bezug nehmend auf den 9. Tätigkeitsbericht halte ich es weiterhin nicht nur für das Recht, sondern auch die Pflicht einer öffentlichen Stelle, alte DDR-Personalbögen auszutauschen. Wenn die Beschäftigten im Zuge der Austauschaktion gebeten werden, einen neuen Personalbogen auszufüllen, so ist die damit verbundene Datenerhebung im Sinne von § 37 Abs. 1 SächsDSG erforderlich und somit zulässig.

Wie ich bei Kontrollen feststellen musste, sind aber auch die neuen Personalbögen oft nicht datenschutzgerecht. Ich empfehle daher die Verwendung des Personalbogens der Anlage 1 der *Verwaltungsvorschrift des SMI zur Begründung und Beendigung eines Beamtenverhältnisses* (SächsABl. 1997, 1060 ff.). Dieser ist mit mir abgestimmt (vgl. 6/5.1.1).

5.1.6 Beanstandung wegen des Ausdrucks privater E-Mails bei einer Landesbehörde

Ich wurde darüber informiert, dass in einem Landesamt der gesamte E-Mail-Verkehr eines Mitarbeiters ausgedruckt wurde. Zu diesem Zeitpunkt hatte die Landesbehörde keine Regelung zur privaten Nutzung von Internet oder E-Mail. Die damalige Amtsleitung hat nach eigenen Angaben vielmehr ihre Mitarbeiter aufgefordert, möglichst oft privat das Internet zu nutzen oder E-Mails zu versenden, um sich mit modernen Kommunikationsmitteln vertraut zu machen. Private E-Mail-Nutzung war mithin in der Behörde statthaft. Die unbedacht gestattete Vermengung dienstlicher und privater Nutzung erwies sich letztendlich als nachteilig.

Trotz der zulässigen Privatnutzung erteilte die damalige Amtsleitung im Juli 2006 den Auftrag zum Ausdrucken des gesamten E-Mail-Verkehrs eines befristet beim Landesamt Beschäftigten, da dieser seinen Dienst nicht wieder aufnehmen werde. Nachdem die betreffenden E-Mails zunächst nur recherchierbar archiviert wurden, wurde auf erneute Anordnung durch die Amtsleitung der Ausdruck der E-Mails gegen Ende Juli begonnen und Anfang August 2006 beendet. Die E-Mails wurden in insgesamt 16 Ordnern abgeheftet, eine Einsichtnahme erfolgte nicht. Mit zwischenzeitlichem Schreiben am Ende des Monats Juli wurde der Betroffene darüber informiert, dass er „seine persönlichen Sachen“ in einer Außenstelle abholen könne.

Anfang August kontrollierten meine Mitarbeiter den Vorgang und sahen die in den Ordnern zusammengestellten E-Mails stichprobenweise durch. Wegen des privaten Bezugs empfahl ich, den Betroffenen anzuschreiben und eine Frist zum Aussortieren der E-Mails ohne dienstlichen Bezug zu setzen. Dies geschah mit Schreiben vom 8. August 2006. Nach einem Zustellproblem konnte der Betroffene noch im August die 16 Ordner durchsehen und die privaten E-Mails entfernen. Mit Schreiben vom 11. September 2006 wurde ich informiert, dass sämtliche E-Mails, die der Betroffene während seiner Tätigkeit im Landesamt erhielt, gelöscht wurden.

Ich habe den Vorgang folgendermaßen bewertet:

Der vorgenommene Zugriff auf die E-Mails stellte keinen Verstoß gegen § 88 TKG dar. Nachdem E-Mails aus dem Postfach eines Betroffenen ausgedruckt wurden, ist das TKG nicht mehr einschlägig. Der Schutz des Fernmeldegeheimnisses endet in dem Moment, in dem die Nachricht bei dem Empfänger angekommen und der Übertragungsvorgang beendet ist (BVerfG vom 2. März 2006, 2 BvR 2099/04).

Der vorgenommene Ausdruck verstieß jedoch gravierend gegen § 37 Abs. 1 SächsDSG. Danach ist es nur zulässig, personenbezogene Daten von Beschäftigten zu verarbeiten, wenn dies zur Eingehung, Durchführung, Beendigung oder Abwicklung des Arbeitsverhältnisses erforderlich ist. Vorliegend war dies nicht der Fall. Zunächst bestand sowohl zum Zeitpunkt der Anordnung als auch dem des tatsächlichen Ausdrucks das Beschäftigungsverhältnis fort. Für eine Abwicklung war ein Ausdruck des gesamten E-Mail-Verkehrs keinesfalls erforderlich. Eine Erforderlichkeit bestand aber auch nicht für die Durchführung des Arbeitsverhältnisses. Zum einen wäre es ausreichend gewesen, gegebenenfalls tatsächlich benötigte E-Mails auszudrucken. Zum anderen ist fraglich, ob es eine derartige Notwendigkeit im Einzelfall gab. Bis zuletzt konnte nicht dargelegt werden, dass eine Nutzung der ausgedruckten E-Mails erfolgte. Unabhängig davon war die gewählte Vorgehensweise jedenfalls unverhältnismäßig. Es hätte vielmehr zunächst versucht werden müssen, die Einwilligung des Betroffenen für den Zugriff auf seine privaten E-Mails zu erlangen. Der Betroffene wurde jedoch erst am 27. Juli 2006 und somit sowohl nach der Archivierung als auch deren Anordnung erstmals angeschrieben und über das beabsichtigte Vorgehen informiert.

Die Unzulässigkeit des Ausdrucks war der damaligen Amtsleitung auch bekannt. Da auch bei einem anderen Beschäftigten der E-Mail-Verkehr überprüft werden sollte, hatte ein Beschäftigter der Landesbehörde, der um Prüfung der Zulässigkeit gebeten wurde, die damalige Amtsleitung auf die erheblichen Bedenken hingewiesen. Dies führte im Ergebnis dazu, dass eine Auswertung der E-Mails in diesem gleichgelagerten Fall unterblieb.

Wegen des tiefgehenden und gravierenden Verstoßes gegen das Sächsische Datenschutzgesetz habe ich das Landesamt gemäß § 29 SächsDSG beanstandet.

Auf dienstlichen Arbeitsplätzen sollten private und dienstliche Datensammlungen auseinander gehalten werden, damit es nicht bei Abwesenheit eines Mitarbeiters zu vergleichbaren Problemen kommt. Auf eine private Nutzung besteht seitens der Beschäftigten zunächst kein Anspruch. Das gilt für die E-Mail-Nutzung aber auch die PC-Nutzung an sich. Ist eine Trennung also technisch zu aufwendig oder nicht ge-

wollt, sollte eine private Nutzung unterbunden werden, so dass der Dienststelle ein unbeschränkter Zugriff auf E-Mail-Daten ermöglicht wird. Daher habe ich dem Landesamt auch mitgeteilt, dass das Verbot der privaten Nutzung des E-Mail-Dienstes in einer normenklaren und transparenten Dienstvereinbarung zur Vermeidung von Wiederholungsfällen in Betracht kommt.

5.1.7 Akteneinsichtnahme des Beamten in seine Personalakte - Vollständigkeit der Personalakten

Im letzten Berichtszeitraum ging eine Beschwerde eines Beamten aus dem Geschäftsbereich einer obersten Dienstbehörde bei mir ein, die zeigt, dass auch oberste Dienstbehörden in Bezug auf die Personalaktenführung nicht immer fehlerfrei sind. Der Beschäftigte, der bei einer Behörde im nachgeordneten Bereich tätig war, dessen Personalakte aber aufgrund seines Dienstranges beim Staatsministerium geführt wurde, beklagte sich darüber, dass er keine vollständige Akteneinsicht in seine Personalakte erhalte. § 120 Abs. 1 SächsBG bestimmt, dass der Beamte Einsicht in seine vollständige Personalakte erhält. Bei meiner Kontrolle musste ich feststellen, dass dem Beamten tatsächlich Schriftstücke vorenthalten worden waren. Die Personalakte war unvollständig geführt und mit dem Dienstverhältnis unmittelbar zusammenhängende Unterlagen waren nicht in der formellen Personalakte vorhanden. Das hing z. T. damit zusammen, dass neben der formellen Personalakte zwei als Sachakten deklarierte Vorgänge geführt wurden. Mindestens ein Vorgang darunter war letztendlich auch als personalaktenrelevant einzuordnen. In den als solchen geführten Sachakten fanden sich zum Teil die Schriftstücke, die in der Personal-Hauptakte fehlten, zum Teil aber auch nicht. Einige Schriftstücke mussten überhaupt erst den einzelnen Akten hinzugefügt werden. Die Aktenführung war diesbezüglich insgesamt inkonsistent. Hinzu kam, dass dem Beschäftigten erst nach Terminvereinbarung und mit einer nicht unerheblichen Vorlaufzeit die Einsichtnahme gewährt wurde. Bei einer funktionierenden Personalverwaltung muss verlangt werden können, dass eine Akteneinsichtnahme in Personalakten kurzfristig, das heißt in wenigen Stunden, ohne tagelang auf einen Termin warten zu müssen, erfolgen kann. Bei dem Anspruch auf Akteneinsichtnahme handelt es sich um ein Betroffenenrecht, dass einen Ausfluss des Grundrechts auf informationelle Selbstbestimmung darstellt. Dies sollte den Personal verwaltenden Stellen immer gegenwärtig sein. Da der Beamte nach dem Gesetz auch Personen mit der Einsichtnahme beauftragen kann, gilt dies z. B. auch für Rechtsbeistände des Betroffenen gleichermaßen. Nach meiner Kontrolle und meiner geäußerten Kritik hat die Dienststelle unverzüglich reagiert und ihrer Aktenführung hierauf eingerichtet. Der Petent konnte die von ihm beanspruchte Akteneinsichtnahme dann kurzfristig durchführen.

Einem weitergehenden Begehren des betroffenen Beamten konnte nicht entsprochen werden. Zutreffend war die Einordnung der Dienststelle von bestimmten Schriftstücken als personenbezogene Sachakte in einem Ordner "Beurteilung", der einen sich in Vorbereitung befindenden Beurteilungsvorgang enthielt. Letztendlich war nach alter Rechtslage und der zur Zeit der Kontrolle geltenden Beurteilungsverordnung nur die eröffnete Beurteilung (auch keine Beurteilungsbeiträge) selbst in die formelle Personalakte aufzunehmen. In der Zeitphase der Erstellung und Vorbereitung der Beurteilung handelte es sich um eine personenbezogene Sachakte. Gleichwohl konnte die Dienststelle, dies habe ich so mitgetragen, eine Akteneinsicht nach § 18 Abs. 3 SächsDSG zurückstellen, da bei Einsichtnahme in den noch nicht abgeschlossenen Vorgang ansonsten der Zweck der Datenverarbeitung nach der Beurteilungsverordnung gefährdet worden wäre. Es muss der Beschäftigungsdienststelle möglich sein, ohne dass die Betroffenen auf das Beurteilungsverfahren Einfluss nehmen können und vorzeitig von vorgesehenen Einzelheiten Kenntnis erhalten, personenbezogene Sachakten in Beurteilungsangelegenheiten zu führen, § 18 Abs. 5 Nr. 3 SächsDSG. Nach der Eröffnung der Beurteilung stehen einer Akteneinsicht aber keine gesetzlichen Gründe mehr entgegen. Ich habe daher der Dienststelle empfohlen, dem Beamten nach Abschluss des Beurteilungsverfahrens auch in die Sachakte Einsicht zu gewähren.

5.1.8 Auftragsdatenverarbeitung durch öffentliche Stellen

In 12/5.1.9 vertrat ich die Auffassung, dass das Führen von Bezügeakten für externe Stellen, insbesondere eingetragene Vereine, unzulässig sei, da es an einer gesetzlichen Grundlage für die Verarbeitung personenbezogener Daten gemäß § 4 Abs. 1 SächsDSG fehlte.

Mit dem Inkrafttreten der Änderungen des Sächsischen Datenschutzgesetzes am 1. Januar 2007 haben sich Veränderungen der Auftragsdatenverarbeitungsregeln ergeben und somit trifft dies nicht mehr uneingeschränkt zu.

§ 3 Abs. 3 des SächsDSG 2003 bestimmte, dass jede öffentliche Stelle als Auftragnehmer *Daten verarbeitende Stelle* ist. Dementsprechend war sie gemäß § 7 Abs. 1 Satz 2 SächsDSG 2003 ebenso - neben dem Auftraggeber - für die Einhaltung der Datenschutzvorschriften verantwortlich. Mithin musste auch datenschutzrechtlich nach § 4 Abs. 1 SächsDSG eine gesetzliche Rechtfertigung für die Datenverarbeitung im Auftrag - hier die Bezügerechnung - vorliegen. Die Anforderung besteht mit der Novellierung nun nach dem Sächsischen Datenschutzgesetz nicht mehr, da der Auftragnehmer nicht mehr (auch) die *Daten verarbeitende Stelle* darstellt, sondern

der Auftraggeber allein *Daten verarbeitende Stelle* ist und auch allein für die Datenverarbeitung verantwortlich ist.

Auch wenn somit das Sächsische Datenschutzgesetz die Tätigkeit öffentlicher Stellen als Auftragnehmer nicht mehr einschränkt, so sind doch die verfassungsrechtlich vorgegebenen Schranken zu beachten. Das gilt hier im Besonderen für die staatliche Verwaltung, die sich nicht quasi nach *ordre de Mufti* - nach Belieben - als Auftragnehmer in der Auftragsdatenverarbeitung betätigen darf. Staatsorganisatorisch bestimmt nämlich Art. 83 Abs. 1 SächsVerf für die gesamte staatliche Verwaltung, dass Aufbau, räumliche Gliederung und Zuständigkeiten der Landesverwaltung nur durch Gesetz geregelt werden können (so ausdrücklich zur Sächsischen Verfassung: Battis, Allgemeines Verwaltungsrecht, S. 61). Dies bedeutet, dass eine öffentliche Stelle der Staatsverwaltung nur dann Auftragnehmer sein kann, wenn ihr diese Tätigkeit gesetzlich als Aufgabe zugewiesen wurde, sie mithin aktiv legitimiert ist (§ 7 SächsDSG enthält im Übrigen nur die Befugnis für den Auftraggeber sich eines Auftragnehmers in der Datenverarbeitung zu bedienen).

Anders stellt sich die Gesetzeslage für die kommunalen Gebietskörperschaften als Träger der Selbstverwaltung dar. Diese können entsprechend Art. 82 Abs. 2 SächsVerf im Rahmen der Gesetze selbst ihre Angelegenheiten regeln. Sie bestimmen daher selbst über die Aufgaben und Zuständigkeit ihrer Verwaltung.

Im Ergebnis bedeutet das, dass das Führen von Bezügeakten für externe Stellen, insbesondere eingetragene Vereine, für öffentliche Stellen der Landesverwaltung ohne gesetzliche Grundlage nach wie vor unzulässig ist. Sofern eine Auftragsdatenverarbeitung durch kommunale öffentliche Stellen als Auftragnehmer erfolgt, bestehen hiergegen jedenfalls keine rein datenschutzrechtlichen Bedenken mehr. Gleichwohl sollte die Datenverarbeitung als Auftragnehmer per Satzung aus haushalterischen und ordnungspolitischen (wettbewerblichen) Gesichtspunkten geregelt worden sein, stellt doch insbesondere die kostenfreie oder nur Unkosten deckende Bezügerechnung für Vereine oder andere Private eine versteckte Subvention - bzw. einen Vermögensvorteil - dar, die zu erlangen, einheitlich zu regeln wäre, sofern man sich nicht auf dünnes Eis begeben möchte.

5.1.9 Verwaltungsermittlungen - Betroffenenrechte

Bereits in 12/5.1.12 hatte ich die Möglichkeiten und Grenzen von Verwaltungsermittlungen anhand eines konkreten Vorgangs dargestellt.

Umso bedauerlicher ist es gewesen, dass ein Betroffener seine Bemühungen, Auskunfts- und Berichtigungsansprüche durchzusetzen, auch in meinem neuen Berichtszeitraum fortsetzen musste, um eine gewisse Rehabilitation zu erreichen. Obwohl der Betroffene sogar mit Staatsministerschreiben von jedem Vorwurf einer dienstrechtlichen Verfehlung entlastet worden war, benötigte das Staatsministerium, nachdem der Betroffene bereits verwaltungsgerichtliche Klage erhoben hatte, viele weitere Monate, um mit dem Betroffenen eine außergerichtliche Einigung in Bezug auf die Berichtigung in den Verwaltungsermittlungsakten und eine Auskunft zu erreichen.

Bis zuletzt ist dem Betroffenen die Einsichtnahme in den Verwaltungsvorgang zu seinen Auskunfts- und Berichtigungsanträgen nicht gewährt worden, obwohl ich der Behörde mitgeteilt hatte, dass ein Akteneinsichtnahmeanspruch in die zu dem Betroffenen geführte personenbezogene Sachakte besteht (§ 18 Abs. 3 Satz 1 SächsDSG).

Was die Verwaltungsermittlungsakten selbst anbelangt, erfolgte eine Berichtigung nach § 19 SächsDSG. Vorgänge dieser Art werden relativ selten an mich herangetragen. Streitig war zwischen der Behörde und dem Betroffenen unter anderem, welche Angaben zu berichtigen sind, da sich in den Unterlagen auch Erwähnungen der Verwaltungsermittler und Angaben von befragten Personen befanden, deren Bekundungen wohl zutreffend wiedergegeben worden waren, die den Betroffenen gleichwohl persönlichkeitsrechtlich belasteten und mit denen er inhaltlich nicht einverstanden war. Eine Berichtigung erfolgte letztendlich bei den objektiv unrichtigen Stellen, d. h. bei den Informationen, die einzelne Angaben über die persönlichen oder sachlichen Verhältnisse vermittelten, die nicht mit der Realität übereinstimmten.

Im Übrigen wurde der Betroffene auf beinahe einhundert Blattseiten der Verwaltungsermittlungsakten erwähnt. In Anbetracht der zunächst intendierten nicht personenbezogenen Verwaltungsermittlungen und der nicht vorhandenen Nähe des Betroffenen zum Untersuchungsgegenstand musste man dies, selbst bei Berücksichtigung einer rechtsaufsichtlichen Funktion des Betroffenen, aufgrund der objektiven Gegebenheiten als eine auffällige Häufung ansehen. Durch eine jeweilige Kopie des entlastenden Staatsministerschreibens, das an sämtlichen Stellen vor den jeweiligen Blättern eingefügt wurde, konnte ein den Betroffenen belastender negativer Eindruck kompensiert werden.

Nicht übersehen werden sollte bei Berichtigungsverfahren (§ 19 Abs. 2 SächsDSG) die Pflicht der Daten verarbeitenden Stelle, die Empfänger übermittelter Daten von Berichtigungen zu unterrichten. Bei der Übersendung von Akten bedeutet dies unter

Umständen einen erhöhten Verwaltungsaufwand, der aber nur in Ausnahmefällen unterbleiben kann (vgl. § 19 Abs. 2 SächsDSG - am Ende). Im vorliegenden Fall ist die Benachrichtigung der Behörde zudem durch die Streuung und Vervielfältigung der Verwaltungsermittlungsakten erschwert worden.

Die Akten sind darüber hinaus gesperrt worden. Sperrung bedeutet die Einschränkung der weiteren Verarbeitung und Nutzung von personenbezogenen Daten. In der Praxis wurden die Akten in einem Referat in versiegelten Kisten verwahrt, in einer anderen Organisationseinheit wurden sie in einem Aktenregal aufgehoben. Der Regalbereich war mit Bändern und Siegeln gesichert, um einen unbefugten Zugriff auszuschließen. Bei beiden Referaten wurde der nunmehr beschränkte Zugang zu den Akten schriftlich dokumentiert. Nach einer Entnahme, z. B. auch bei einer Nachkontrolle durch meine Behörde wurden die Kisten, bzw. die Regalreihen erneut gesichert und mit einem neuen Siegel versehen.

Das Staatsministerium verweist auf die durch das Hauptstaatsarchiv festgestellte Archivwürdigkeit. Die generelle Anbietungspflicht an das Archiv ist rechtlich vorgesehen (§ 5 SächsArchivG). Auch wenn sie aus archivrechtlichen Gründen nachvollziehbar ist (das Handeln - auch das rechtswidrige - des Staates soll für die Nachwelt nachvollziehbar sein), so ist es aus Datenschutzgründen schwer erträglich, dass rechtswidrig zusammengetragene und Betroffene belastende Aktenkonvolute archiviert werden sollen. Persönlichkeitsrechtsverletzungen werden auf diese Weise perpetuiert. Der Vorgang kann jedenfalls solange nicht archiviert werden, bis auch notwendige datenschutzrechtliche Feststellungen in Bezug auf die Hauptbetroffenen erfolgt sind. Solange ist die gesamte Akte zur Aufgabenerfüllung noch erforderlich (vgl. § 20 Abs. 2 SächsDSG).

5.1.10 Das neue Allgemeine Gleichbehandlungsgesetz

Im Sommer des Jahres 2006 hatte der Deutsche Bundestag das Allgemeine Gleichbehandlungsgesetz (AGG) verabschiedet. Das Gesetz findet Anwendung bei Beschäftigungsverhältnissen öffentlicher, aber auch privater Arbeitgeber. Aufgrund der weitgehenden Rechte, die Beschäftigten, die benachteiligt wurden (vgl. §§ 13, 14, 15), zugestanden werden und wegen Klagerechten für Personalvertretungen und Gewerkschaften (§ 17) sowie einer auf den Arbeitgeber abgewälzten Beweislast (§ 22) ist dieser veranlasst, bei vielen Vorgängen, die sich auf eine Entscheidung zugunsten von Mitarbeitern beziehen, eine Dokumentation zu betreiben. Auf diese Weise werden personenbezogene Daten - Mitarbeiterdaten - verarbeitet. Das neue Gesetz ist im Rahmen der zugunsten des Arbeitnehmers geltenden Datenschutzbestimmungen

zu berücksichtigen. Nach § 37 Abs. 1 SächsDSG kann die öffentliche Stelle Daten von Bewerbern und Beschäftigten zur Eingehung, Durchführung, Beendigung und Abwicklung des Dienst- oder Arbeitsverhältnisses im Rahmen der Erforderlichkeit verarbeiten. In der Praxis dürfte sich der Schwerpunkt bei der Datenverarbeitung von Bewerberfragebögen hin zu Einstellungsfragebögen verlagern. Datenschutzrechtlich ist dies - im Sinne des Erforderlichkeitsgrundsatzes - durchaus zu begrüßen, auch wenn dies in dem Bemühen begründet sein mag, diskriminierungsfrei Daten zu verarbeiten. Inhaltlich wird es im Stadium der Bewerbung darauf ankommen, dass potenziell zu einer Diskriminierung geeignete Daten (Geburtsdaten, Angaben zu Geschlecht und Staatsangehörigkeit, Sozialangaben etc.) zur Identifizierung oder zum Nachzeichnen eines Lebenslaufes erhoben werden, nicht aber um Entscheidungen auf Grundlage dieser Einzelangaben zu treffen. Auch Spezialgesetze können, wie bei der Frage nach der Schwerbehinderteneigenschaft, Datenverarbeitung rechtfertigen.

Ähnliches gilt auch für Personalakten Beschäftigter. Bei Stellenausschreibungen, Beförderungen, bei der Vergabe von Leistungsprämien werden, wenn mehrere Mitarbeiter für Maßnahmen zur Auswahl stehen, regelmäßig tatbestandlich die Bestimmungen des AGG zu beachten sein. Wenn auch das Gleichbehandlungsgesetz explizit keine Dokumentation einer gleichbehandlungsgerechten Auswahl erfordert, so wird man doch der öffentlichen Stelle zuzugestehen haben, dass sie in Anbetracht der gesetzlichen Beweislastsituation und der Rechte der klagebefugten Beschäftigten und Vereinigungen Vorsorge trifft, um eine Gleichbehandlung nachweisen zu können. Von einer Dokumentationspflicht ist insoweit auszugehen. Es ist z. B. zu dokumentieren, weshalb ein bestimmter Mitarbeiter eine Stelle erhalten soll, die Mitbewerber aber nicht. Dennoch wird eine (Gleichbehandlungs-)Dokumentation nicht in der Personalakte selbst erfolgen können. Die Entscheidung selbst, die Verfügung einem Mitarbeiter eine Leistungsprämie zuzubilligen oder das Schreiben, mit dem ein Bewerber die Zusage zu einer Stelle erhält, kann in der formellen Personalakte abgelegt werden. Die Entstehungsgeschichte, die die Auswahlentscheidung nachvollziehbar macht, gehört in eine personenbezogene Sachakte. So ist es auch bisher herkömmlich z. B. bei Personalauswahlentscheidungen praktiziert worden.

Lösen lässt sich die Kollision von Dokumentationspflicht und datenschutzgerechter Verarbeitung der Angaben nur, wenn die Grundsätze der Datensparsamkeit und Datenvermeidung bei der Dokumentation beachtet werden (§ 9 Abs. 1 Satz 2 SächsDSG) - und dies im Hinblick auf Umfang, Tiefe und Ausmaß der Datenverarbeitung. Dem Grundsatz der Datenvermeidung Rechnung tragend sollten nur die tatsächlich erforderlichen Angaben in einer Dokumentation aufgenommen werden. Außerdem wäre bei der Verarbeitung der Daten in der Personalakte darauf zu achten,

dass keine Angaben mit Doppelbezug, etwa Daten von Mitbewerbern gleich mit aufgenommen werden, sondern lediglich die Daten zu dem jeweiligen betroffenen Beschäftigten.

Soweit Dokumentationen als Personalakten geführt werden, unterliegen sie dem Personalakten- und vollständigen Einsichtnahmerecht des Beschäftigten nach dem Sächsischen Beamtengesetz bzw. dem für Angestellten und Arbeiter des öffentlichen Dienstes weitgehend angenäherten Personalaktenrecht. Im Hinblick auf die Führung in personenbezogenen Sachakten, unterliegen die Daten den gesetzlichen Auskunfts- und Einsichtnahmerechten (§ 18 SächsDSG). Bei der Einsichtnahme können auch Daten mit Doppelbezug offenbart werden. Die Angaben sollten solange gespeichert bleiben, bis die Rechtsmittelfristen abgelaufen sind. Danach sind die Unterlagen, soweit sie nicht archivierungswürdig sind, zu löschen. Es besteht eine Löschungspflicht für die Unterlagen, die nicht mehr zur Aufgabenerfüllung benötigt werden. Ab wann zu löschen ist, kann im Einzelfall schwierig sein, zu entscheiden, da zu berücksichtigen ist, dass in Gleichbehandlungsfragen Betroffene von einer möglichen Benachteiligung keine Kenntnis hatten. Die übrigen Betroffenenrechte des dritten Abschnitts des Sächsischen Datenschutzgesetzes - Berichtigungs- und Löschungsansprüche - sind ebenso einschlägig, wenn die Daten in personenbezogenen Sachakten verarbeitet werden. Bei Berichtigung und Löschung kann die Verbindung der Daten eines Betroffenen mit anderen personenbezogenen Daten durchaus zu Schwierigkeiten führen. Ich stehe den Daten verarbeitenden Stellen beratend zur Seite.

Was für die nach Sächsischem Datenschutzgesetz Daten verarbeitenden Stellen gilt, gilt im Grundsatz auch für die nach dem dritten Abschnitt des Bundesdatenschutzgesetzes Daten verarbeitenden Stellen, die nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG personenbezogene Sachakten in Gleichbehandlungsfragen zu führen befugt sind (vgl. § 2 Abs. 3 SächsDSG). In diesen Fällen sind die Betroffenenrechte nach dem Bundesdatenschutzgesetz zu beachten.

5.1.11 Erklärungen in der Personalakte - Bekenntnis zur freiheitlichen demokratischen Grundordnung

Vereinzelt ist an mich die Frage gerichtet worden, ob die im Bereich der Staatsregierung in Formularform verwendete Erklärung zum Bekenntnis zur freiheitlichen demokratischen Grundordnung datenschutzrechtlich zulässig sei (vgl. SächsABl. 2004, Nr. 30 Anlagen 1 und 3). Als bedenklich wird dabei zum Teil die als Anlage beigefügte Übersicht über extremistische Vereinigungen hervorgehoben. Die Anlage dient Bewerbern und einzustellenden Beschäftigten als Anhaltspunkt, welche

Organisationen als extremistisch zu betrachten sind. Auf dem Formular selbst hat der einzustellende Beschäftigte sein Bekenntnis zu erklären, dass er keine Bestrebungen gegen die freiheitliche demokratische Grundordnung unterstützt und darüber hinaus, dass er nicht Mitglied einer hiergegen gerichteten Organisation in den letzten fünf Jahren war. Natürlich ist auch die Erklärung der Nicht-Zugehörigkeit zu einer extremistischen Vereinigung ein personenbezogenes Datum. Gleichwohl halte ich die hierauf bezogene Datenverarbeitung unter Bezugnahme auf eine Anlage, die eine Liste von extremistischen Vereinigungen enthält, noch für verhältnismäßig, da sie in Bezug auf die persönliche Eignung (vgl. Art. 92 Abs. 2 SächsVerf) von Bedeutung ist. Ich erhebe daher keine datenschutzrechtlichen Bedenken.

5.1.12 Einverständniserklärung zur Einsichtnahme in die Personalakte bei Bewerbungen aus dem öffentlichen Dienst

In unregelmäßigen Abständen wird mir die Frage gestellt, ob es zulässig sei, bei Bewerbungsverfahren im öffentlichen Dienst die Bewerber-Personalakten anderer öffentlicher Stellen hinzuzuziehen. Das Sächsische Beamtengesetz differenziert. Eine Einsichtnahme ohne Einwilligung ist bei Erforderlichkeit durch Behörden desselben Geschäftsbereichs bzw. bei vorgesetzten Dienstbehörden möglich (vgl. § 121 Abs. 1 SächsBG). Grundsätzlich ist auch eine Beiziehung von Personalakten mit Einwilligung des Betroffenen vorstellbar. Diese ist aber wiederum auch nur nach Notwendigkeit durchzuführen. Eine Erforderlichkeit seitens der anfordernden - und einstellenden - Stelle wird dann regelmäßig erst anzunehmen sein, wenn der betroffene Bedienstete auch tatsächlich eingestellt oder übernommen werden soll, andernfalls sollte die datenschutzrechtliche Erforderlichkeit aus Revisionsgründen aktenkundig gemacht werden. Im letzteren Fall ist nach § 121 Abs. 2 SächsBG zu verfahren. § 121 Abs. 3 SächsBG, die Pflicht, sich auf das Erforderliche zu beschränken, ist zu beachten. Die oben stehenden Grundsätze gelten bei Angestellten und Arbeitern gleichermaßen.

5.2 Personalvertretung

5.2.1 Grenzen der Unterrichtungspflicht zugunsten des Personalrats - Beurteilungsdaten einzelner Beschäftigter

Immer wieder erhalte ich Anfragen, ob es zulässig sei, dem Personalrat die einzelnen Angaben des letzten Beurteilungsverfahrens personenbezogen, das heißt unter Benennung der beurteilten Mitarbeiter, mitzuteilen. Die Nachfragen erfolgen manchmal im Zusammenhang mit Beförderungsverfahren, zum Teil aber auch unabhängig hiervon. Offenbar besteht bei vielen Personal verwaltenden Dienststellen, aber auch bei den

Personalräten selbst Unsicherheit in Bezug auf die Frage, inwieweit dem Ansinnen der Personalräte nach dieser Form der Datenübermittlung Rechnung zu tragen ist bzw. die Daten tatsächlich offenbart werden müssen.

§ 73 Abs. 2 SächsPersVG bestimmt, dass die Personalvertretung zur Durchführung ihrer Aufgaben rechtzeitig und umfassend zu unterrichten ist. Ihr sind auch die hierfür erforderlichen Unterlagen vorzulegen. Absatz 2 Satz 3 und 4 der Vorschrift geben dabei einen genaueren gesetzlichen Anhaltspunkt zu der Fragestellung. Die Beurteilungen selbst werden nach ihrer Eröffnung als personalaktenrelevante Schriftstücke in die formelle Personalakte eingefügt. Diese werden somit Teil der Personalakte. Bei den einzelnen Beurteilungsangaben handelt es sich um Personalaktendaten. Nach Satz 3 des § 73 Abs. 2 SächsPersVG dürfen Personalakten nur mit Zustimmung der Beschäftigten von durch von diesen bestimmten Mitgliedern der Personalvertretungen eingesehen werden. Satz 4 legt darüber hinaus fest, dass dienstliche Beurteilungen auf Verlangen der Beschäftigten der Personalvertretung zur Kenntnis zu bringen sind. Personalakten und Beurteilungsdaten sollen mithin nach den gesetzlichen Bestimmungen freiwillig, das heißt nur mit Wissen und Wollen der Beschäftigten gegenüber dem Personalrat offenbart werden.

Im Ergebnis wird man daher personalvertretungs- und datenschutzrechtlich etwaige Begehren der Personalvertretungen in Bezug auf Beurteilungsdaten abzuweisen haben.

Was die Beförderungsverfahren selbst angeht, können dem Personalrat die Unterlagen zugänglich gemacht werden, die ihm einen Überblick über das Beförderungsverfahren und die abgeschlossenen und anstehenden Beförderungen geben. Hierfür sind wiederum die Einzelangaben zur Beurteilung nicht erforderlich. Informationsrechte der Personalvertretung im Übrigen unter 10/5.2.

5.3 Einwohnermeldewesen

5.3.1 Das neue Meldegesetz und die Meldewesen-IT-Infrastruktur in Sachsen

Mit den letzten Änderungen des Melderechtsrahmengesetzes wurden den Ländern gesetzgeberisch zahlreiche Änderungen aufgetragen, die durch das novellierte Sächsische Meldegesetz im Sommer des Jahres 2006 umgesetzt worden sind. Zu den wichtigsten Veränderungen hierbei zählen Festlegungen zu einer landesweiten und länderübergreifenden Kommunikation der Meldebehörden im Wege der elektronischen Datenübermittlung und die einfache Melderegisterauskunft über das Internet

(GVBl. 2006, S. 388). Zusätzlich trat im Februar 2006 die Änderung des Gesetzes über die Errichtung der Sächsischen Anstalt für kommunale Datenverarbeitung in Kraft, mit der ein von der Sächsischen Anstalt für kommunale Datenverarbeitung betriebenes Landesmelderegister etabliert wird. Maßgebend ist § 4a SAKDG. Bereits in meinem letzten Tätigkeitsbericht hatte ich diese Veränderungen angekündigt (12/5.3.2). Nach diesen Gesetzgebungsakten des Freistaates ist im Wege der Föderalismusdiskussion durch das *Gesetz zur Änderung des Grundgesetzes* im Spätsommer des letzten Jahres das Meldewesen in die ausschließliche Gesetzgebung des Bundes übergegangen (BGBl. I, S. 2043).

Das geänderte Sächsische Meldegesetz sieht vor, dass weitere melderechtsfremde Daten in den Melderegistern verwaltet werden. Ich habe mich immer gegen eine solche Entwicklung gewandt. Zu den Daten, die eigentlich nicht in die Melderegister gehören, zählen die Steueridentifikationsnummer, die aufgrund bundesgesetzlicher Regelung (§ 139b AO) im Melderegister aufgenommen wird, ebenso wie die Angaben zu Waffen- und Sprengstofferlaubnissen. Positiv anzumerken ist, dass das Merkmal *erwerbstätig/nicht erwerbstätig* nicht mehr in den Meldedatensätzen vorgesehen ist. In Bezug auf die einfache Melderegisterauskunft über das Internet ermöglicht § 32a Abs. 2 und 4 SächsMG, dass die Auskünfte auch auf automatisiert verarbeitbaren Datenträger oder durch Datenübertragungen bzw. per automatisiertem Abruf, erteilt werden können. Ein automatisierter Abruf ist allerdings nicht zulässig, wenn der Betroffene dieser Art der Auskunftserteilung widersprochen hat (§ 32a Abs. 4 Satz 4 SächsMG, vgl. auch 5.3.5).

Zu der Funktionsfähigkeit der Kommunikation der Meldebehörden im Wege der elektronischen Datenübermittlung im Freistaat und Länder übergreifend konnte ich bis zum Ende des Berichtszeitraums noch keine nennenswerten Details in Erfahrung bringen.

Bei dem Landesmelderegister, dem so genannten kommunalen Kernmelderegister (KKM), wird, so sieht es der Gesetzgeber vor, lediglich ein Teildatensatz verarbeitet. Übermittlungs- und Auskunftssperren, also auch die Widersprüche der Betroffenen sind durch die örtlichen (gemeindlichen) Meldebehörden an das KKM weiterzugeben und dort zu berücksichtigen.

Das kommunale Kernmelderegister befand sich zum Ende des Berichtszeitraums noch im Aufbau.

5.3.2 Novelle der Sächsischen Meldeverordnung

Auch in diesem Berichtszeitraum war ich mit den rechtlichen und technischen Änderungen im Bereich des Meldewesens beschäftigt. Das zuständige Staatsministerium beteiligte mich bei den Änderungen der Sächsischen Meldeverordnung. Der erste, die IT-Infrastruktur im Bereich Meldewesen regelnde Teil der Verordnung, ist bereits seit dem 24. Dezember 2006 in Kraft. Mit dem mir zur Stellungnahme vorgelegten zweiten Teil der Verordnung sollte die regelmäßige Datenübermittlung der Meldebehörden an Behörden und öffentliche Stellen im Sinne des Meldegesetzes näher geregelt werden.

Die Beteiligung des Sächsischen Datenschutzbeauftragten nach § 26 SächsDSG (vgl. auch § 14 Abs. 6 Satz 3 GeschoSReg) in die Verordnungsgebung ist im Interesse des Rechts auf informelle Selbstbestimmung der Bürger von einer gewissen Bedeutung. Aufgrund der Einführung moderner Kommunikationstechnologien in das Meldewesen - und das Meldegesetz ist bereichsspezifisches Datenschutzrecht - haben die Normsetzungsverfahren auch eine Weichen stellende Bedeutung. Bedauerlich ist, dass von den 14 von mir übersandten Hinweisen und Änderungswünschen lediglich neun Berücksichtigung fanden und ebenso die Tatsache, dass der Umfang der zu übermittelten Daten in einigen Fällen nachträglich verändert wurde. So hatte ich insbesondere den automatisierten Abruf durch die Staatskanzlei (§ 26; fehlende (gesetzliche) Erforderlichkeit), durch den Verfassungsschutz (§ 34), die Vermessungsverwaltung (§ 34; wegen nicht mehr überschaubarer datenschutzorganisatorischer Risiken), die Kassenärztliche Vereinigung (§ 35; es besteht keine Erforderlichkeit für einen automatisierten Abruf) in Frage gestellt.

Schwerwiegend ist allerdings, dass der mir vorgelegte Entwurf der Verordnung drei aus meiner Sicht bedeutende Bestimmungen nicht enthielt. Ohne auf die Einrichtung eines automatisierten Abrufverfahrens für die Regierungspräsidien (§ 38 SächsMeldVO), bei dem die Erforderlichkeit aus meiner Sicht nicht hinreichend dargelegt wurde, und die getroffene Übergangsregelung (§ 40 SächsMeldVO) näher eingehen zu wollen, stellt die Regelung des § 39 SächsMeldVO m. E. einen Bruch im Normengefüge des sächsischen Melderechts dar.

§ 39 SächsMeldVO soll die Rechtsgrundlage für ein generelles automatisiertes Abrufverfahren für Behörden und öffentliche Stellen des Freistaates Sachsen im Umfang der einfachen Melderegisterauskunft (Vor- und Familiennamen, Doktorgrad und gegenwärtige Anschriften) bilden. Eine Generalklausel zur Einrichtung einer automatisierten Abrufmöglichkeit von Meldedaten für einen nicht abschließend be-

stimmten Empfängerkreis gab es bisher weder im Sächsischen Meldegesetz noch in der darauf basierenden Datenübermittlungsverordnung. Die Bestimmung ist nicht mehr systemgerecht, denn der automatisierte Abruf von Meldedaten ist als eine spezielle Form der regelmäßigen Datenübermittlung gemäß § 29 Abs. 5 SächsMG nur zulässig, soweit dies durch Bundes- oder Landesrecht *unter konkreter* Festlegung des Anlasses und des Zwecks der Übermittlung, der Empfänger und der zu übermittelnden Daten bestimmt ist. Diese im Meldegesetz vorgeschriebenen Festlegungen können gesetzlicher Art sein oder nach § 36 Nr. 4b SächsMG durch das zuständige Staatsministerium in einer Verordnung getroffen werden. Vor dem Erlass einer Verordnungsregelung ist für jedes in § 5 Abs. 1 oder 2 SächsMG genannte Datum durch den Verordnungsgeber gesondert zu prüfen, ob die Datenübermittlung für die Aufgabenerfüllung des Datenempfängers erforderlich ist. Eine Unterscheidung zwischen „einfache Melderegisterauskunft - Adressauskunft“ oder „Erweiterte Auskunft“ wie im privaten Bereich kennt das Meldegesetz im Bereich der Datenübermittlung an Behörden nicht. Im Meldewesen wird davon ausgegangen, dass die Behörden die Daten erhalten, die für deren Aufgabenerfüllung erforderlich sind. Der Erforderlichkeitsgrundsatz gilt für alle Daten nach § 5 Abs. 1 SächsMG. Einen vereinfachten Weg, die Adressdaten einer Person zu erlangen, sieht das Meldegesetz für Behörden und öffentliche Stellen nicht vor.

Da der automatisierte Abruf von Daten im Vergleich zur herkömmlichen regelmäßigen Datenübermittlung die schwerwiegendere Übermittlungsart darstellt, da er einer Gesamtdatenübermittlung gleichkommt und zudem weitergehende datenschutzorganisatorische Risiken beinhaltet, muss nicht nur die regelmäßige Datenübermittlung als solche, sondern auch die Art und Weise der Übermittlung im Hinblick auf den Zweck angemessen sein. Eine regelmäßige Datenübermittlung im Wege des automatisierten Abrufverfahrens kann dann gerechtfertigt sein, wenn typischerweise eine besondere Eilbedürftigkeit der Datenübermittlung zum Schutz von Rechtsgütern gegeben ist oder die Vielzahl der notwendigen Datenübermittlungen dies erforderlich macht. Diesen Grundsätzen folgend ist in der bisherigen Sächsischen Meldedatenübermittlungsverordnung und auch - abgesehen von § 39 SächsMeldVO - in der neuen Sächsischen Meldeverordnung, durch den Verordnungsgeber jeder Empfänger regelmäßiger Datenübermittlungen unter Festlegung des Datenumfanges konkret geregelt. Datenschutzrechtlich bedenklich ist bereits, dass die Regelungen der Verordnung (§§ 29 bis 38 SächsMeldVO) die gemäß § 29 Abs. 5 SächsMG erforderliche Festlegung des Anlasses und Zwecks des automatisierten Abrufs vermissen lassen, da bezüglich dieser beiden Kriterien lediglich allgemein auf die spezialgesetzlichen Normen, welche die Grundlage des behördlichen Handelns bilden, Bezug genommen wird.

Der neue § 39 SächsMeldVO eröffnet den sächsischen Behörden und öffentlichen Stellen, ohne die im Verordnungsgebungsverfahren erforderliche, vorgeschaltete Erforderlichkeits- und Verhältnismäßigkeitsprüfung, die Möglichkeit zum automatisierten Abruf von Meldedaten. Die pauschale Regelung führt aber auch die Notwendigkeit der Einzelfestlegungen für die in der Verordnung genannten Stellen und Behörden (§§ 25 bis 28 und 29 bis 38 der SächsMeldVO) in gewisser Weise ad absurdum. Würden nämlich nach dem Sächsischen Meldegesetz allgemeine Regelungen, wie die des § 39 SächsMeldVO, für die Einrichtung des automatisierten Abrufs als datenschutzorganisatorisch besonders risikobehafteter Übermittlungsform genügen, bedürfte es in der Verordnung auch keiner konkreten Regelung zu den übrigen Übermittlungen.

Um Behörden und öffentlichen Stellen einen generellen automatisierten Abruf der Einwohnerdaten in dem Umfang, wie private Anfrager Daten im Rahmen des § 32 SächsMG erhalten, zu ermöglichen, wäre aus meiner Sicht zunächst die folgende rechtspolitische Grundsatzentscheidung zu treffen: Alle Behörden und öffentliche Stellen des Freistaates Sachsen erhalten im Rahmen des § 29 SächsMG generell Zugang zu den Daten, die Privatpersonen im Rahmen der sog. einfachen Melderegisterauskunft gemäß § 32 SächsMG mitzuteilen sind.

Eine solche rechtspolitische Grundsatzentscheidung wurde mit der Novelle des Sächsischen Meldegesetzes 2006 nicht getroffen. Stattdessen sieht die Verordnung meines Erachtens ohne gesetzliche Grundlage im Sächsischen Meldegesetz die Erlaubnis der Einrichtung eines generellen automatisierten Abrufs vor. Damit gehört Sachsen gemeinsam mit Rheinland-Pfalz zu den einzigen Ländern, die eine solche Generalklausel für behördliche Auskünfte ohne gesetzlichen Unterbau in der Landesmeldeverordnung geregelt haben. Andere Bundesländer, wie zum Beispiel der Freistaat Bayern, haben die Regelung entsprechend deren Bedeutung in die Landesmeldegesetze direkt aufgenommen.

Abschließend bleibt mir nur festzustellen, dass in Ermangelung einer Rechtsgrundlage für die Generalklausel im Sächsischen Meldegesetz, im Hinblick auf die mangelnde Bestimmtheit, auch was den Empfängerkreis angeht, die Einrichtung des in § 39 SächsMeldeVO vorgesehenen automatisierten Abrufs im Umfang der einfachen Melderegisterauskunft für Behörden des Freistaates Sachsen mit den derzeit geltenden Regelungen des Sächsischen Meldegesetzes nicht vereinbar ist.

5.3.3 Einrichtung eines nicht ordnungsgemäßen Melderegisters und datenschutzorganisatorische Mängel bei einer Gemeinde als Meldebehörde

Eine nicht alltägliche Eingabe erhielt ich von einer Petentin, einer von ihrem Mann geschiedenen und getrennt lebenden Ehefrau eines Bürgermeisters einer Gemeinde, die zu Recht den Umgang dieser Gemeinde mit ihren Meldedaten kritisierte. Die Petentin beklagte sich darüber, dass sie von der Meldebehörde eine Antwort auf eine schriftliche Bitte um Auskunftserteilung gemäß § 24 Abs. 1 SächsMG nicht erhalten habe. Das Auskunftsersuchen bezog sich auf die Rückmeldung ihrer neuen Wohnanschrift an die Gemeinde durch die neue Wohnsitzgemeinde (Zuzugsgemeinde). Darüber hinaus äußerte sie unter Bezugnahme auf konkrete Einzelheiten den Verdacht, durch die Meldebehörde könne das Meldegeheimnis verletzt worden sein, da ihr früherer Ehemann und Bürgermeister sich unberechtigt ihre Meldedaten verschafft habe. Damit kam ein Vorgang ins Rollen, den man als durchaus merkwürdig bezeichnen muss.

In der mir gegenüber abgegebenen Stellungnahme führte die Gemeindeverwaltung zunächst aus, dass Melderegisterauskünfte grundsätzlich nur auf schriftliche Anfrage erteilt und eine Kopie als Nachweis im Amt verbleiben würde. Im vorliegenden Fall sei eine Melderegisterauskunft nicht erteilt worden. Außerdem versicherte mir der Bürgermeister selbst, er habe keinerlei Daten, die ihm als Dienstherr und Leiter der Gemeindeverwaltung bekannt geworden seien, für andere als für dienstliche Zwecke genutzt.

Zusätzlich war wegen einer Dienstaufsichtsbeschwerde die Rechtsaufsichtsbehörde in das Verfahren involviert. Diese teilte mir auf meine Anfrage hin ihre Auffassung mit, dass der Bürgermeister als oberste Dienstbehörde, der bei der Gemeinde Beschäftigten, als solcher die Befugnis habe, in die von den Mitarbeitern geführten Karteien und Dateien Einsicht zu nehmen, auch, um die ordnungsgemäße Aktenführung zu prüfen. Ungeachtet dessen habe er ein berechtigtes Interesse gehabt, den Wohnort seiner geschiedenen Frau zur Kenntnis zu bringen, da er gerichtliche Hilfe in Anspruch zu nehmen beabsichtigt habe. Die Erhebung bzw. Kenntnisnahme der neuen Wohnanschrift durch den Bürgermeister wurde bestätigt. Sie war dadurch begünstigt, das sämtliche Post an die Gemeinde über den Bürgermeister selbst ging.

Die Stellungnahmen befriedigten nicht, zumal der Vorgang letztendlich in dem verwirrenden Umstand gipfelte, dass die Petentin die gewünschte Auskunft - nach einer Dienstaufsichtsbeschwerde bei der Rechtsaufsichtsbehörde - vom Einwohnermeldeamt einer anderen Gemeinde erhielt, die aufgrund einer bloßen Vereinbarung

mit der von der Petentin angefragten Gemeinde die Aufgaben der Meldebehörde der betroffenen Gemeinde „übernommen“ hatte und dort quasi eine Neben(Melde-)stelle betrieb. Eine gesetzliche Stütze hierfür gab es nicht, da eine formelle Genehmigung nach dem Sächsischen *Gesetz über kommunale Zusammenarbeit* (vgl. § 36 Abs. 1, § 7 Abs. 1 SächsKomZG) durch die zuständige Rechtsaufsichtsbehörde nicht erfolgt war.

Ich kam nicht umhin, den gesamten Vorgang zu beanstanden. Dabei bemängelte ich zwei voneinander getrennt zu betrachtende datenschutzrechtliche Verstöße.

1. Es handelte sich um einen *strukturellen Datenschutzverstoß*:

Meldebehörden sind nach § 2 Abs. 1 SächsMG die Gemeinden. Der gestellte Antrag auf Auskunftserteilung war nach § 24 Abs. 1 Nr. 1 SächsMG zu beantworten. Die Auskunftserteilung steht grundsätzlich nicht im Ermessen der Behörde. Die nicht erteilte Auskunft durch die Meldebehörde der Gemeinde verstieß gegen § 24 SächsMG und verletzte das Persönlichkeitsrecht der Auskunftssuchenden. Daran ändert auch nichts die aufgrund der Beschwerde nachträglich erteilte Auskunft durch die Meldebehörde der anderen Gemeinde. Eine rechtsaufsichtlich genehmigte Vereinbarung nach dem Sächsischen Gesetz über die kommunale Zusammenarbeit zur Führung des Melderegisters der Gemeinde bei der auskunftgebenden Gemeinde existierte ja nicht. Die seit 1995 bestehende Vereinbarung zur Übernahme der Aufgaben der Meldebehörde der Gemeinde durch die andere Meldebehörde verstieß gegen melde- und damit datenschutzrechtliche Vorschriften. Natürlich war der Vorgang über den Einzelfall hinaus überaus gravierend. Die „beauftragte“ Meldebehörde war gar nicht zuständig, verfügte aber seit Jahren über die Meldedaten der anderen Gemeinde.

2. Es lag ein *allgemeiner datenschutzorganisatorischer Verstoß* vor:

Der Bürgermeister ist aufgrund gesetzlicher Stellung gemäß § 53 Abs. 1 SächsGemO für die sachgemäße Erledigung der Aufgaben und den ordnungsmäßigen Gang der Gemeindeverwaltung verantwortlich und regelt die innere Organisation der Gemeindeverwaltung. Die bestehende Organisationsstruktur der Gemeinde weist ein Einwohnermeldeamt als Meldebehörde aus. Als sensible personenbezogene Daten sind Meldedaten vor unbefugter Verarbeitung durch das Meldegeheimnis (§ 9 SächsMG) besonders geschützt. Das Meldegeheimnis verbietet beispielsweise den Beschäftigten, sich Meldedaten für eigene Zwecke zu beschaffen. Soweit ein Mitarbeiter der Meldebehörde Meldedaten für eigene Zwecke (z. B. zur Vorbereitung eines Klassentreffens) benötigt, muss er wie ein Außenstehender Antrag auf Melde-

registerauskunft nach § 32 SächsMG stellen, über den er nicht selbst entscheiden darf (vgl. Darré/Rimmele/Thalheim/Wunsch, Sächsisches Meldegesetz, 2. Aufl., § 9, Rdnr. 7). Zum Schutz personenbezogener Daten gilt in einer Gemeindeverwaltung (einer Bündelungsbehörde), wie vom Bundesverfassungsgericht gefordert, eine informationelle Gewaltenteilung der unterschiedlichen funktionalen Stellen. Daraus folgt, dass Meldedaten innerhalb der öffentlichen Stelle Gemeinde grundsätzlich nur von Mitarbeitern der Meldebehörde verarbeitet werden dürfen; die Datenweitergabe an andere Organisationseinheiten innerhalb der Gemeindeverwaltung ist streng zu prüfen und nur im Rahmen der Aufgabenerforderlichkeit zulässig.

Demgegenüber sah die Ablauforganisation der Gemeindeverwaltung vor, jeglichen Posteingang über den Bürgermeister zu leiten. Die damit verbundene grundsätzliche Verarbeitung von Meldedaten durch den Bürgermeister verstieß unter anderem gegen § 4 Abs. 1 SächsMG. Aus § 4 Abs.1 SächsMG ergibt sich für die Meldebehörde die Pflicht vor jeder Verarbeitung von Meldedaten zu prüfen, ob im konkreten Fall eine Rechtsvorschrift die beabsichtigte Maßnahme der Datenverarbeitung erlaubt oder der Betroffene eingewilligt hat (§ 4, Rdnr. 1, a. a. O.). Der Bürgermeister ist nicht Mitarbeiter der Meldebehörde und eine Rechtsvorschrift, die ihm die Verarbeitung der Meldedaten anlassfrei erlauben würde, ist nicht ersichtlich. Nach § 9 Abs. 1 SächsDSG haben öffentliche Stellen, die personenbezogene Daten verarbeiten, alle personellen, technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um eine den Vorschriften des Datenschutzgesetzes entsprechende Datenverarbeitung zu gewährleisten. Die bestehende organisatorische Regelung wurde dieser Forderung nicht gerecht. Sie verstieß auch gegen schutzwürdige Interessen der Betroffenen nach § 22 SächsMG und das Meldegeheimnis.

Nur, wenn es für die eigene Aufgabenerfüllung als Dienstherr und Leiter der Gemeindeverwaltung, etwa für dienstaufsichtliche Maßnahmen gegen Mitarbeiter der Meldebehörde, erforderlich gewesen wäre, hätte der Bürgermeister zweckgebunden Kenntnis von den Meldedaten der Antragstellerin nehmen dürfen.

Die festgestellte Kenntnisnahme über die Rückmeldung der Anmeldung der neuen Hauptwohnung von der dortigen Meldebehörde durch den Bürgermeister war deshalb unbefugt und rechtswidrig. Der Bürgermeister hätte - ebenso wie jeder andere (jedermann) - einen Antrag nach § 32 Abs. 1 SächsMG stellen können, um die neue Anschrift seiner von ihm getrennt lebenden Ehefrau zu erhalten. Die Kenntnisnahme ohne Antragstellung ermöglichte es der Meldebehörde zudem nicht, von ihrer nach dem Gesetz vorgeschriebenen pflichtgemäßen Ermessensausübung vor der Auskunftserteilung Gebrauch zu machen. Eine Prüfung nach einem Auskunftsverbot

nach § 32 Abs. 4 SächsMG bzw. einer eingetragenen Auskunftssperre nach § 34 SächsMG war damit von vornherein ausgeschlossen.

Ich hatte zur Kenntnis zu nehmen, dass sich der Bürgermeister unter Verletzung datenschutzrechtlicher Regelungen und Ausnutzung seiner Dienststellung Meldedaten für private Zwecke beschafft hatte und das in seinen Stellungnahmen verneinte.

Nach meiner Beanstandung teilte mir der Bürgermeister mit, dass meine Forderungen zur Beseitigung der datenschutzrechtlichen Mängel erfüllt worden seien. Es sei eine durch die Rechtsaufsichtsbehörde genehmigte Zweckvereinbarung zwischen seiner und der anderen Gemeinde zur Übertragung der Aufgaben des Melde-, Pass- und Ausweiswesens geschlossen worden. Darüber hinaus sei durch eine entsprechende Dienstanweisung eine Veränderung der Organisation des Posteingangs vorgenommen worden, welche die datenschutzrechtlich geforderte funktionale Trennung der Behörden gewährleistet.

5.3.4 Übermittlung von Jubiläumsdaten an Landräte und Regierungspräsidenten

Wie ich in Erfahrung brachte, erhielten ein Landrat und der Präsident eines Regierungspräsidiums von den Meldebehörden kreisangehöriger Gemeinden bzw. einer kreisfreien Stadt sog. Jubiläumsdaten von Einwohnern übermittelt. Das ist kein Einzelfall. Ich muss vielmehr davon ausgehen, dass auch noch andere - kommunale und regionale - Funktionsträger abseits gesetzlicher Regelungen regelmäßig Meldedaten übermittelt bekommen. Der Fall ist übertragbar auf viele ähnliche Vorgänge, bei denen es um die (regelmäßige) listenweise Nutzung von Meldedaten geht.

Eine *regelmäßige Übermittlung* von Meldedaten, um Bürgern zum Geburtstag zu gratulieren, Nettigkeiten zu übermitteln und sich als Amtsträger in Erinnerung zu bringen, ist weder gesetzeskonform noch datenschutzgerecht. Zwar habe ich in meinem 6. Tätigkeitsbericht auch die Auffassung mitgeteilt, dass eine Übermittlung der Jubiläumsdaten zum Beispiel an einen Bürgermeister das Grundrecht auf informationelle Selbstbestimmung der Jubilare nicht beeinträchtige, da diese Übermittlung ein *Weniger* sei, als eine Veröffentlichung, die ja nach § 33 Abs. 2 SächsMG zulässig sei (6/5.3.7). Die zunehmend ungenierte Inanspruchnahme von Meldedaten, um sie bei ihrer Verarbeitung einem gewissen (kommunal-)politischen Mehrwert zuzuführen, veranlasst mich nun, Grundsätzliches in Erinnerung zu rufen.

Die Verarbeitung personenbezogener Daten darf nur *normenklar* und *transparent*, auf gesetzlicher Grundlage erfolgen. Das gilt im Besonderen im Meldewesen. Eine Über-

mittlung der Jubiläumsdaten an Landräte und Regierungspräsidenten kann nicht allein auf § 33 Abs. 2 SächsMG gestützt werden, eine Bestimmung, die die Veröffentlichung von Daten zulässt. Die Sächsische Meldedatenübermittlungsverordnung als einschlägige Rechtsvorschrift sieht eine Übermittlung von Jubiläumsdaten ausschließlich an die Sächsische Staatskanzlei vor. Eine regelmäßige Übermittlung von Jubiläumsdaten an Landräte und Regierungspräsidenten verstößt erst recht gegen § 29 Abs. 5 Satz 1 SächsMG, da sie nicht normativ geregelt und vorgesehen ist.

Selbst wenn von keiner regelmäßigen, sondern einer Übermittlung von Jubiläumsdaten auf Anforderung nach § 29 Abs. 1 SächsMG ausgegangen wird, ist von einer unzulässigen Übermittlung personenbezogener Daten durch die Meldebehörde auszugehen, da die vom Gesetzgeber vorgeschriebene Prüfung der Meldebehörde, ob die angeforderten Jubiläumsdaten für die Aufgabenerfüllung des Empfängers erforderlich sind, negativ ausfällt.

Es kommt für die (unzulässige) Übermittlung von Jubiläumsdaten an Landräte oder Regierungspräsidenten letztlich nicht darauf an, dass nach § 33 Abs. 2 SächsMG die Meldebehörde Jubiläumsdaten veröffentlichen und an Presse, Rundfunk oder andere Medien zum Zwecke der Veröffentlichung übermitteln darf. Entscheidend ist die Tatsache, dass für eine Übermittlung von Meldedaten an andere Behörden die dafür erforderliche spezialgesetzliche Regelung fehlt. Auch ein Ausweichen auf die allgemeinen gesetzlichen Regelungen im Sächsischen Datenschutzgesetz, wie § 13 Abs. 2 Nr. 2 SächsDSG, kommt nicht in Betracht. Der Gesetz- und Verordnungsgeber hat mit dem Sächsischen Meldegesetz und der Sächsischen Meldedatenübermittlungsverordnung die Verarbeitung von Meldedaten abschließend geregelt. Im Übrigen fehlt es bei Anwendung des § 13 Abs. 2 Nr. 2 SächsDSG, der das Speichern, Verändern und Nutzen personenbezogener Daten für andere Zwecke unter anderem zulässt, wenn die Daten allgemein zugänglich sind oder die Daten verarbeitende Stelle sie - wie oben ausgeführt - veröffentlichen dürfte, an der Übermittlungsbefugnis der Meldebehörde für diese Daten.

Ich habe das SMI gebeten, die Meldebehörden aufsichtsrechtlich anzuweisen, die Übermittlung von Jubiläumsdaten an Landräte und Regierungspräsidenten einzustellen. Melderecht muss am Gesetz orientiert und übersichtlich bleiben. Es besteht ansonsten die Gefahr, dass im Freistaat ohne gesetzliche Grundlage Privatsammlungen von Teildatensätzen aus den Meldebehörden entstehen. Gratulieren kann (und sollte) der Bürgermeister.

5.3.5 Rechte und Widerspruchsmöglichkeiten der Betroffenen nach dem sächsischen Melderecht

Immer wieder stelle ich fest, dass die betroffenen Bürger keine Kenntnisse von den ihnen nach dem Gesetz zustehenden Rechten und Widerspruchsmöglichkeiten haben (vgl. auch 12/5.3.2).

Auch in Bezug auf die Auskunftssperre besteht Unkenntnis. Eine Auskunftssperre wird auf Antrag oder von Amts wegen eingetragen (§ 34 Abs. 1 Satz 1 SächsMG). Ausreichend für die Eintragung ist nicht nur eine irgendwie geartete Belästigung, sondern erforderlich ist eine Gefahr für Leben, Gesundheit, die Freiheit oder ähnliche schutzwürdige Interessen des Meldepflichtigen. Die Auskunftssperre verhindert allerdings nur Übermittlungen an Private (§ 34 Abs. 2 SächsMG), was offenbar die wenigsten Betroffenen wissen. Auch scheint wenig bekannt zu sein, dass eine Auskunftssperre nicht bedeutet, dass man danach unbehelligt bleibt. Von Amts wegen ist die Meldebehörde gehalten, in den Fällen, in denen eine Auskunft begehrt wird, den Betroffenen anzuhören (§ 34 Abs. 1 Satz 2 SächsMG). Die Auskunftssperre soll nämlich nicht dazu dienen, dass sich Meldepflichtige zum Beispiel auch ihren Zahlungsverpflichtungen entziehen können. Was die Fallmengen angeht, so stelle ich fest, dass die Auskunftssperren in der Verwaltungspraxis nicht so häufig sind. Ich möchte daher den Meldebehörden empfehlen, die Betroffenen über die Rechtslage eingehender zu informieren.

Im Übrigen haben die Betroffenen nach dem Gesetz die Möglichkeit, Widerspruch gegen Datenübermittlungen einzulegen. Kenntnis hiervon haben die Betroffenen immer noch zu wenig und es wird demzufolge immer noch zu wenig Gebrauch von den Widerspruchsmöglichkeiten gemacht:

Nach § 30 Abs. 2 Satz 3 SächsMG haben Betroffene die Möglichkeit, einer Übermittlung ihrer Daten an öffentlich-rechtliche Religionsgesellschaften ihrer - Religionsgesellschaften zugehörigen - Familienangehörigen per Widerspruch zu unterbinden.

Nach § 32 Abs. 4 Satz 4 SächsMG können Meldepflichtige einem automatisierten Abruf bei der einfachen Melderegisterauskunft widersprechen.

Nach § 33 Abs. 4 Satz 1 SächsMG haben die Betroffenen das Recht, eine Auskunftserteilung an Parteien, Wählergruppen und anderen Trägern von Wahlvorschlägen im Zusammenhang mit Wahlen, der Veröffentlichung ihrer Namensangaben, Anschriften im Zusammenhang mit Alters- und Ehejubiläen an Presse, Rundfunk oder andere

Medien sowie der Übermittlung ihrer Namens- und Anschriftendaten an Adressbuch-Verlage und ähnliche Firmen zu widersprechen.

Neben den im Gesetz ausdrücklich genannten Widerspruchsrechten der Einwohner hat die aktuelle Rechtsprechung die Betroffenen weiter gestärkt. Mit Urteil vom 23. Juni 2006 (Az. 6 C 05/05) zum Hamburgischen Meldegesetz hat das Bundesverwaltungsgericht festgestellt, dass die Meldebehörde eine *einzelne* Melderegisterauskunft nicht erteilen darf, wenn diese erkennbar für Zwecke der Direktwerbung begehrt wird und der Betroffene einer Übermittlung seiner Daten für solche Zwecke zuvor ausdrücklich widersprochen hat. Der Meldepflichtige kann der Übermittlung seiner Daten zu Werbezwecken dabei generell - ohne Angabe von Gründen - widersprechen. Die Entscheidung des Bundesverwaltungsgerichts ist für alle sächsischen Meldebehörden bindend und auch bei jedem Einzelauskunftsverlangen - dies ist wichtig - zu beachten. Die Meldebehörden werden die entsprechenden datenschutzorganisatorischen Vorkehrungen zur Beachtung dieser Rechtsprechung zu betreiben haben.

Zusammenfassend dürfte in der Praxis von besonderem Gewicht sein, dass die Betroffenen, die ihre Anschriftenangaben in einem überschaubaren Empfängerkreis verarbeitet wissen wollen, dafür Sorge tragen, dass keinerlei Daten an Adressbuchverlage gelangen (vgl. § 33 Abs. 3 SächsMG). Hierzu gehört auch das gemeindliche Adressbuch. Die Nutzung der meldegesetzlichen Rechte alleine wird jedoch nicht den erhofften Erfolg dahingehend bringen, dass man zukünftig von Werbezuschriften verschont bleibt, wenn nicht gleichzeitig der Betroffene in seinem Privatbereich alles Angemessene dazu beiträgt, dass seine Daten nur bei Erforderlichkeit preisgegeben werden. Insbesondere bei Preisausschreiben und vertraglichen Regelungen sollten die Betroffenen darauf achten, dass einer Weiternutzung ihrer Anschriftendaten, insbesondere zu Werbezwecken, ausgeschlossen wird. Im Übrigen ist insbesondere ein Widerspruch bei der einfachen Melderegisterauskunft im Wege des automatisierten Abrufs und die nicht ausdrücklich geregelte Widerspruchsmöglichkeit gegen Datenübermittlungen zu Marketingzwecken zu empfehlen.

An den Widerspruch selbst sind hinsichtlich der Form und im Hinblick auf die Urheberschaft keine hohen Anforderungen zu stellen. Insbesondere ist ein persönliches Erscheinen - gar unter Vorlage eines Ausweises - regelmäßig nicht erforderlich. Als Hilfestellung für die Betroffenen habe ich ein Antrags-/Widerspruchsformular, das alle Betroffenenrechte berücksichtigt, als Anhang beigelegt (vgl. 16.3.2).

5.3.6 Ordnungswidrigkeitenverfahren und Ermittlungen im Meldewesen

Nach § 25 SächsMG hat die Meldebehörde darauf zu achten, dass das Melderegister vollständig und richtig ist. Sie hat von Amts wegen oder auf Antrag des Betroffenen das Melderegister fortzuschreiben.

Im letzten Berichtszeitraum erreichten mich Beschwerden von Bürgern, die sich durch die Meldebehörden verfolgt und unverhältnismäßig in ihren Persönlichkeitsrechten beeinträchtigt gesehen haben.

In einem Fall hatte die Meldebehörde versucht, die Anwesenheit des Betroffenen in einer Wohnung in einem nicht geringen Zeitraum zu beobachten bzw. abzuschätzen, um darauf hin eine quantitative Berechnung und Gegenüberstellung von mehreren Wohnungen des Petenten vorzunehmen und auf diesem Wege dessen Hauptwohnung zu ermitteln. In der Tat können eigene Ermittlungen der Meldebehörden zu tiefer gehenden Eingriffen in das informationelle Selbstbestimmungsrecht führen. Die Behörde kann - wie im geschilderten Fall geschehen - den Tagesablauf, das Verlassen der Wohnung, Rückkehr zur Wohnung, Besucher (Lebenspartner und Freunde) nachzeichnen, um eine Entscheidung im Hinblick auf die Hauptwohnung treffen zu können. An den Status der Hauptwohnung selbst sind auch gesetzliche Folgen geknüpft, wie u. a. Wahlrecht und Steuerpflicht. Insofern können die eigenen Ermittlungen wegen der mit der Hauptwohnung verbundenen Weiterungen verhältnismäßig sein, sie sind aber erst dann durchzuführen, wenn die Anhörungen und Auskünfte des Meldepflichtigen selbst keine melderechtlich tragbaren Ergebnisse erbringen. Die Meldebehörde hat bei dem Verfahren der Fortschreibung des Melderegisters also gestuft vorzugehen und zu versuchen, zunächst mit dem mildesten Mittel das Ziel zu erreichen, also ganz im Sinne einer strengen Erforderlichkeit zu handeln. Bei ihrem Tätigwerden hat die Meldebehörde darüber hinaus eigene Mitarbeiter einzusetzen. Es gilt das Prinzip der informationellen Gewaltenteilung innerhalb der Gemeindeverwaltung. Darüber hinaus unterliegen die mit den Ermittlungen zum Wohnsitz erfassten und verarbeiteten Daten einer strengen Zweckbindung und den Regelungen zur Löschung gemäß § 26 Abs. 1 Nr. 2 SächsMG bzw. Sperrung nach § 21 Abs. 2 Satz 2 SächsDSG. Im von mir geprüften Einzelfall war der Betroffene seiner Meldepflicht nach § 10 SächsMG nicht nachgekommen. Auch eine Ordnungswidrigkeit stand damit im Raum (§ 35 Abs. 1 Nr. 3 SächsMG). Für die nicht ordnungsgemäße Anmeldung gab es dabei tatsächliche Anhaltspunkte und auch durch eine erfolgte Anhörung konnte keine weitergehende Klärung erreicht werden. Aufgrund der durch die Behörde sicherzustellenden Zuverlässigkeit des Melderegisters als Informationsgrundlage für die gesamte Verwaltung und Rechtspflege und der durch Unrichtigkeit

oder Unvollständigkeit der Daten möglicherweise beeinträchtigten schutzwürdigen Interessen Dritter und des Betroffenen selbst, war die Meldebehörde in Bezug auf das Entschließungsermessen gebunden und hatte letztendlich mit Ermittlungen zu beginnen. Einen Datenschutzverstoß konnte ich trotz der Eingriffstiefe bei der Datenverarbeitung - abgesehen von einer datenschutzorganisatorischen Unzulänglichkeit, der Beteiligung von Ordnungsamtsmitarbeitern anstatt Beschäftigten der Meldebehörde bei den Ermittlungen - nicht feststellen.

5.4 Personenstandswesen

5.4.1 Bilddatenübermittlung an Krankenkassen aus staatlichen Registern

Im Zusammenhang mit Datenerhebungen zur neuen Krankenversichertenkarte erhielt ich eine Anfrage der Staatsregierung, ob eine direkte Übermittlung der Lichtbilddaten aus dem Passregister beziehungsweise aus dem Personalausweisregister an Krankenkassen zulässig sei. Nach den sozialgesetzlichen Bestimmungen soll die neue Versichertenkarte - bis auf Ausnahmefälle - auch ein Lichtbild des Versicherten enthalten (§ 291 Abs. 2 SGB V). Vorgeschlagen wurde dabei eine Erhebung der Lichtbilddaten ohne Kenntnis bzw. Einwilligung der Betroffenen. Zwar gestatten die Bestimmungen des SGB V die Verarbeitung von Lichtbilddaten der Versicherten, jedoch ist hiervon eine Übermittlung von Lichtbilddaten aus dem Passregister z. B. zu unterscheiden. Im Ergebnis habe ich eine Zulässigkeit verneint.

Lichtbilddaten aus den staatlichen Registern zu übermitteln, um sie ohne Einwilligung auf den Versichertenkarten aufzubringen, hätte so gesetzlich normiert sein müssen. Eine gesetzliche Stütze für derartige Übermittlungen und Registerdatennachnutzungen findet sich nicht im Gesetz und hätte insofern eine unzulässige Zweckänderung der Datenverarbeitung der Registerdaten dargestellt. Pass- und Personalausweisgesetz bieten öffentlichen Stellen lediglich die Möglichkeit, in gesetzlich beschriebenen Fällen Lichtbilddaten zu vergleichen bzw. abzugleichen. Pass- und Personalausweisregister sind auch nicht als Auskunftsregister angelegt. Auch wären die Versicherten selbst gehalten, ihren vertraglichen Mitwirkungspflichten nachzukommen, um ihre Gesundheitsversorgung zu sichern. Das setzt voraus, dass die Krankenversicherungen die Versicherten auffordern, entsprechende Lichtbilder beizubringen oder diese von den Versicherten selbst anfertigen. Sicherlich bedeutet das mehr Aufwand. Mehraufwand begründet aber datenschutzrechtlich keine Erforderlichkeit.

5.5 Kommunale Selbstverwaltung

5.5.1 Stadtrats- und Kreistagssitzungen - Live-Übertragungen per Fernsehen, Hörfunk und Internet

Bereits in 12/5.5.9 hatte ich mich zu Fragen im Zusammenhang mit der Veröffentlichung von Unterlagen zu Stadtratssitzungen befasst.

Etwa zeitgleich wendeten sich im neuen Berichtszeitraum eine ostsächsische Stadt und ein ostsächsischer Landkreis an mich mit der Fragestellung, ob und inwieweit Gemeinderats- bzw. Landkreissitzungen im Internet übertragen werden könnten. Bereits zuvor hatte ich schon Anfragen zur Zulässigkeit von Live-Fernsehübertragungen. Aufgrund der weiterentwickelten computergestützten Verarbeitungsmöglichkeiten wird man in Bezug auf die Eingriffstiefe bei Hörfunk- bzw. Fernsehübertragungen keinen großen Unterschied mehr im Vergleich zu Bild-/Ton-Internetübertragungen, bei denen die Möglichkeit einer digitalen Weiterverarbeitung vorausgesetzt werden kann, machen können. Die Frage der Art und Weise der Weiterverarbeitung wird zumindest im Hinblick auf Verhältnismäßigkeitsgesichtspunkte einzubeziehen sein. Wer heute mit einer Ungeschicklichkeit auffällt, kann im Falle von veröffentlichten Bild- und Ton-Aufzeichnungen morgen bei „you tube“ im Internet vorgeführt werden. Die Frage ist daher aktuell und von grundsätzlicher Bedeutung.

Eine Internet-Übertragung, und das gilt für Fernseh- und Hörfunkübertragungen gleichermaßen, kann zunächst einmal nur bei öffentlichen Sitzungen überhaupt in Betracht gezogen werden. Soweit es um Angelegenheiten geht, die dem Datenschutz und Persönlichkeitsrechtsschutz unterliegen bzw. um von der Sache her als nicht öffentlich zu handhabende Angelegenheiten, scheiden die thematisierten (Live-)Veröffentlichungsformen ohnehin aus.

Zu den öffentlichen Sitzungen haben die Einwohner und jedermann Zugang (§ 37 Abs. 1 Satz 1 SächsGemO, vgl. auch § 33 Abs. 1 SächsLKrO). Die Ratsmitglieder müssen auch dulden, bei den öffentlichen Sitzungen von den Zuhörern und Zusehern in ihren Reden und optisch wahrgenommen zu werden. Auch die Mitschrift von Reden durch die Zuhörer und die anschließende Wiedergabe wird als sozialadäquat und zulässig zu betrachten sein (§ 48 Abs. 1 Nr. 2 UrhG). Damit und mit dem Öffentlichkeitsgrundsatz des § 37 SächsGemO ist aber noch nicht festgelegt, dass beliebiges Verhalten bei der Verarbeitung der Daten auf der Sitzung statthaft wäre. So hat der Ratsvorsitzende hausrechtlich die Möglichkeit, ungenehmigte fotografische Aufnahmen, Hör-Mitschnitte, das Videografieren und den Einsatz von

Webcams durch Teile der Öffentlichkeit zu untersagen. Ob er aber verpflichtet ist, derartige Datenverarbeitungen zu unterbinden, wird davon abhängen, inwieweit eine geduldete bzw. genehmigte oder auch durch die Gemeinde oder den Landkreis selbst veranlasste Veröffentlichung zulässig ist.

Dabei wird im Einzelnen zu betrachten und zu differenzieren sein, ob Ratsmitglieder, ob Bedienstete in Wort und Bild aufgenommen und inwieweit Zuhörer und Zuschauer der öffentlichen Sitzungen in die Übertragung einbezogen werden sollen sowie, ob es sich um eine nur ausschnittartige Veröffentlichung oder um eine vollständige Übertragung einer Sitzung handelt. Am meisten interessiert wohl die Frage, inwieweit Ratsmitglieder in den Sitzungen veröffentlicht werden können.

Ausschnitte aus Gemeinderatssitzungen in Funk und Fernsehen, als Teil einer zusammenfassenden Presseberichterstattung bei herausgehobenen (zeitgeschichtlichen) Ereignissen sind üblich und bleiben noch datenschutzrechtlich verhältnismäßig, soweit der Zuschauer- und Zuhörerbereich regelmäßig hiervon nicht betroffen, die involvierten Mandatsträger informiert sind und eine im Zusammenhang vollständige Sitzungswiedergabe in Bild und Ton nicht erfolgt (vgl. auch §§ 22, 23 KunstUrhG). Z. T. werden Redner gefragt, aber häufig erfolgt in diesen Fällen der Presseberichterstattung auch keine Tonwiedergabe, sondern ein Bericht des Medienunternehmens. Einen Anspruch auf Bild- und Höraufnahmen bei Gemeinderat und in Kreistagssitzungen ergibt sich gleichwohl nicht aus dem Sächsischen Gesetz über die Presse. Es entscheidet der Hausherr.

Demgegenüber wäre eine vollständige Ton- und Bildwiedergabe z. B. via Internet ein weitergehender qualitativer Eingriff in die Persönlichkeitsrechte der Betroffenen, denn die Intensität der Datenverarbeitung ist eine gänzlich andere als bei einer bloßen Zusammenfassung. Handelt es sich auch um eine Wiedergabe im Bild, so ist das Kunsturhebergesetz mit maßstäblich (§ 22 KunstUrhG). Entscheidend wäre nach dem Kunsturhebergesetz, ob die kommunalen Mandatsträger als relative Personen der Zeitgeschichte anzusehen sind und ob sie diesen weitergehenden Eingriff zu dulden haben.

Gemeinderats- und Kreistagsmitglieder sind nach dem Gesetz ehrenamtliche Mandatsträger, die gleichwohl verpflichtet sind, an den Sitzungen teilzunehmen. Die Gemeinde- und Kreisräte sind keine Ehrenbeamte, sondern lediglich „ehrenamtlich tätig“, einem Ehrenbeamtenverhältnis wegen deren politischen Funktion lediglich angenähert (§ 35 SächsGemO). Im Übrigen nimmt der Gemeinde- bzw. Kreisrat sein Mandat nach seiner freien nur durch das öffentliche Wohl bestimmten Überzeugung

wahr. Im Sinne von Art. 28 GG ist die kommunale Vertretungskörperschaft als Ganzes eine Volksvertretung, aber auf der anderen Seite handelt es sich bei Gemeinderat und Kreisrat auch um Verwaltungsorgane, nicht um Parlamente im Sinne des (staatsrechtlichen) klassischen Parlamentsbegriffs. Das (demokratisch legitimierte) Verwaltungshandeln überwiegt auch in der Aufgabenwahrnehmung, nicht so sehr eine politische Darstellung wie bei Abgeordneten, die mit zunehmender Öffentlichkeit mehr Wirkung entfaltet. Umgekehrt könnte hingegen die sachorientierte Verwaltungstätigkeit im Rahmen der interkommunikativen Ratsarbeit Schaden nehmen, wenn es wegen der Veröffentlichungen zunehmend auf Aussehen, Redegewandtheit und die Wortwahl ankäme. Manches Ratsmitglied müsste sich bei einer vollständigen Wiedergabe seiner Wortbeiträge vielleicht hüten, sich überhaupt noch zu Wort zu melden und Entscheidendes könnte hinter verschlossenen Türen ausgehandelt werden, dies wäre kontraproduktiv für den kommunalgesetzlich normierten Öffentlichkeitsgrundsatz, der auch den offenen Diskurs einschließt. Dass die kommunalen Vertretungskörperschaften also keine Parlamente darstellen, muss insofern auch praktische Auswirkungen haben.

Individualrechtlich jedenfalls können die für Parlamente geltende Verfassung, die Gesetze und Verhältnisse nicht einfach auf den Gemeinderat, den Kreistag und dessen Mitglieder übertragen werden. Steht der einzelne Gemeinde- oder Kreisrat in einem öffentlich-rechtlichen Amtswalterverhältnis, anders als ein Abgeordneter, ist er anders gestellt, verfügt er weder über Immunität noch Indemnität, sind die Gemeinde- und Kreistage wegen ihres beschränkten Wirkungskreises keine Gemeinschaft relativer Personen der Zeitgeschichte, so ist dem in Umfang, Tiefe und Ausmaß der Datenverarbeitung Rechnung zu tragen. Werden Fernsehübertragungen von Parlamentssitzungen anerkanntermaßen einseitig durch die Präsidien entschieden und in Hausordnungen geregelt, so können Gemeinde- und Kreisräte unverhältnismäßig in ihrem Grundverhältnis betroffen sein, soweit eine tiefer gehende Datenverarbeitung der Sitzungen der kommunalen Vertretungskörperschaften im Sinne von vollständigen Veröffentlichungen und nicht mehr zu kontrollierenden Datenverarbeitungen der öffentlichen Sitzungen erfolgt. § 37 Abs. 1 Satz 1 SächsGemO enthält nur die Festlegung, dass Ratssitzungen öffentlich oder nicht-öffentlich unter Berücksichtigung der berechtigten Interessen Einzelner und des öffentlichen Wohls stattzufinden haben. Die räumlich-gegenwärtige Öffentlichkeit bei Ratssitzungen genügt dem Öffentlichkeitsgrundsatz aber bereits. Differenzierungen nimmt das Gesetz nicht vor. Ratsmitgliedern ist daher zumindest die Möglichkeit zu geben, in eine weitergehende Öffentlichkeit, als es das Gesetz erfordert, einzuwilligen (§ 4 Abs. 3 SächsDSG bzw. § 4a BDSG und § 22 Abs. 1 Satz 1 KunstUrhG). Fraglich ist wegen der Berücksichtigung der einzelnen Räte als Grundrechtsträger daher m. E. auch, ob z. B. eine

Veröffentlichung via Internet mit kommunaler Rechtssetzung, z. B. mit einer Geschäftsordnung oder auch per Satzung für alle Mitglieder der Vertretungskörperschaft pauschal und verbindlich vorgegeben werden kann.

Sofern Beschäftigte der Verwaltung betroffen sind, so gilt Entsprechendes. Für Mitarbeiter, die sich beruflich in der Öffentlichkeit bewegen, wie etwa Beigeordnete, wird man wiederum einseitig eine zusammenfassende Berichterstattung zulassen können, wenn ein zeitgeschichtlicher Grad erreicht wird. Im Übrigen wäre auch wiederum eine Einwilligung vonnöten.

Letztendlich bergen vollständige Veröffentlichungen von Ratssitzungen via Internet, Fernsehen oder Rundfunk noch die Möglichkeit, dass betroffene Einwohner und andere Personen in Wort und Bild mit veröffentlicht werden, so z. B. bei Fragestunden in öffentlichen Sitzungen - vgl. § 44 Absatz SächsGemO - oder bei anderer Gelegenheit, selbst bei Zwischenrufen. Eingewilligt werden müsste aber auch in diesen Fällen. Aus Praktikabilitätsgründen sollte für diesen Bereich eine Ton- und Bildveröffentlichung nicht angestrebt werden.

Im Ergebnis wird man also gerichtsfest Veröffentlichungen von Ratssitzungen nur über die Einwilligung herstellen können. Die Einwilligung hat freiwillig zu erfolgen, d. h. ihre Verweigerung muss für den Grundrechtsträger folgenlos bleiben. Leicht umzusetzen wird eine Veröffentlichung dann in der Regel nicht mehr sein, da datenschutzorganisatorisch zu vermeiden ist, dass Bild- und Tonaufnahmen Nicht-Einwilligender übertragen werden. Die entsprechenden personellen und technischen datenschutzorganisatorischen Vorkehrungen können aufwendig werden, wenn bei einer Veröffentlichung auf Nicht-Einwilligende und den Zuschauerbereich Rücksicht genommen werden soll. Personen sind im Bild auszublenden bzw. nicht im Ton zu übertragen. Gegen eine derartig am Gesetz orientierte und den Interessen der Grundrechtsträger Rechnung tragende Haus- oder Geschäftsordnungsregelung, die Veröffentlichungen zulässt, wird man datenschutzrechtlich aber nichts einzuwenden haben. Ob lückenhafte Veröffentlichungen dieser Art noch Sinn machen, ist eine ganz andere Frage.

Unberührt und von obigen Ausführungen zu unterscheiden ist die Thematik der zu Verwaltungszwecken von der Kommune selbst veranlassten Ton-Aufzeichnungen zum Zweck der Anfertigung von Protokollen. Die Aufzeichnung des gesprochenen Wortes kann zur Aufgabenerfüllung erforderlich sein und ist immer dann zulässig, wenn sie normativ geregelt ist, so dass die betroffenen Ratsmitglieder von dieser Datenverarbeitung positiv Kenntnis haben. Eine Weiterverarbeitung im Sinne einer

Veröffentlichung findet dabei aber wegen der Zweckbindung auch nicht statt (vgl. 10/5.5.4).

5.5.2 Informationsschreiben der Gemeinde an weggezogene (abgemeldete) Einwohner

Aufgrund des starken Wegzuges von Einwohnern aus sächsischen Gemeinden versuchen die Gebietskörperschaften verschiedentlich bei wegziehenden Einwohnern durch Informationsschreiben das Interesse an einer Wiederkehr zu wecken (Informationsschreiben über die gemeindliche Entwicklung allgemein, Zusendung von Stellenangeboten etc.). Hiergegen ist grundsätzlich nichts einzuwenden, denn diese Absicht ist durchaus eine Angelegenheit der örtlichen Gemeinschaft, die der kommunalen Selbstverwaltung zuzurechnen ist.

Selbstverständlich unterliegt aber auch diese Datenverarbeitung dem Recht auf informationelle Selbstbestimmung. Rechtliche Bestimmungen sind einzuhalten. Eine Nutzung der Melderegister ohne Kenntnis der Betroffenen zum Zweck von Anschreiben ist nicht zulässig. Das Melderecht sieht eine Verarbeitung von aus der Gemeinde weggezogenen Personengruppen nach Listen nicht vor (vgl. § 29 Abs. 1 Satz 2 SächsMG). Das Sächsische Meldegesetz ist abschließend. Meldegesetzlich kann das Anliegen, wegziehende oder weggezogene Bürger an ihre Heimatgemeinde zu binden, nicht gelöst werden.

Eine Datenverarbeitung nach allgemeinen Datenschutzregeln bleibt aber möglich. Da es sich bei dem Zweck durchaus um eine Angelegenheit im Sinne von Art. 28 Abs. 2 GG i. V. m. § 1 Abs. 2 SächsGemO handelt, ist es datenschutzrechtlich zulässig, für wegziehende Einwohner ein Informationsblatt bereitet zu halten und diesen die Möglichkeit zu geben, sich für weitere Informationen und Anschreiben der Gemeinde zu registrieren und in diese Datenverarbeitung einzuwilligen (§ 4 Abs. 3 SächsDSG). Einwilligungsschreiben könnten auch über das Internet - vorzugsweise zum Herunterladen - verbreitet werden. Zusätzlich empfehle ich, in Bezug auf die beabsichtigte Datenverarbeitung zumindest einen Beschluss des Stadtrates herbeizuführen und diesen ortsüblich bekanntzumachen.

5.5.3 Verschwiegenheitspflicht der Gemeinderäte

Auch im letzten Berichtszeitraum gab es wieder Vorgänge, die im Zusammenhang mit der Verschwiegenheitspflicht von Gemeinderäten bzw. Mitarbeitern kommunaler Verwaltungen gestanden haben. Bereits in der Vergangenheit hatte ich über Beispiele

berichtet (10/5.5.5; 11/5.5.4). Wie schwierig sich der Bereich im Einzelfall rechtlich und praktisch darstellen kann, mag nachfolgendes Beispiel zeigen.

Bei einem Vorgang war ein Stadtrat in den Verdacht geraten, Angaben aus einem als Grundstücksverkaufsangelegenheit und darüber hinaus baurechtlich und denkmalschutzrechtlich zu behandelnden Vorgang an eine Zeitung gegeben zu haben. U. a. wurden durch die Veröffentlichung der Zeitung Einzelheiten zu den vom Eigentümer gemachten Aufwendungen bekannt. Offenbart wurden einzelnen Stadträten die personenbezogenen Angaben anlässlich einer Akteneinsichtnahme nach § 28 Abs. 4 SächsGemO. Danach wurden die Informationen in nicht-öffentlicher Sitzung eines Ausschusses thematisiert, bevor sie an die Zeitung gelangten. Die Stadt selbst verneinte, die Angaben an die Zeitung weitergegeben zu haben. Soweit die in Rede stehende Information an die Presse tatsächlich durch einen Stadtrat erfolgt war, wurde gegen die Verschwiegenheitspflicht nach § 19 Abs. 2 und § 37 Abs. 2 SächsGemO verstoßen. Wer für die Datenübermittlungen letztendlich tatsächlich verantwortlich war, konnte ich im Berichtszeitraum aber nicht aufklären.

Allgemein bleibt zu sagen, dass die Verschwiegenheitspflicht des § 19 SächsGemO dem Schutz der Interessen der Allgemeinheit, aber auch des einzelnen Bürgers dient. Vom Schutzzweck und vom Inhalt her kann man sie mit der Pflicht zur Amtsverschwiegenheit nach § 78 SächsBG für Beamte und § 9 BAT-O für Angestellte und Arbeiter gleichsetzen (vgl. Menke/Arens - Gemeindeordnung für den Freistaat Sachsen, 4. Aufl., § 19 Rdnr. 2 f.). Gesetzlich ist die Verschwiegenheit besonders anzuordnen, wenn sie nicht gesetzlich vorgeschrieben ist. Sie kann aber auch aus der Natur der Sache folgen. Bei Akten der Stadtverwaltung, die im Hinblick auf ihren Inhalt der Amtsverschwiegenheit unterlegen haben, ist von einer Verschwiegenheit auszugehen, denn die Amtsverschwiegenheit wirkt fort, d. h. die erst mit Quorum mögliche Einsichtnahme in Verwaltungsakten der Stadt durch Stadträte kann nicht dazu führen, dass der Amtsverschwiegenheit unterliegende Informationen einen geringeren Schutz genießen. Natürlich verfügen einzelne Gemeinderäte auch nicht über die Befugnis selbständig zu entscheiden, ob die Voraussetzungen für die Geheimhaltung gegeben sind oder nicht. Eine Verschwiegenheit besteht solange, bis sie vom Gemeinderat im Einvernehmen mit dem Bürgermeister aufgehoben wird. (vgl. Menke/Arens - Gemeindeordnung für den Freistaat Sachsen, 4. Aufl., § 37 Rdnr. 8). Die Verschwiegenheitspflicht des § 37 SächsGemO umfasst zudem auch alle Kenntnisse, die durch die Teilnahme an einer nicht-öffentlichen Sitzung erlangt worden sind.

Offen geblieben war letztendlich auch, ob ein Mitarbeiter der Stadtverwaltung, der Zugang zu den Akten gehabt hatte, ein in die Akten Einsicht nehmender Stadtrat oder ein Stadtrat, der an der nicht-öffentlichen Ausschusssitzung teilgenommen hatte, Einzelangaben an die Zeitung gab. Auch eine Beteiligung mehrerer Personen war denkbar. Eine Aufhebung der Verschwiegenheit als Voraussetzung für eine Freigabe war nach Auskunft der Stadtverwaltung zu keinem Zeitpunkt erfolgt. So war in jedem Fall von einem datenschutzrechtlichen Verstoß gegen § 16 SächsDSG (Übermittlung an nicht-öffentliche Stellen) auszugehen, denn sowohl die Stadträte, Ausschüsse, als auch die Verwaltungsmitarbeiter sind Teil öffentlicher Stellen im Sinne von § 2 Abs. 1 SächsDSG. Und eine unbefugte Übermittlung personenbezogener Daten ist niemals erforderlich und somit immer ein Datenschutzverstoß.

Strafrechtlich kamen mehrere Bestimmungen in Betracht, § 39 SächsDSG, § 203 StGB (und § 353b StGB in Bezug auf Gemeindebedienstete).

Bei einer möglichen Datenübermittlung durch einen Gemeinderat wäre es nach § 203 StGB für eine Verletzung von Privatgeheimnissen erforderlich, dass ein Geheimnis durch die offenbarende Person als Amtsträger oder als für den öffentlichen Dienst besonders Verpflichteten unbefugt offenbart worden ist. Aufwendungen und Kosten waren im vorliegenden Fall als personenbezogenes Geschäfts- und Betriebsgeheimnis im Sinne von § 203 StGB schutzwürdig. Eine Offenbarung lag mit einer Information an die Presse und einer anschließenden Veröffentlichung vor, ein unbefugtes Handeln auch. Fraglich war jedoch nach neuerer Rechtsprechung, ob Gemeinderäte überhaupt als Amtsträger einzuordnen sind, § 203 Abs. 2 Nr. 1 StGB. Dies richtet sich nämlich nach § 11 Abs. 1 Nr. 2 StGB. Bisher wurde in der Literatur und in der Rechtsprechung überwiegend davon ausgegangen, dass Gemeinderäte als Inhaber öffentlicher Ämter auch als Amtsträger anzusehen seien (vgl. 12./5.5.3, S. 75 ff. m. w. N.; vgl. Menke/Arens - Gemeindeordnung für den Freistaat Sachsen, 4. Aufl., § 35 Rdnr. 1). Der BGH hat in einer Entscheidung vom 9. Mai 2006 (5 StR 453/05) jedoch entgegen der Auffassung der Vorinstanz die Amtsträgerschaft nur für den Fall bejaht, dass konkrete Verwaltungsaufgaben übertragen worden sind, die über die Mandatstätigkeit in der kommunalen Volksvertretung hinausgehen. Im Übrigen wird § 11 Abs.1 Nr. 2 b und c StGB verneint. Die Frage, ob der Gemeinderat Amtsträger ist, richtet sich zukünftig bei vergleichbaren Fällen somit - folgt man dem BGH - also maßgeblich danach, ob eine Beauftragung mit konkreten Verwaltungsaufgaben stattgefunden hat oder nicht. Dies dürfte zu einer empfindlichen Strafbarkeitslücke in der Praxis führen.

Letztendlich wäre nach § 39 SächsDSG die Begehung einer Ordnungswidrigkeitenhandlung nach § 38 Abs. 1 Nr. 1 bis 8 gegen Entgelt oder in Bereicherungsabsicht oder Schädigungsabsicht strafbar. Auch der Versuch ist nach dieser Bestimmung bereits strafbar. Da im vorliegenden Fall Stadträte nicht auf das Datengeheimnis verpflichtet worden waren, wobei sich ein Teil der Stadträte dem widersetzte, wäre auch Nr. 3 nicht mehr in Frage gekommen. In Betracht wäre lediglich noch eine Verarbeitung in Form einer unbefugten Übermittlung nach § 38 Abs. 1a SächsDSG gekommen, was eine Übermittlung in Bereicherungs- oder Schädigungsabsicht vorausgesetzt hätte, so z. B. wenn der Presseinformant bezahlt worden sein sollte oder auf eine Ansehensbeeinträchtigung des Betroffenen abgezielt worden wäre.

Vgl. des Weiteren 12/5.5.3 zu der Thematik und zur Notwendigkeit der Verpflichtung auf das Datengeheimnis bei Gemeinderäten.

5.5.4 Geschäftsführerbezüge bei Eigenbetrieben und kommunalwirtschaftlichen Gesellschaften

Im letzten Berichtszeitraum bin ich mehrfach auf die Befugnis zur Veröffentlichung der Bezüge und Gehälter von Geschäftsführern kommunaler Unternehmen angesprochen worden. Zum einen geht es um die Frage, ob die Veröffentlichung der Bezüge des Geschäftsführers eines Eigenbetriebes erfolgen kann und muss und zum anderen um die Frage, ob den Vertretungskörperschaften der Kommunen Gehaltsstrukturen und einzelne Gehälter bei Eigenbetrieben zugänglich gemacht werden können, bzw. zu machen sind. Soweit es um Einzelangaben geht, handelt es sich selbstverständlich um personenbezogene Daten (§ 3 Abs. 1 SächsDSG, vgl. auch § 3 Abs. 1 BDSG).

Eigenbetriebe sind rechtlich nicht verselbständigte Organisationseinheiten einer Gebietskörperschaft, z. B. einer Gemeinde. Sie sind daher funktionale Stellen im Sinne von § 2 Abs. 1 SächsDSG. Soweit Betriebe in Privatrechtsform betrieben werden und von der öffentlichen Stelle - z. B. der Gemeinde - beherrscht werden, sind sie Stellen im Sinne von § 2 Abs. 2 Satz 1 und 2 SächsDSG. Letztere Stellen fallen nicht unter das Eigenbetriebsgesetz und die Eigenbetriebsverordnung.

Für Eigenbetriebe gilt, dass nach § 7 SächsEigBVO die Vorschriften über die Bilanz und die Gewinn- und Verlustrechnung, die Bewertungsvorschriften und die Vorschriften über den Anhang für den Jahresabschluss des 3. Buches des Handelsgesetzbuches (HGB) sinngemäß Anwendung finden, was zur Folge hat, dass Gehaltsangaben offenbart werden. § 10 Abs. 1 SächsEigBVO bestimmt zudem, dass § 286 Abs. 2, 3, 4 HGB keine Anwendung findet. Der Geschäftsführer z. B. ist eine „sonstige für den Eigenbetrieb in leitender Funktion tätige Person“ nach § 10 Abs. 1

SächsEigBVO. Nach dieser Bestimmung findet § 285 Nr. 9 HGB daher z. B. für diesen Anwendung. Da eine entsprechende Anwendbarkeit in § 10 Abs. 1 SächsEigBVO normiert ist, kommt es nicht darauf an, ob es sich im Sinne von § 285 Nr. 9 HGB um eine „Personengruppe“ handelt. Insofern können auch eindeutig zuordenbare Einzelangaben zu Bezügen eines einzelnen Führungsmitarbeiters bekannt werden. Ich habe insoweit keine datenschutzrechtlichen Bedenken, zumal im Falle eines privaten Unternehmens eine Veröffentlichung auch möglich wäre, auch wenn im Einzelfall nach § 286 Abs. 4 HGB eine Unterlassung von Angaben erfolgen kann. Aus Transparenzgründen jedenfalls wird die Veröffentlichung von Geschäftsführerbezügen (öffentlicher) Kommunalwirtschaftsbetriebe daher und wohl auch unter Verhältnismäßigkeitsgesichtspunkten verfassungsrechtlichen Anforderungen genügen.

Was die übrigen Beschäftigten von Eigenbetrieben angeht, werden an den Tarifverträgen orientierte Gehaltsstrukturen die Regel sein, die eine gewisse Transparenz gewährleisten. Ohnehin sind die Personalkosten in den Haushaltsplan aufzunehmen und damit für die Vertretungskörperschaften kostenmäßig nachvollziehbar. Eine Offenbarung der Bezüge einzelner Beschäftigter bedeutet dies noch nicht und würde nur gemessen an der Bedeutung und im Einzelfall in nicht-öffentlicher Sitzung beraten werden können.

Ein Zugriff auf die nicht individualbezogenen Gehaltskosten im Ganzen ergibt sich bei verselbständigten Betrieben in Privatrechtsform - bei Stellen nach § 2 Abs. 2 Satz 1 und 2 SächsDSG - für die Vertretungskörperschaft des Eigentümers ebenfalls regelmäßig über den zuständigen Ausschuss. Die Bekanntmachung einzelner Gehaltsposten in nicht-öffentlichen zuständigen Ausschüssen wird sich wiederum nur im Einzelfall, etwa bei Verdacht einer unerlaubten Handlung begründen lassen. Gegen eine Bekanntmachung der Gesamtkosten der in leitender Funktion tätigen Personen gegenüber dem Rat, einem seiner Organe oder der Öffentlichkeit, begegnen meinerseits im Licht des § 285 HGB keinen datenschutzrechtlichen Bedenken.

5.5.5 Überprüfung der Wählbarkeit eines Stadtrats durch den Bürgermeister

Eine betroffene Stadträtin wandte sich an mich, nachdem sie vom Bürgermeister aufgefordert worden war, auf einer Ältestenratssitzung zu ihrem Hauptwohnsitz Stellung zu nehmen. Die Gesamtumstände ließen den Schluss zu, dass hierfür Melderegisterdaten genutzt worden waren.

Nach § 34 Abs. 1 SächsGemO scheidet ein Mitglied aus dem Gemeinderat aus, wenn während der Wahlperiode der Verlust seiner Wählbarkeit eintritt oder bekannt wird, das heißt, wenn es nicht mehr Bürger der Gemeinde ist. Bürger der Gemeinde ist nach § 15 Abs. 1 SächsGemO jeder Deutsche im Sinne des Artikels 116 GG, der das 18. Lebensjahr vollendet und seit mindestens drei Monaten seine Hauptwohnung in der Gemeinde hat. Die Feststellungen über das Ausscheiden trifft der Gemeinderat. Vorsitzender des Gemeinderats und Leiter der Gemeindeverwaltung ist der Bürgermeister (§ 51 Abs. 1 SächsGemO).

Die Gemeinde ist auch Meldebehörde. Der Meldepflichtige hat bei jeder An- oder Abmeldung mitzuteilen, welche weiteren Wohnungen er hat und welche Wohnung seine Hauptwohnung ist. Ändern sich die für die Bestimmung der Hauptwohnung maßgeblichen Umstände, hat dies der Meldepflichtige innerhalb von zwei Wochen der Meldebehörde der neuen Hauptwohnung schriftlich mitzuteilen (§ 12 Abs. 4 SächsMG). Die Meldebehörde ist bei unrichtigem oder unvollständigem Melderegister befugt, von Amts wegen oder auf Antrag des Betroffenen zu berichtigen oder zu ergänzen (§ 25 SächsMG). Ergeben sich konkrete Anhaltspunkte, dass bestimmte Meldedaten unrichtig sein könnten, ist die Meldebehörde verpflichtet, sich im Rahmen des Möglichen und Zumutbaren um die Aufklärung des Sachverhalts zu bemühen (Darré/Rimmele/Thalheim/Wunsch, Sächsisches Meldegesetz, 2. Aufl., § 25 Rdnr. 6). Meldedaten unterliegen dem Meldegeheimnis nach § 9 SächsMG.

Der Bürgermeister ist gleichzeitig Vorsitzender des Gemeinderats und Leiter der Gemeindeverwaltung. Als Vorsitzender des Gemeinderats ist er für dessen gesetzmäßiges Handeln einschließlich rechtmäßig zustande kommender Beschlüsse verantwortlich. Die Teilnahme eines seine Wählbarkeit nicht mehr besitzenden Stadtrats ist gesetzwidrig.

Meine Kontrolle ergab, dass aus Sicht des handelnden Bürgermeisters Anhaltspunkte für eine Änderung der Hauptwohnung vorgelegen hatten.

Der Bürgermeister handelt in vergleichbaren Fällen nicht als Meldebehörde, sondern als Vorsitzender des Gemeinderats. Datenschutzgerecht ist dann folgende Vorgehensweise: Der Bürgermeister kann - wie unter den Umständen des konkreten Vorgangs - ein entsprechendes Auskunftsersuchen an die Meldebehörde richten und Meldedaten verarbeiten (§ 29 Abs. 7 SächsMG). In der Folge wäre es ihm sodann möglich, Zweifel am eingetragenen Hauptwohnsitz bei der Meldebehörde vorzutragen und diese kann dann von ihrem Recht auf Fortschreibung des Melderegisters nach § 25 SächsMG Gebrauch machen und bei der Stadträtin nachfragen bzw. Ermittlungen

durchführen. Eine Befassung im Stadtrat oder dem Ältestenrat wird hingegen regelmäßig ohne eine Offenbarung von Meldedaten Betroffener erfolgen können.

5.5.6 Verwendung pflichtwidrig nicht gelöschter Daten in Disziplinarverfahren sowie in Ermittlungsverfahren

Ein Verwaltungsbediensteter einer großen sächsischen Stadt, der in einem Disziplinarverfahren Vorermittlungen zu einem kommunalen Beamten führte, wandte sich mit der Frage an mich, ob personenbezogene Daten, die unzulässig, da nicht mehr für die Aufgabenerfüllung erforderlich, gespeichert waren, im Disziplinarverfahren verwendet werden dürften. Konkret handele es sich um Daten aus länger zurückliegenden und abgeschlossenen Ordnungswidrigkeitenverfahren, die, obwohl für die Erfüllung der Aufgaben der Behörde nicht mehr erforderlich, noch nicht gelöscht bzw. vernichtet worden seien. Die Staatsanwaltschaft verfüge nun über diese Daten, die sie im Rahmen eines Ermittlungsverfahrens beschlagnahmt habe.

Die Speicherung personenbezogener Daten entgegen der gesetzlichen Löschungspflicht ist eine unzulässige Verarbeitung dieser Daten, was einer weiteren Nutzung dieser Daten - zu welchem Zweck auch immer - grundsätzlich entgegensteht. Gemäß § 20 Abs. 1 SächsDSG sind personenbezogene Daten zu löschen, wenn ihre Speicherung unzulässig oder ihre Kenntnis für die speichernde Stelle zur Erfüllung ihrer Aufgaben nicht mehr erforderlich ist. Personenbezogene Daten, die in Ordnungswidrigkeitenverfahren rechtmäßig erhoben wurden, dürfen für die Dauer des Verfahrens und dessen Durchführung verarbeitet werden. Ist das Verfahren abgeschlossen, etwa durch Zahlung eines Verwarnungs- oder Bußgeldes oder durch Einstellung, sind die Daten zur Erfüllung der Aufgaben der Verfolgungsbehörde nicht mehr erforderlich, sie sind zu löschen.

Das Gesetz trifft in § 21 SächsDSG Aussagen über den Umgang mit personenbezogenen Daten, die zu sperren sind. Für den Fall, dass personenbezogene Daten in Akten gespeichert sind und eine Löschung der Daten nicht in Betracht kommt, da (andere) Teile der Akte zur Aufgabenerfüllung noch erforderlich sind (§ 20 Abs. 2 SächsDSG), sieht § 21 Abs. 2 SächsDSG eine Sperrung dieser Daten vor. Darüber hinaus sind Daten in Akten zu sperren, wenn eine unzulässige Speicherung festgestellt wird. § 21 Abs. 4 Satz 2 SächsDSG bestimmt, dass personenbezogene Daten, die unzulässig in Akten gespeichert sind, ohne Einwilligung des Betroffenen nicht mehr genutzt werden dürfen. Demgegenüber erlaubt § 21 Abs. 4 Satz 1 SächsDSG die Nutzung gesperrter Daten, die nicht unzulässig gespeichert sind, ohne Einwilligung des Betroffenen für bestimmte Zwecke, unter anderem zu Aufsichts- oder

Kontrollzwecken. Aus der Gesamtschau der Vorschrift erschließt sich, dass unzulässig in Akten gespeicherte Daten ohne Einwilligung des Betroffenen gar nicht, auch nicht zu Aufsichts- oder Kontrollzwecken verarbeitet werden dürfen. Nichts anderes kann für unzulässig automatisiert gespeicherte Daten gelten, da der Gesetzgeber von vornherein davon ausgeht, dass diese bei Vorliegen der Voraussetzungen von § 20 Abs. 1 SächsDSG unverzüglich gelöscht werden und es nicht - wie im Fall von Akten (§ 20 Abs. 2 SächsDSG) - zu einer weiteren Speicherung und Sperrung kommen kann.

Der Stadt als verantwortlicher Stelle war damit eine Verarbeitung der Daten, die pflichtwidrig nicht gelöscht worden waren, verwehrt.

Die Staatsanwaltschaft hingegen durfte die beschlagnahmten Daten für die Erfüllung ihrer Aufgaben nutzen. Die Unzulässigkeit der Speicherung durch die Behörde zieht kein Verarbeitungsverbot für die Strafverfolgungsbehörde nach sich.

Allerdings darf die Verwaltungsbehörde der Stadt die von ihr unzulässig gespeicherten Angaben, die die Staatsanwaltschaft rechtmäßig verarbeitet, sich nicht von letzterer „zurückübermitteln“ lassen oder bei dieser erheben, etwa im Wege der Akteneinsicht, um sie dann für ihre eigenen Zwecke zu verarbeiten. Der Makel der Unzulässigkeit der Speicherung könnte durch die Verarbeitung durch die Staatsanwaltschaft bezüglich der städtischen Verwaltungsbehörde nicht behoben werden und würde gewissermaßen wieder aufleben.

An der Durchführung eines disziplinarrechtlichen Verfahrens ist die Stadt dennoch nicht gehindert. Sie kann nur nicht auf unzulässig gespeicherte Daten zurückgreifen, sondern ist auf die Entscheidung der Staatsanwaltschaft bzw. des Gerichts angewiesen und kann diese zur Grundlage einer eigenen Entscheidung machen (§ 15 SächsDO).

5.6 Baurecht; Wohnungswesen

In diesem Jahr nicht belegt.

5.7 Statistikwesen

5.7.1 Schülerregister-Vorhaben der Kultusministerkonferenz

Mein im letzten Tätigkeitsbericht am Ende des Abschnittes 5.7.5 angekündigtes Bemühen, daran zu arbeiten, dass die landesweiten (pseudonymisierten) Schüler- und Lehrerregister und gar das bundesweite (pseudonymisierte) Schüler- und Lehrer-

register nicht zustande kommen, hat einige Früchte getragen: Inzwischen habe ich meine Kollegen in den anderen Bundesländern, wenn auch mit gewissen Abstufungen, an meiner Seite; zugleich ist es erfreulicherweise dabei geblieben, dass das SMK, und zwar namentlich erklärtermaßen inzwischen auch der Staatsminister persönlich, eine dem Vorhaben der KMK gegenüber widerstrebende Haltung eingenommen hat, und der Staatsminister hat bei dem einen oder anderen seiner Kollegen - wenn auch vergleichsweise vorsichtige - Unterstützung bekommen, zumal das Echo in den Medien zum Teil doch recht heftig gewesen ist. Der vom SMK zugunsten des Datenschutzes (und wohl auch der sinnvollen Verwendung von Steuergeldern) bewiesene Mut, dem Gruppendruck innerhalb der KMK zu widerstehen, ist hoch zu veranschlagen. Im Einzelnen ist die Entwicklung folgende gewesen:

Im Dezember 2005 hat das SMK in einer Stellungnahme zu dem von der FDP-Fraktion im Sächsischen Landtag unter Bezugnahme auf meinen 12. Tätigkeitsbericht zugunsten einer auf pseudonymisierte Daten beschränkten Schülerstatistik eingebrachten Antrag (LT-DS-Nr.: 4/3240) mitgeteilt, dass Sachsen sich bei einem unlängst von der KMK gefassten Beschluss zur Fortsetzung der Maßnahmen zur Einführung einer auf der Grundlage von Individualdatensätzen und unter Verwendung eines von allen Ländern anzuwendenden Merkmalskataloges aufzubauenden Schüler- und Lehrerstatistik der Stimme enthalten habe, und zwar mit Blick auf die von mir geltend gemachten datenschutzrechtlichen Bedenken.

Im Frühjahr 2006 hat der Kultusminister dann im Schul- und im Innenausschuss das Vorhaben der KMK in dem Sinne verteidigt, dass Sachsen sich von dem schon seit langem beschlossenen Vorhaben nicht gänzlich fernhalten könne und soweit nötig dann eben die erforderlichen gesetzlichen Grundlagen schaffen müssen werde, allerdings nur vorbehaltlich einer Klärung der datenschutzrechtlichen Fragen! Während ich in diesen Ausschussberatungen noch nicht hatte bestreiten können, mit meinen Einwänden gegen das Vorhaben der KMK unter meinen Kollegen anscheinend eher alleinzustehen, hatte sich das inzwischen schon geändert, wie sich dann im Sommer 2006 fast schlagartig gezeigt hat: Aufgrund meiner eingangs erwähnten Ankündigung und einer Initiative meines sachsen-anhaltischen Kollegen als damaligen Vorsitzenden der Datenschutzkonferenz des Bundes und der Länder tauchte nunmehr das Thema *Datenschutz* auch in Protokollen des von der KMK eingerichteten einschlägigen Arbeitsausschusses auf, wie sich im Juli 2006 aus einer Antwort der damaligen KMK-Präsidentin an meinen ebenfalls inzwischen sehr aktiv gewordenen schleswig-holsteinischen Kollegen ergab. Ende September äußerte sich der sächsische Kultusminister dann in der Presse deutlich zu dem Vorhaben der KMK - und schon zwei Tage später war dieses bundesweit ein Thema für die Presse, naturgemäß

gerade auch unter Bezugnahme auf Sachsen; im Vorfeld der Oktober-Sitzung der KMK äußerte sich nunmehr auch der BfDI kritisch. Während der Vorsitzende der Statistik-Kommission der KMK, der hessische Staatssekretär Jacobi, noch damit zitiert werden konnte, es gebe keine datenschutzrechtlichen Probleme, setzten sich die Kultusminister von Niedersachsen und, deutlicher, Nordrhein-Westfalen vorsichtig von dem Bestreben der KMK ab - eine Zeitung titelte damals zu recht „Sächsisches ‚Nein' wirkt ansteckend".

Am 13. Oktober 2006 erklärte Staatsminister Flath bei einer Fragestunde im Landtag (Anfrage des Abg. Dr. Bartl, LT-DS-Nr.: 4/6612), dass er *die Auffassung des Sächsischen Datenschutzbeauftragten teile und mit seiner Äußerung in der Öffentlichkeit den Anstoß dafür gegeben zu haben hoffe, dass die Angelegenheit nunmehr erstmals unter den Ministern der KMK gründlicher diskutiert werde, sowie dass er, namentlich auch im Hinblick auf die in der DDR ab dem 14. Lebensjahr vergebene „Personenkennzahl" seine Aufgabe darin sehe, die Schüler davor zu schützen, dass sie allzu sehr durchleuchtet würden*.

Nach der Herbstkonferenz der KMK meldete die Süddeutsche Zeitung (21. Oktober 2006) „wachsende Kritik an der Schülerdatei". Die 72. Konferenz der Datenschutzbeauftragten am 26./27. November 2007 hat dann die unter 16.2.17 abgedruckte Entschließung zum Thema verabschiedet.

In der Folgezeit ist es zu Gesprächen von Vertretern der KMK mit solchen der Datenschutzbeauftragten gekommen, einschließlich einer von der KMK unter Beteiligung von Datenschützern und Bildungsforschern veranstalteten Arbeitstagung „Datengewinnungsstrategie für die Bildungsstatistik", auf der ich meine Auffassung erstmals vor einer größeren Öffentlichkeit habe vertreten können. Der auf Datenschutzseite dabei erkennbar gewordene Widerstand gegen die Pläne der KMK hat wieder ein beträchtliches Medienecho (Februar 2007) gefunden.

Der derzeitige Stand ist Folgender:

Die KMK-Spitze lässt inzwischen immerhin knappe Leitlinien ihres Vorhabens verfassen, die sie der Datenschutz-Seite zukommen lässt, damit auf dieser Grundlage ein Dialog zustande kommt. Aus diesen Texten kann man ersehen, dass die KMK sich in Richtung auf eine *stärkere*, nämlich stärkeren Schutz gegen Deanonymisierungsmöglichkeiten bietende, *Pseudonymisierung* der Datensätze bewegt (Verzicht auf Schul- und Klassenidentifikator nicht mehr ausgeschlossen; Gewinnung des zu verwendenden Identifikators mittels Hash-Funktion aus den natürlichen Identifikatoren wie Namen usw.) und auch bei der zentralen Datenhaltung von ihren früheren Maximalvor-

stellungen vorsichtig abzurücken scheint, letzteres, nachdem die Kultusministerien der drei mitteldeutschen Länder sich entschieden gegen das Ziel einer bundesweiten Zusammenfassung der Schüler- bzw. Lehrer-Datensätze ausgesprochen haben.

Aber die von KMK-Seite unterbreiteten Texte bleiben bisher in Vielem verdächtig vage und lassen unverändert keine an grundsätzlichen statistik- bzw. datenschutzrechtlichen Erwägungen ausgerichtete Grundkonzeption erkennen; zugleich hat man den Eindruck, dass die KMK-Vertreter die Datenschutz-Seite für die Verhandlungen über solche unzulänglichen Texte unter für ein rechtlich tragfähiges Ergebnis absolut schädlichen Zeitdruck zu setzen versuchen. Außerdem preschen besonders entschiedene Mitglieder der KMK, wie etwa Schleswig-Holstein, mit besonders weitgehenden und verfassungsrechtlich fragwürdigen landesrechtlichen Regelungen für auf Individualdatensätzen beruhende Landes-Statistiken vor, während andererseits ja noch über die Grundkonzeption verhandelt werden soll.

Die auf Datenschutzseite von Schleswig-Holstein, Nordrhein-Westfalen (Vorsitz des Arbeitskreises Statistik der DSK) sowie Sachsen und dem jeweiligen Vorsitzenden der DSK zu führenden Verhandlungen mit Vertretern der KMK versprechen daher in jeder Hinsicht sehr schwierig zu werden. Erste gemeinsame Besprechungen haben nach dem Berichtszeitraum stattgefunden. Hier ging es vor allem darum, erst einmal eine gemeinsame Basis zur Verständigung zu finden.

Rechtlich wird es vor allem um folgende Fragen bzw. Themen gehen:

(1) Die Dienlichkeit der zu verarbeitenden Daten für Steuerungs- und vor allem für Zwecke der Verbesserung der Leistungsfähigkeit des Bildungssystems in Deutschland und insbesondere des Unterrichtserfolges (auch im Sinne des Abschneidens bei internationalen Leistungsvergleichen wie etwa „PISA“) ist höchst fraglich. Im Bereich der Forschung, auch der staatlicherseits besonders geförderten Forschung (vgl. FAZ vom 14. November 2007, S. 4 „Mehr Forschung für mehr Bildung“) werden inzwischen viel detailliertere, das Unterrichtsgeschehen einbeziehende Daten verwertet, um zu Erkenntnissen zu gelangen, die tatsächlich geeignet wären, von der Bildungspolitik und der Kultusbürokratie für die Verbesserung des Bildungswesens genutzt zu werden.

(2) Das Fehlen jeder Argumentation auf KMK-Seite, aus der sich die Erforderlichkeit der von dieser weiterhin mit großer Entschiedenheit gewollten *Totalerhebung* ergeben könnte, bestärkt mich in meiner Überzeugung, dass diese Totalerhebung nicht erforderlich und daher verfassungswidrig wäre.

(3) (1) und (2) kann man dahingehend zusammenfassen, dass Erkenntnisse für die Verbesserung von Schule nur aus vielen tiefgehenden, insbesondere das Unterrichtsgeschehen und konkrete Schülerleistungen betreffenden Daten, nicht aber aus einer riesigen Gesamtheit an der Oberfläche bleibender Daten aller Schüler gewonnen werden können.

Dies ist so offensichtlich, dass es verfassungsrechtliche Qualität hat oder, anders ausgedrückt, die Einschätzungsprärogative von Exekutive oder auch Gesetzgeber überschritten wäre. Der Aufbau einer solchen großen und zugleich so gut wie unnützen Datensammlung wäre bildungspolitisch bloße Symbolpolitik, die damit verbundenen Eingriffe in das Grundrecht auf informationelle Selbstbestimmung nicht zu rechtfertigen.

(4) Die Unterscheidung und Abgrenzung von *Statistik* und *Verwaltungsvollzug* bei den (primären) Erhebungszwecken und die Trennung der ausschließlich Statistikzwecken dienenden Erhebung und Weiterverarbeitung in organisatorischer Hinsicht hat zur Folge, dass

(a) die ausschließlich statistischen Zwecken dienenden Erhebungsmerkmale in einem formellen Gesetz festgelegt werden müssten (vgl. 12/5.7.5, Teil [1]; alles Folgen aus dem Volkszählungsurteil des Bundesverfassungsgerichts) und

(b) keine Beschränkung der Auswertungsmöglichkeiten, insbesondere der Auswertungs-Thematik, für Dritte, insbesondere die Wissenschaft, aber auch für die Statistikbehörden selbst bestehen dürfte (das ist bei der bloßen Statistik im Verwaltungsvollzug anders).

(5) Nachrangig

(5.1) die Frage der Nützlichkeit der Erhebung und Weiterverarbeitung der Merkmale Schulzugehörigkeit (über Schulidentifikator) und Klassenzugehörigkeit (über Klassenidentifikator), weil diese Merkmale ein starkes Identifizierungsrisiko bieten, und die

(5.2) Unzulässigkeit einer individualdatensatzbezogenen länderübergreifenden Auswertung (vgl. 12/5.7.5 unter [2.3], 2. Absatz).

5.7.2 Kommunale Bürgerumfrage der Stadt Dresden 2007

Wie bereits im Jahr 2002 hat die Dresdner Stadtverwaltung auch bei der Durchführung ihrer „Kommunalen Bürgerumfrage 2007“ (auf der Grundlage einer Satzung

vom 5. Juli 2007, Dresdner Amtsblatt Nr. 27/07), von ihren Einwohnern wieder einmal mehr wissen wollen, als die Stadt angeht. Das hat sich auch in Befremden oder gar Empörung betroffener Bürger niedergeschlagen, die sich bei mir über die Befragung beschwert haben und denen ich im Ergebnis nur habe raten können, einfach das Ausfüllen des Fragebogens zu unterlassen. Denn die Stadt hat die von mir auch diesmal (auf der Grundlage der Beteiligungspflicht nach § 8 Abs. 3 SächsStatG) geltend gemachten Einwände gegen Teile der Datenerhebung, konkret gegen den Entwurf der der Bürgerumfrage zugrunde zu legenden Satzung, im Wesentlichen unberücksichtigt gelassen.

So war erneut bei einer Vielzahl von erfragten Angaben deren mögliche Bedeutung für ein mögliches konkretes (zuständigkeitsgemäßes) Handeln der Stadtverwaltung nicht zu erkennen, was jedoch Voraussetzung dafür ist, dass die Stadt die Angaben über ihre Einwohner überhaupt erheben darf (vgl. ausführlich meine Stellungnahme zur Kommunalen Bürgerumfrage der Stadt Dresden von 2002, 10/5.7.4). So lassen sich z. B. Fragen nach Ernährungsgewohnheiten, Rauchen, Alkoholkonsum, körperlicher Betätigung und Gesundheitsvorsorge, dem Wohlbefinden und der Arbeitssituation oder der Beurteilung der persönlichen wirtschaftlichen Lage, die Frage nach dem ganz persönlichen Bereich zuzurechnenden Umzugsgründen oder das Abfragen von sozialen Kontakten zu Verwandten und sogar Nachbarn in keinerlei Verbindung zu irgendeiner amtlichen Tätigkeit der Stadt bringen.

Trotz meiner rechtlichen Hinweise hat die Stadt weiterhin auch an der rechtswidrigen Befragung von 16- und 17jährigen Jugendlichen festgehalten (vgl. 10. TB a. a. O. unter 3., Seite 55): Auch sie sind erneut in die Umfrage mit einbezogen worden, ohne dass hierfür eine Einwilligung der Sorgeberechtigten (zusätzlich zur Zustimmung des Jugendlichen) seitens der Stadt gefordert worden ist.

Der zwischen der Stadt Dresden und mir in der Sache geführte Schriftwechsel hat gezeigt: Die Rechtspositionen von Stadt, SMI (das die Stadt unterstützt) und mir sind unverändert, die Argumente sind ausgetauscht. In Anbetracht der Tatsache, dass die Rechtslage unverändert ist, habe ich keinen Anlass, meine Rechtsauffassung zu revidieren. Einen Weg zu einem Einvernehmen über eine datenschutzrechtlich bzw. statistikrechtlich einwandfreie Lösung bei der zukünftigen Durchführung entsprechender Bürgerumfragen sehe ich zurzeit nicht, zumal die Stadt sich sogar schon befremdlich wenig bemüßigt gefühlt hat, mir pflichtgemäß (§ 27 Abs. 1 Nr. 1 SächsDSG) den Fragebogen und dessen Begleitschreiben sowie eine Erläuterung zur Rücklaufkontrolle (Datennutzung für Erinnerungsschreiben?) zukommen zu lassen. Es dürfte auch interessant sein, wie hoch am Ende die Rücklaufquote gewesen ist. So

kommt es stark auf den Daten-Selbst-Schutz der Betroffenen an - sie haben hier die Möglichkeit, sich nicht zu beteiligen. Allerdings ist das nicht der Sinn der Regelung des Sächsischen Statistikgesetzes, das amtliche Statistiken der Kommunen, und zwar auch wenn sie ohne Auskunftspflicht durchgeführt werden, in ihrem Erhebungsprogramm auf das begrenzt, was die Kommune für die Ausübung ihrer Zuständigkeiten also, für die Wahrnehmung ihrer Aufgaben braucht (vgl. § 8 Abs. 1 und 2 SächsStatG i. V. m. § 6 Abs. 3 Satz 1, Abs. 6 Satz 2 SächsStatG) - bloße Neugier ist kein legitimer Beweggrund (amtlichen) Kommunalstatistik; sog. Stadtforschung ist Forschung, und Forschung ist nach unserer Rechtsordnung, insbesondere auch Art. 28 Abs. 2 GG, keine den kommunalen Gebietskörperschaften zukommende Aufgabe.

Eines allerdings muss man der Landeshauptstadt zugute halten: Ihre Verfehlungen auf diesem Gebiet bleiben nicht verborgen - inwieweit woanders im Freistaat von allen Kommunen die schon erwähnte, in § 8 Abs. 3 SächsStatG ausgesprochene Pflicht, Entwürfe von Statistiksatzungen (dem Statistischen Landesamt und) mir einzureichen, eingehalten wird, entzieht sich meiner Kenntnis; nicht selten versuchen es kleinere Kommunen, wie ich dann aus Eingaben erfahre, mit statistischen Erhebungen ohne Satzung und womöglich sogar ohne kommunale Statistikstelle (§ 9 SächsStatG).

5.8 Archivwesen

5.8.1 Noch einmal: Wahrung der Befugnisse der staatlichen Archivverwaltung bei der vorweggenommenen generalisierenden Entscheidung über die Archivwürdigkeit der ihr anzubietenden Unterlagen

In 12/5.8.1 habe ich in Abschnitt (1) im letzten Absatz sowie in Abschnitt (3) dargelegt, dass die durch Verwaltungsvorschriften über die Anbietung und Aussonderung von Unterlagen stattfindende *vorweggenommene Pauschal-Entscheidung der Archiverwaltung* darüber, welche personenbezogenen Daten nach Archivrecht gespeichert und welche (nach Sächsischem Datenschutzgesetz oder bereichsspezifischen Regeln) gelöscht werden, die *zuständige Archivbehörde* zu treffen hat. Zuständige Archivbehörde ist gemäß § 3 Abs. 1 SächsArchivG das *Sächsische Staatsarchiv*. Im Unterschied zu den beiden von mir im 12. Tätigkeitsbericht beurteilten Verwaltungsvorschriften sollte in dem mir diesmal gemäß § 26 SächsDSG vorgelegten Entwurf einer „Gemeinsamen Verwaltungsvorschrift der Sächsischen Staatskanzlei und der Sächsischen Staatsministerien zur Anbietung und Aussonderung von Personalakten - VwVAusPersAkten, an der geplanten *gemeinsamen Verwaltungsvorschrift* auch das SMI und damit die oberste Aufsichtsbehörde für das

staatliche Archivwesen des Freistaates Sachsen (§ 3 Abs. 2 SächsArchivG) beteiligt sein. Dies ändert jedoch nichts daran, dass als handelnde Behörde auf Seiten der Archivverwaltung mit dem SMI eine sachlich - genauer gesagt: instanziell - unzuständige Behörde als in der Sache über die Verarbeitung personenbezogener Daten entscheidende Behörde aufträte, falls der Entwurf in Kraft gesetzt würde. Es gehört nach herrschender, insbesondere vom Bundesverwaltungsgericht (Entscheidung vom 9. März 2005 - 6 C 3/04, NJW 2005, 2330, DVBl. 2005, 1324 und DöV 2005, 873) bekräftigter Meinung zu den Rechtmäßigkeitsvoraussetzungen insbesondere auch eines Eingriffes in das Grundrecht auf informationelle Selbstbestimmung, dass dieser durch die instanziell zuständige (vom Gericht wie vielfach üblich als Teil der *sachlichen* Zuständigkeit angesehen, vgl. Kopp/Ramsauer Rdnr. 5a zu § 3 VwVfG) Behörde vorgenommen wird. Das Gericht hat insbesondere bekräftigt, dass eine Aufsichtsbehörde zwar auf die zu treffende Entscheidung Einfluss nehmen, ohne konkretes Vorliegen der Voraussetzungen eines ihr rechtlich eingeräumten Selbsteintrittsrechtes jedoch nicht anstelle der ihrer Aufsicht unterstehenden Behörde tätig werden darf (unter II.2 der Gründe). Das Vorliegen der Voraussetzungen eines Selbsteintrittsrechtes des SMI als oberster Aufsichtsbehörde für das staatliche Archivwesen des Freistaates Sachsen vermag ich vorliegend nicht zu erkennen, solche Voraussetzungen sind (unverändert gegenüber dem von mir seinerzeit im 12. Tätigkeitsbericht dargestellten Vorgang) auch nicht dargetan.

An diesem Ergebnis ändert sich auch nicht etwa dadurch etwas, dass nach dem Entwurf bei der Erhebung der personenbezogenen Daten, die der Archivverwaltung zu übergeben sind, sowie bei der im Akt der Übergabe enthaltenen Übermittlung der betreffenden Daten durch die abgebende Behörde auf Archivverwaltungsseite jeweils das Sächsische Staatsarchiv und damit die zuständige Stelle beteiligt sein soll. Denn eine solche in concreto rechtmäßig durchgeführte tatsächliche Verarbeitung ändert nichts daran, dass die Entscheidung über die Übermittlung (zumindest im Falle zwingend vorgesehener Übergabe an das Sächsische Staatsarchiv), die Entscheidung über die für manche Fallgruppen vorgesehene durch bloße Übersendung des *Anbietungsverzeichnisses* stattfindende Datenübermittlung, aber auch die Entscheidung über die Nicht-Anbietung (der in der Verwaltungsvorschrift nicht zur Übergabe oder Anbietung vorgesehenen Unterlagen) als Vorentscheidung über die Löschung der betreffenden personenbezogenen Daten (vorbehaltlich des § 5 Abs. 5 Satz 2 SächsArchivG, auf den der Entwurf der Verwaltungsvorschrift ausdrücklich hinwies), nicht vom Sächsischen Staatsarchiv als der zuständigen Behörde, sondern - bestenfalls (siehe dazu nachstehend) - vom SMI als trotz seiner Eigenschaft als oberster Aufsichtsbehörde für das staatliche Archivwesen unzuständiger Behörde durch (Beteiligung an der) Inkraftsetzung der Verwaltungsvorschrift getroffen würde.

Hinzu kam, dass, wie auch seinerzeit, nicht in der gebotenen Weise sichergestellt wäre, dass die zuständige Archivbehörde (oder überhaupt eine Archivbehörde, also insbesondere auch das SMI) in der ihre ihm im Gesetz übertragene alleinige Entscheidungskompetenz sichernden Weise befugt sein würde, *einseitig* die Verwaltungsvorschrift außer Kraft zu setzen, wenn es ihrer Auffassung nach die korrekte Anwendung der nach dem Sächsischen Archivgesetz für die Entscheidung nach § 5 Abs. 4 Satz 1 anzuwendenden Maßstäbe verlangt.

Die im Entwurf vorgesehenen Öffnungsklauseln, die dem Sächsischem Staatsarchiv als der zuständigen Behörde Modifikationsmöglichkeiten einräumten, würden an dieser grundsätzlichen, zu weit gehenden Bindung nur recht wenig ändern, weil sie richtig verstanden nur sehr geringe Befugnisse zur Erweiterung der Pflichten zur Übergabe bzw. Anbietung ermöglichten.

Geht man übrigens davon aus, dass es sich bei den dem Sächsischen Staatsarchiv Erweiterungsmöglichkeiten einräumenden Klauseln um eine Art Ermächtigung handelt, so wird man wohl in diesen beiden Klauseln dem Sächsischen Staatsarchiv die Befugnis verliehen sehen müssen, durch Bekanntmachung im Sächsischen Amtsblatt die Verwaltungsvorschrift (der Staatskanzlei und der Staatsministerien!) durch einseitige Bekanntmachung zu modifizieren - aber eben in engen Grenzen!

Die aufgewiesenen rechtlichen Probleme dürften sich alle lösen lassen, wenn auch vielleicht nur außerhalb ausgetretener juristischer Pfade.

5.9 Polizei

5.9.1 Mitteilungen über tatverdächtige Polizisten in „WE-Meldungen“

Der Datenschutzbeauftragte einer Polizeidirektion wies mich darauf hin, dass in den polizeiintern verbreiteten „WE-(Wichtige Ereignis)-Meldungen“ tatverdächtige Polizisten unter vollständiger Angabe der Personalien und ihrer Dienststelle gemeldet würden. Sie würden damit in der gesamten sächsischen Polizei unter Umgehung der Unschuldsvermutung bloßgestellt, ohne dass dies in jedem Einzelfall zur Aufgabenerfüllung erforderlich sei. Als Beispiel führte er eine WE-Meldung an, in der ein Polizist des Ladendiebstahls bezichtigt wurde - zu Unrecht, wie sich später herausstellte.

Ich habe wie folgt Stellung genommen: Personenbezogene Daten dürfen auch in WE-Meldungen nur verarbeitet werden, soweit dies zur Aufgabenerfüllung erforderlich, d. h. zwingend notwendig, ist. Bei der Bewertung, ob die Übermittlung des vollständigen Namens und Vornamens eines tatverdächtigen Polizeibeamten in den WE-

Meldungen zur polizeilichen Aufgabenerfüllung erforderlich ist, darf das Schutzgebot des Dienstherrn gegenüber seinen Beamten nach § 99 SächsBG nicht außer Acht gelassen werden. Diese Vorschrift ist in der verfassungsgerichtlichen Rechtsprechung dahingehend konkretisiert worden, dass der Dienstherr den Beamten vor Schäden an dessen Rechtsgütern zu bewahren hat, soweit die Risiken für diese Rechtsgüter mit der Stellung als Amtsträger in Zusammenhang stehen. Zu den zu schützenden Rechtsgütern zählen namentlich auch die Ehre des Bediensteten und sein Recht, seinen Dienst unbeeinträchtigt verrichten zu können. Hieraus folgt m. E., dass Name und Vorname eines tatverdächtigen Beamten nur auf Anfrage einer Polizeidienststelle bei dem Urheber der WE-Meldung übermittelt werden dürfen. Diese Beschränkung erlaubt einerseits, im konkreten Fall doch vollständig informiert zu werden, und verhindert andererseits, dass der betroffene Beamte regelmäßig und ohne dass dies für die Mehrzahl der mitlesenden Kollegen zur Aufgabenerfüllung erforderlich wäre, unter Umgehung der Unschuldsvermutung bloßgestellt wird. Dies dient auch der Gewährleistung eines geordneten Dienstbetriebes.

Damit die für nähere Informationen in Betracht kommende Dienststelle erfährt, ob es notwendig ist, die Personalien des konkreten Beamten zu erfahren, ist es aber sachgerecht, zumindest die Dienststelle des betreffenden Beamten in der WE-Mitteilung zu erwähnen.

Wie mir der anfragende behördliche Datenschutzbeauftragte mitteilte, fand meine Anregung Gehör.

5.10 Verfassungsschutz

5.10.1 Verfassungswidrige Beobachtungstätigkeit des Landesamtes für Verfassungsschutz

Den im Berichtszeitraum schwerwiegendsten Verstoß gegen den Datenschutz hat das Landesamt für Verfassungsschutz Sachsen (LfV) begangen. Es ließ ein auf seine Tätigkeit bezogenes Urteil des Verfassungsgerichtshofes des Freistaates Sachsen vom 21. Juli 2005 unbeachtet und beobachtete ca. 1½ Jahre lang angebliche Angehörige der Organisierten Kriminalität (OK) praktisch unverändert weiter. Dabei sind die Rechte vieler unbescholtener Personen verletzt worden. Das LfV wurde hieran durch seine Aufsichtsbehörde, das SMI, nicht gehindert. Auch es selbst war bisher nicht in der Lage, seine verfassungswidrige Tätigkeit zu erkennen. Das alles darf in einem freiheitlichen demokratischen Rechtsstaat nicht passieren. Ich kenne bundesweit keinen auch nur annähernd ähnlichen Vorgang.

Mit Urteil vom 21. Juli 2005 hatte der Verfassungsgerichtshof in einem Normenkontrollverfahren (Vf. 67-II-04, abrufbar unter www.justiz.sachsen.de/esaver/internet/2004_067_II/ 2004_067_II.pdf) mehrere Vorschriften des Sächsischen Verfassungsschutzgesetzes als mit der Verfassung des Freistaates Sachsen nur in verfassungskonformer Auslegung vereinbar erkannt. Hinsichtlich der dem LfV seit dem 9. September 2003 übertragenen Befugnisse zur Beobachtung der Organisierten Kriminalität erkannte der Verfassungsgerichtshof, dass das LfV wegen der besonderen Ausprägung des Trennungsgebotes in Art. 83 Abs. 1 SächsVerf („Der Freistaat unterhält keinen Geheimdienst mit polizeilichen Befugnissen“) die sog. Organisierte Kriminalität nur beobachten darf, wenn mit der Beobachtung zugleich herkömmliche Ziele und Aufgaben des Verfassungsschutzes (z. B. Beobachtung des Links- oder Rechtsextremismus etc.) verfolgt werden. Sowohl die einschlägige Zuständigkeitsnorm (§ 1 Abs. 2 Nr. 2 SächsVSG) als auch die einschlägige Aufgabennorm (§ 2 Abs. 1 Nr. 5 SächsVSG) müssten, so der Verfassungsgerichtshof, *verfassungskonform* dahingehend *ausgelegt* werden, dass

> „die Zuständigkeit für die Zusammenarbeit des Landesamtes für Verfassungsschutz mit anderen Ländern und dem Bund in Angelegenheiten der Sammlung und Auswertung von Informationen über Bestrebungen und Tätigkeiten Organisierter Kriminalität nur besteht“ bzw. die Aufgabe der OK-Beobachtung nur dann verfassungskonform sei, wenn „die Wahrnehmung der Aufgabe zugleich zu dienen bestimmt ist“
>
> a) zum bzw. dem Schutz vor Bestrebungen oder Tätigkeiten, die sich gegen die freiheitliche demokratische Grundordnung oder den Bestand oder die Sicherheit des Bundes oder der Länder richten oder
>
> b) zum bzw. dem Schutz vor Bestrebungen im Geltungsbereich des Grundgesetzes, die durch Anwendung von Gewalt oder darauf gerichtete Vorbereitungshandlungen auswärtige Belange der Bundesrepublik Deutschland gefährden.“ Urteil I. 1. und 2. (S. 2).

Zur Begründung führte der Verfassungsgerichtshof u. a. wörtlich aus:

> „Art. 83 Abs. 3 Satz 1 SächsVerf hindert den Gesetzgeber des Freistaates Sachsen, die Beobachtung von Bestrebungen und Tätigkeiten Organisierter Kriminalität durch das Landesamt für Verfassungsschutz in den Fällen vorzusehen, in denen die Tätigkeit des Landesamtes nicht gleichzeitig dem Schutz der freiheitlichen demokratischen Grundordnung oder des Bestandes oder der Sicherheit des Bundes oder der Länder oder vor Bestrebungen im Geltungsbereich des Grundgesetzes,

> die durch Anwendung von Gewalt oder darauf gerichtete Vorbereitungshandlungen auswärtige Belange der Bundesrepublik Deutschland gefährden, dienen soll.“ Urteil C. I. 2. (S. 17).
>
> „Aus diesen Erwägungen folgt, dass das Landesamt für Verfassungsschutz nach Art. 83 Abs. 3 Satz 1 SächsVerf auf seine klassischen Aufgaben, die letztlich auf den Verfassungsschutzbegriff des Bundes in Art. 73 Nr. 10 Buchst. b und c GG zurückgehen, und auf seine herkömmlichen Tätigkeiten, die in Art. 87 Abs. 1 GG für die Verfassungsschutzbehörden des Bundes zum Ausdruck kommen, beschränkt ist.“ Urteil C. I. 2. Buchstabe a Doppelbuchstabe ee (S. 19).

Dies waren klare und unmissverständliche Äußerungen. Mit ihnen wurde zudem im Hinblick auf das Trennungsgebot nur das wiederholt, was der Gerichtshof bereits in seinem „Ersten Polizeigesetz-Urteil“ vom 14. Mai 1996 (44-II-94) gesagt hatte. Ich hatte daher Anlass zur Nachfrage, als ich Ende März 2006 aus der Lokalpresse erfuhr, dass das LfV

> „seit zwei Jahren ‘weit im Vorfeld polizeilicher Ermittlungen’ Hinweise auf organisierte verbrecherische Machenschaften (beobachtet). Sechs Fall-Komplexe würden derzeit bearbeitet, heißt es. Sie beträfen sowohl osteuropäische als auch deutsche OK in Sachsen (…).“

Im 2. Quartal 2006 kontrollierte ich das LfV deshalb zunächst schriftlich, sodann in fünf Kontrollbesuchen an Ort und Stelle hinsichtlich der durch das dortige Referat „Organisierte Kriminalität“ erhobenen und gespeicherten personenbezogenen Daten. Meine Kontrolle ergab schwerwiegende Verstöße des LfV gegen die Rechtsordnung, namentlich die nach dem 21. Juli 2005 nahezu unverändert fortgesetzte Beobachtung der angeblichen OK-Szene und die entsprechende Zusammenarbeit mit anderen Ländern und dem Bund, für die nach dem gesetzeskräftigen (§ 14 Abs. 2 SächsVerfGHG) Urteil vom 21. Juli 2005 die gesetzliche Grundlage nicht mehr im erforderlichen Umfang vorhanden war. Ich stellte fest, dass in zumindest vier der fünf kontrollierten OK-Aktenkomplexe der nach dem Urteil notwendige Bezug zu den klassischen Aufgaben und herkömmlichen Tätigkeiten des Verfassungsschutzes nicht im erforderlichen Ausmaß vorhanden war. Die Aktivitäten der beobachteten angeblichen OK-Szene verstießen in einigen, durchaus nicht allen Fällen zwar gegen Strafgesetze. Die Bezüge zu herkömmlichen Zielen des Verfassungsschutzes im Sinne des Urteils waren jedoch äußerst schwach, randständig und unausgeprägt. Eine Gefährdung der freiheitlichen demokratischen Grundordnung oder eines sonstigen, in dem o. g. Urteil genannten Schutzgutes war objektiv nicht erkennbar. Ein unbe-

fangener Fachmann hätte die Akten der Strafverfolgung, d. h. der Polizei und Staatsanwaltschaft, und nicht dem Verfassungsschutz zugeordnet. Zielrichtung und Vorgehensweise waren mit den Aufgaben des Verfassungsschutzes zumeist und überwiegend nicht zu vereinbaren. Im Hinblick auf die Zeit nach dem 21. Juli 2005 konnte ich keine wesentliche Änderung oder gar Einstellung der Beobachtungs- und Zusammenarbeitsaktivitäten des LfV feststellen, die durch das Urteil des Verfassungsgerichtshofes begründet gewesen wäre. Ich erhielt insgesamt den Eindruck, dass die Tätigkeit des LfV im Hinblick auf die angebliche OK-Szene auf einer Anpassung der Bewertung des Urteils an die Praxis des LfV beruhte. Richtig wäre das Gegenteil gewesen, nämlich die umgehende Anpassung der Praxis des LfV an das Urteil.

Durch diesen Verstoß gegen den Grundsatz der Gesetzmäßigkeit der Verwaltung (Art. 20 Abs. 3 GG; Art. 3 Abs. 3 SächsVerf) war das Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG; Art. 33 SächsVerf) einer Vielzahl von Betroffenen, beileibe nicht nur Angehörigen der angeblichen OK-Szene oder Personen, die das LfV für solche hielt, sondern nicht selten auch völlig Unbeteiligten, schwer verletzt worden. Über die Art und Weise der „Beobachtung“ und die schweren, mitunter sachlich nicht nachvollziehbaren Eingriffe in die Persönlichkeitsrechte der Betroffenen möchte ich mich hier nicht auslassen. Mit Schreiben vom 2. Oktober 2006 beanstandete ich deshalb förmlich das SMI als oberste Verfassungsschutzbehörde nach § 29 Abs. 1 SächsDSG. Mit Schreiben vom 4. Oktober 2006 unterrichtete ich außerdem den Sächsischen Landtag nach § 30 Abs. 2 SächsDSG durch eine gekürzte Fassung meiner Beanstandung über den schwerwiegenden Verstoß des LfV gegen die Rechtsordnung (LT-DS 4/6639, unter www.landtag.sachsen.de/slt_online/de/infothek/index.asp?page=dokumente/index.aspx). Der Staatsminister des Innern nahm meine Beanstandung zum Anlass, die Parlamentarische Kontrollkommission des Sächsischen Landtages (PKK) um Befassung mit der Angelegenheit zu bitten. Seitdem befasst sich dieses Gremium aus zwei CDU-, einem SPD- und zwei PDS-Abgeordneten ebenfalls mit der Frage der Rechtmäßigkeit der Beobachtung der angeblichen OK-Szene. Zu einigen der Sitzungen der PKK wurde ich hinzugezogen. Dies dauerte bis zum Ende des Berichtszeitraums an.

Noch während meiner Kontrolle hatte der Sächsische Landtag zudem am 28. April 2006 ein Gesetzgebungsverfahren (GVBl. S. 129 ff.) abgeschlossen, durch das die erst seit dem 9. September 2003 bestanden habenden Befugnisse des LfV zur Beobachtung der OK wieder vollständig gestrichen bzw. aufgehoben worden waren. Dieses Gesetz war am 28. Mai 2006 in Kraft getreten.

Meiner Beanstandung wurde seitens SMI und LfV heftig widersprochen. Sowohl vor als auch nach meiner Beanstandung fand ich eine merkwürdig verhärtete Verteidigung der juristisch unhaltbaren Argumentation des LfV vor. Diese Argumentation lautete sinngemäß: Zwar seien in der Tat keine „Bestrebungen“ erkenntlich, da die beobachteten OK-Kreise nicht politisch motiviert seien. Jedoch dürfte die OK-Szene beobachtet werden, da sich die darin begangenen Straftaten als „Tätigkeiten“ gegen die freiheitliche demokratische Grundordnung richteten. Die begangenen Straftaten seien namentlich Verstöße gegen „die im Grundgesetz konkretisierten Menschenrechte“, einem Merkmal der freiheitlichen demokratischen Grundordnung in § 3 Abs. 2 Nr. 7 SächsVSG. Da dies so sei, seien die Voraussetzungen des Urteils vom 21. Juli 2005 erfüllt und das LfV zur Beobachtung der Szene befugt gewesen. Mit anderen Worten: Eine Straftat - etwa eine Körperverletzung zwischen zwei Angehörigen der beobachteten OK-Szene - verletze die körperliche Unversehrtheit, die als Grundrecht im Grundgesetz konkretisiert sei. Daher richte sie sich gegen die freiheitliche demokratische Grundordnung und deshalb dürfe der Verfassungsschutz die Täter beobachten.

Diese Argumentation wurde vom LfV bis hinauf in die Fachebene des SMI vertreten. Lediglich einer der beteiligten hohen Beamten hatte in einer ersten „Schrecksekunde“ die Konsequenzen des Urteils ernsthaft erwogen, sich dann jedoch der aus dem LfV stammenden o. g. Auffassung ebenfalls angeschlossen. Über diesen Mangel an kritischem Juristenverstand bin ich noch heute irritiert.

Andererseits rief die Argumentation bei unabhängigen, nicht dem LfV oder den einschlägigen Aufsichtsstrukturen des SMI verhafteten Juristen in Rechtsprechung und Verwaltung Unverständnis und Kopfschütteln hervor. Denn selbstverständlich handelt es sich bei den „im Grundgesetz konkretisierten Menschenrechten“ um Grundrechte, d. h. um Abwehrrechte der Betroffenen gegen die öffentliche Gewalt. Verletzt ein Grundrechtsträger einen anderen Grundrechtsträger am Körper, so hat die öffentliche Gewalt für eine ordentliche Strafverfolgung und zukünftige Prävention zu sorgen. Sie kommt damit ihrer aus der freiheitlichen demokratischen Grundordnung folgenden Pflicht zur Gewährleistung des Rechtsstaates nach. Keinesfalls aber wird mit einer Körperverletzung unter Grundrechtsträgern die freiheitliche demokratische Grundordnung gefährdet. Auch müsste die Ablehnung der „im Grundgesetz konkretisierten Menschenrechte“ Ausdruck einer grundsätzlich auf die Ersetzung oder wesentliche Modifizierung der freiheitlichen demokratischen Grundordnung gerichteten Tätigkeit sein. Die Gesetzgeber der Verfassungsschutzgesetze wollten mit dieser Formulierung diejenigen zum Beobachtungsobjekt machen, die den Katalog an Menschenrechten eines modernen, westlich-parlamentarischen

Staates prinzipiell ablehnen, etwa da sie diesen Katalog für bestimmte Menschen oder Menschengruppen nicht gelten lassen wollen. Dies und nichts anderes ist der Sinn von § 3 Abs. 2 Nr. 7 SächsVSG. Verhaltensweisen, die lediglich dem entsprechen, was der Gesetzgeber in § 3 Abs. 3 SächsVSG als „Organisierte Kriminalität" beschrieben hatte, konnten nach dem Urteil alleine nicht mehr die Beobachtung durch das LfV rechtfertigen.

Das Urteil machte indes deutlich, dass die Aufgabe der Beobachtung nicht mehr bestand, wenn sich die Gefährdung der freiheitlichen demokratischen Grundordnung alleine durch eine OK-Verhaltensweise ergab. Nach dem Urteil musste in jedem Fall ein über die kriminelle Verhaltensweise hinausgehendes „Mehr" hinzutreten, um zu „Tätigkeiten" der OK zu gelangen, die die freiheitliche demokratische Grundordnung gefährden. „Reine" OK-Verhaltensweisen, etwa die Anwendung von Gewalt, § 3 Abs. 3 Nr. 2 SächsVSG, oder die Einflussnahme auf die Justiz, § 3 Abs. 3 Nr. 3 SächsVSG, waren ohne dieses „Mehr" nach dem Urteil nicht mehr geeignet, eine im Sinne des Verfassungsschutzes relevante Gefahr für die freiheitliche demokratische Grundordnung zu begründen.

Zur Rechtfertigung der Beobachtung der angeblichen OK-Szene führte das LfV des Weiteren aus, dass die Polizei aufgrund des Legalitätsprinzips diese Beobachtung nicht leisten dürfe bzw. könne. Gemeinsam sei die Vorfeldaufklärung im Bereich der OK abgedeckt. Verdichteten sich vage Hinweise zu strafverfolgungsrelevanten Informationen, könne die Bearbeitung an die Polizei abgegeben werden. Genau dieses „Zusammenwirken" aber widersprach der bereits im o. g. ersten Polizeigesetzurteil 1996 sowie im Urteil vom 21. Juli 2005 erkannten strengen Auslegung von Art. 83 Abs. 3 SächsVerf. Erstaunlich ist dabei, dass dem LfV die Existenz des Trennungsgebots durchaus bewusst war, da es darauf hinwies, dass eine Befugniserweiterung der Polizei bzgl. des Einsatzes nachrichtendienstlicher Mittel eben dem Trennungsgebot widerspräche. Die vorgenannten Einschätzungen des LfV blieben durch das SMI unwidersprochen.

Das LfV wehrte sich jedoch nicht nur mit Argumenten gegen meine Kontrolle. Im Zusammenhang mit meiner Kontrolle - nachdem das für die Arbeit des LfV negative Ergebnis im Hause bekannt war - wurde ein mich betreffender so genannter „Sicherheitsvermerk" gefertigt, mit dem Ziel, diese Kontrolltätigkeit zu diskreditieren. Die Amtsleitung bewertete ihn jedoch als gegenstandslos. Trotzdem wurde der Inhalt dieses Vermerkes später an die Öffentlichkeit lanciert. Dieses Vorgehen ist ein Skandal im Skandal. Von einer konsequenten Kontrolle des Verfassungsschutzes werde ich mich dadurch jedoch nicht abhalten lassen. Im Gegenteil.

Zur Behebung der festgestellten Verstöße forderte ich in meiner Beanstandung, dass die gespeicherten personenbezogenen Daten aus dem OK-Bereich nach dem Abschluss der laufenden Kontrolle durch die PKK unabhängig von ihrem Speicherungsort und der Speicherungsart, nachdem sie zunächst dem zuständigen Archiv angeboten wurden und dieses die Archivwürdigkeit verneint hat oder über sie nicht fristgemäß entschieden hat, zu löschen waren, da ihre Speicherung unzulässig war, § 7 Abs. 5 SächsVSG i. V. m. § 5 Abs. 1 SächsArchivG, § 7 Abs. 2 Satz 1 SächsVSG. Außerdem forderte ich, dass die Daten bis zu ihrer Löschung für die Erfüllung der Aufgaben des LfV nicht mehr verwendet werden durften. Ferner forderte ich, dass das LfV seine Bediensteten künftig regelmäßig sowie bei gegebenem Anlass über die Rechtsfolgen von Entscheidungen des Verfassungsgerichtshofes des Freistaates Sachsen zu belehren und das SMI seine Rechtsaufsicht über das LfV zu verstärken hatte, um Wiederholungen sicher auszuschließen.

Hinsichtlich dieser Forderungen behielt ich mir eine weitere Kontrolle nach Ablauf eines angemessenen Zeitraums vor.

Aufgrund der in dieser Sache gemachten Erfahrungen werde ich künftig Vorgängen, die sich auf das LfV beziehen, besondere Aufmerksamkeit widmen.

Für ein Fazit der Angelegenheit ist es noch zu früh, zumal wesentliche Abschnitte der öffentlichen und politischen Auseinandersetzung jenseits des Berichtszeitraums liegen. Was bleibt, ist die Tatsache, dass sich Teile der Exekutive mit einer Mischung aus Fahrlässigkeit und zielgerichtetem Vorsatz über eine bindende Entscheidung der dritten Gewalt hinweg gesetzt haben und wenig Reue an den Tag legten.

5.10.2 Informationelles Bloßstellen eines Betroffenen in der Antwort der Staatsregierung auf eine Kleine Anfrage

Im Rahmen der Beantwortung einer Kleinen Anfrage eines Abgeordneten erkundigte sich die Staatsregierung hinter dem Rücken des Betroffenen bei einem seiner privaten Auftraggeber, einer politischen Stiftung, über seine geschäftlichen Aktivitäten. Ich habe diesen Verstoß gegen § 12 Abs. 1, 4, 2 Satz 1 SächsDSG (Datenerhebung) beanstandet.

Was war passiert? Mit einer Kleinen Anfrage an die Staatsregierung hatte ein Abgeordneter der Fraktion X des Sächsischen Landtages insgesamt vier Fragen zu einer namentlich genannten Person, ihrem Verhältnis zur Partei Y und der „der Y nahe stehenden Stiftung“ gestellt und den Betroffenen als „Mann mit engen Kontakten zum Geheimdienst“ beschrieben. Unter anderem fragte der Abgeordnete, ob

der Betroffene für die Staatsregierung, die Partei Y oder die (…) Stiftung „Beiträge verfasst bzw. Veranstaltungen durchgeführt“ habe und, wenn ja, „an welchen von öffentlichen Geldern direkt oder indirekt finanzierten bzw. teilfinanzierten Publikationsorganen“ er seit 1990 mitgewirkt habe „und welche Lehraufträge er gegebenenfalls ausgeführt“ habe. Die Staatsregierung beantwortete die Fragen zusammenfassend wie folgt:

> „Nach Auskunft der Stiftung (…) hat diese mit [Vorname und Name des Betroffenen] verschiedene Veranstaltungen durchgeführt. Nachfolgend sind die zumindest teilweise mit öffentlichen Geldern des Freistaates Sachsen direkt oder indirekt finanzierten Veranstaltungen aufgelistet, an denen [Name des Betroffenen] seit 1999 mitwirkte.“

Auf meine schriftliche Anfrage bestätigte das SMI nach einigem Hin und Her schließlich, dass „ein beteiligtes Ressort“ „die Kleine Anfrage an die (…) Stiftung e. V. mit der Bitte um Beantwortung (…) weitergeleitet“ habe. Die Stiftung habe wie „(…) erkennbar geantwortet“. Das andere Ressort habe die erforderliche Abwägung zwischen datenschutzrechtlichen Belangen und dem Informationsrecht des Abgeordneten vorgenommen. Die Erhebung und Nutzung der Daten sei ferner zulässig gewesen, da diese Daten im Rahmen der Verwendungsnachweisprüfung vom Empfänger der institutionellen Förderung mitzuteilen seien.

Das war leider eine Fehleinschätzung. Denn die Staatsregierung hätte bei der Stiftung e. V. gar keine Informationen zum Betroffenen erheben dürfen, da die politische Stiftung als Privater nicht in ihren Verantwortungsbereich fällt. Dies ergibt sich aus Folgendem:

(a) Öffentliche Stellen dürfen sich personenbezogene Daten nur beschaffen, wenn ihre Kenntnis zur Erfüllung ihrer Aufgaben erforderlich ist, § 12 Abs. 1 SächsDSG. „Aufgabe“ der Staatsregierung bei der Beantwortung Kleiner Anfragen ist es nach Art. 51 Abs. 1 SächsVerf, die Fragen einzelner Abgeordneter „nach bestem Wissen unverzüglich und vollständig zu beantworten“. Die Verpflichtung der Staatsregierung soll den Abgeordneten „die zur Ausübung ihres Mandats erforderliche Information verschaffen“ (BVerfGE 13, 123, 125; 57, 1, 5; 67, 100, 129; 92, 136). Das derart begründete Informationsinteresse besteht jedoch nicht unbegrenzt (s. BVerfGE 70, 355: „grundsätzlich“). Anfragen sind nur zulässig, soweit sie sich auf Bereiche beziehen, für die die Regierung unmittelbar oder mittelbar verantwortlich ist (vgl. Beschluss des 13. Bundestages vom 1. Oktober 1997 i. V. m. BT-Drs. 13/6149, S. 3). Bei der Beantwortung hat die Staatsregierung nach Art. 51 Abs. 2 SächsVerf des

Weiteren eventuell entgegenstehende „Rechte Dritter“ zu respektieren; als „Recht Dritter“ kamen hier insbesondere das allgemeine Persönlichkeitsrecht (in seiner Ausprägung als Recht auf informationelle Selbstbestimmung, Art. 33 SächsVerf) sowie ggf. Betriebs- und Geschäftsgeheimnisse des Betroffenen in Betracht (Hömig in Seifert/Hömig, GG, 7. Aufl. 2003, Art. 43 Rdnr. 2, 3).

Somit war klar, dass Auftragsverhältnisse zwischen der Stiftung, die rechtlich als eingetragener Verein firmiert, und deren Auftragnehmern, hier dem Betroffenen, von vornherein nicht in den Verantwortungsbereich der Staatsregierung fallen können. Demgemäß durfte die Staatsregierung hierüber auch keine Daten erheben, da insoweit ein Informationsinteresse anfragender Abgeordneter nicht bestehen konnte. Ein Informationsinteresse anfragender Abgeordneter hätte wegen der Verwendung öffentlicher Gelder für Zuwendungen an politische Stiftungen allenfalls zu den „im Rahmen der Verwendungsnachweisprüfung“ eventuell bei der Staatsregierung bereits gespeicherten Informationen bestanden.

(b) Ein zweites kam hinzu: Die Erhebung von Daten zur Person des Betroffenen hätte, wenn sie denn zulässig gewesen wäre, beim Betroffenen selbst stattfinden müssen (Grundsatz der Datenerhebung beim Betroffenen, § 12 Abs. 2 Satz 1 SächsDSG). Dies ist spätestens seit der Anerkennung des Rechts auf informationelle Selbstbestimmung durch das Bundesverfassungsgericht im Jahr 1983 geboten: „Unter den Bedingungen der modernen Datenverarbeitung wird der Schutz des Einzelnen gegen unbegrenzte Erhebung … seiner persönlichen Daten von dem allgemeinen Persönlichkeitsrecht des Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG umfasst. Das Grundrecht gewährleistet insofern die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen“ (BVerfGE 65, 1). Demgemäß bestimmt § 12 Abs. 2 Satz 1 SächsDSG, dass personenbezogene Daten, die nicht allgemein zugänglich sind, „beim Betroffenen mit seiner Kenntnis zu erheben“ sind.

Eine Erhebung der Daten beim Betroffenen wäre leicht und einfach möglich gewesen. Es hätte genügt, sich die Telefonnummer des Betroffenen zu verschaffen und diesen unmittelbar unter Mitteilung des Erhebungszwecks, § 12 Abs. 2 Satz 2 SächsDSG, zu befragen. Dadurch hätte der Betroffene auch Kenntnis von der zu seiner Person gestellten Anfrage des Abgeordneten und dem Verwendungszweck erhalten. So jedoch blieb das Verfahren für den Betroffenen völlig intransparent. Er hatte keine Möglichkeit, sich zu äußern und eventuell gegen eine Veröffentlichung sprechende Gründe vorzutragen. Er hat erst aus der veröffentlichten Landtags-Drucksache erfahren, dass die Staatsregierung hinter seinem Rücken Daten über ihn

erhoben hat. Nur ergänzend sei vermerkt, dass die Voraussetzungen, unter denen das Gesetz eine Datenerhebung bei Dritten ausnahmsweise erlaubt, § 12 Abs. 4 Nr. 1 bis 8 SächsDSG, nicht vorgelegen haben.

Ich habe das SMI aufgefordert, die Bediensteten, die parlamentarische Anfragen beantworten, nachweislich über die Rechtslage im Zusammenhang mit Artikel 51 Abs. 1 SächsVerf zu belehren und insbesondere darauf hinzuweisen, dass generell besondere Vorsicht dann angebracht ist, wenn Informationen zu einzelnen Menschen, d. h. personenbezogene (auch personenbeziehbare, § 3 Abs. 1 SächsDSG) Daten, durch Abgeordnete angefragt werden. Das SMI ist dem gefolgt.

5.10.3 Zu Gast bei Freunden oder die Macht des Geldes

„Zu Gast bei Freunden“ lautete das Motto der Fußballweltmeisterschaft 2006 in Deutschland. Einige Freunde, nämlich die deutschen Sicherheitsbehörden, haben zur reibungslosen Gewährleistung dieses Großereignisses der Unterhaltungsindustrie allerdings auch Maßnahmen durchgeführt, bei denen man im privaten Bereich die Freundschaft unverzüglich aufkündigen würde. So mussten sich alle Personen, die beruflich mit der WM zu tun haben wollten, „freiwillig“ einem Akkreditierungsverfahren unterwerfen. In diesem steuerte u. a. das LfV ohne gesetzliche Grundlage lediglich auf der Grundlage „freiwilliger“ Einwilligungen der Betroffenen Erkenntnisse bei. Diese wurden schließlich an den privaten Veranstalter, die FIFA, übermittelt. Mit anderen Worten: U. a. das LfV überprüfte auf der Grundlage nicht genügender „Einwilligungen“ jeden Würstchenverkäufer und trug dazu bei, dass der Chef des Würstchenverkäufers die Ja/Nein-Entscheidung über die Zulassung des Würstchenverkäufers erhielt.

Meine mehrfach und schriftlich vorgetragenen Bedenken, wonach die bestehenden gesetzlichen Regelungen nicht ausreichten und die „Einwilligung“ der Betroffenen nicht freiwillig sein konnte, stießen im SMI auf taube Ohren. Mir schien, dass die dort anzutreffende „Augen zu und durch-Mentalität“ auch dem Umstand geschuldet war, dass die damalige Bundesregierung der FIFA weitgehende - nach deutschem Recht vielleicht zu weitgehende - Sicherheitsversprechen gemacht hatte. Von dieser großen Linie, die die Bundesregierung im Hinblick auf die massiven wirtschaftlichen Interessen der Veranstalter und Verwertungsrechteinhaber eingeschlagen hatte, wollte man sich nicht mehr durch kleinliche verfassungsrechtliche Bedenken etwa zur „Freiwilligkeit“ oder der erforderlichen speziellen gesetzlichen Grundlage für die Mitwirkung des Verfassungsschutzes an den Zuverlässigkeitsüberprüfungen abbringen lassen.

Im Einzelnen:

„Einwilligungen“ begegnen in Arbeitsverhältnissen oder in Bezug auf Arbeitsverhältnisse schweren Bedenken. Wahre „Freiwilligkeit“ gibt es im Bereich von Arbeits- oder Dienstverhältnissen nicht. Alleine die Angst um den Arbeitsplatz, d. h. die wirtschaftliche Existenz, wird abhängig Beschäftigte kaum ihre Einwilligung in ihre Überprüfung durch Polizei und Verfassungsschutz verweigern lassen. Ihre „*Einwilligung*“ in den Abgleich ihrer Daten mit den polizeilichen und nachrichtendienstlichen Dateien und die im Einzelfall erfolgende Speicherung ist tatsächlich eher unfreiwillig und damit zumeist wertlos.

Doch selbst wenn die Einwilligung wirklich freiwillig erteilt worden wäre, wäre die Rechtmäßigkeit des Verfahrens zumindest im Hinblick auf die Mitwirkung des LfV an der insoweit fehlenden gesetzlichen Aufgabenzuweisung gescheitert. Zwischen der Überprüfung durch die Polizei und der durch den Verfassungsschutz bestand ein Unterschied: Während die Polizei durch den Gesetzgeber mit der Aufgabe der Gefahrenabwehr beauftragt worden ist, sind dem Verfassungsschutz in erster Linie die „Sammlung und Auswertung von Informationen“, in zweiter Linie die Mitwirkung an gesetzlich bestimmten Sicherheitsüberprüfungen und weiteren genau bestimmten Überprüfungen als Aufgabe übertragen worden. Nach keinem Verfassungsschutzgesetz in Bund oder Ländern hat der Verfassungsschutz die Aufgabe, an „Zuverlässigkeitsüberprüfungen“ von Arbeitnehmern für Veranstalter von Großereignissen mitzuwirken. Über die insofern erforderliche, jedoch fehlende gesetzliche Aufgabenzuweisung hilft die „Einwilligung“ der Betroffenen eben nicht hinweg. In einem Rechtsstaat darf sich keine Behörde neue Aufgaben auf der Grundlage von Einwilligungen erschließen. Der verfassungsrechtlich verankerte Grundsatz vom Vorbehalt des Gesetzes besagt, dass alle wesentlichen Grundrechtseingriffe durch ein von der Volksvertretung beschlossenes Gesetz geregelt sein müssen. Das Instrument der Einwilligung mag Lücken in bestehenden gesetzlich zugewiesenen Aufgaben schließen helfen; es ist kein Instrument zur Begründung von Aufgaben, die einer Behörde gesetzlich nicht zugewiesen sind. Hinzu kommt: In der verfassungsgerichtlichen Rechtsprechung ist anerkannt, dass eine Aufgabe umso mehr einer speziellen gesetzlichen Grundlage bedarf, je intensiver sie Grundrechte berührt. In unserem Fall waren die Erkenntnisse des LfV zum Zwecke der Akkreditierung letztendlich an einen Privaten übermittelt worden. Das ist - wie § 12 Abs. 3 SächsVSG zeigt - nicht per se ausgeschlossen, aber jedenfalls nur auf gesetzlicher Grundlage und nicht auf Grund von „Einwilligungen“ zulässig. Gerade da hier die Voraussetzungen des § 12 Abs. 3 SächsVSG nicht erfüllt waren, hätten die Übermittlungen nicht auf Grund von Einwilligungen vorgenommen werden dürfen. Dies

gilt in besonderem Maße für so grundrechtlich heikle Behördentätigkeit wie die eines Nachrichtendienstes.

Auch § 12 Abs. 1 SächsVSG schied als Grundlage für die Übermittlung personenbezogener Daten durch das LfV an das BfV und letztlich an die FIFA aus. § 12 Abs. 1 Satz 1 SächsVSG erlaubt die Übermittlung personenbezogener Daten durch das LfV an öffentliche Stellen, „wenn dies zur Erfüllung seiner Aufgaben erforderlich ist oder Empfänger die Daten zum Schutz der freiheitlichen demokratischen Grundordnung oder sonst für Zwecke der öffentlichen Sicherheit benötigen“. Die Aufgaben des LfV sind abschließend in § 2 SächsVSG aufgezählt. Die Mitwirkung des LfV an Überprüfungen von Personen ist in § 2 Abs. 2 SächsVSG abschließend geregelt. Die Mitwirkung im Akkreditierungsverfahren gehört nicht dazu. Die Übermittlungen konnten also nicht zur Aufgabenerfüllung des LfV erforderlich sein, da keine derartige gesetzliche Aufgabe des LfV besteht. Auch benötigte der Empfänger, das BfV, die Daten nicht zum Schutz der freiheitlichen demokratischen Grundordnung, sondern zum Zwecke „der Minimierung von personellen Gefährdungspotenzialen“ bei der Fußball-WM 2006, einer davon wesensverschiedenen polizeilichen Aufgabe. Als einziger Zweck der Übermittlung durch das LfV wäre mithin die „öffentliche Sicherheit“ geblieben. Diese dem Wortlaut nach weite Vorschrift ist jedoch u. a. wegen ihrer Grundrechtsrelevanz eher eng auszulegen. Dafür spricht auch das Zitat der Rechtsprechung des BVerfG durch den Verfassungsgerichtshof des Freistaates Sachsen in seinem Urteil vom 21. Juli 2005 (Vf. 67-II-04) zum Sächsischen Verfassungsschutzgesetz (Urteil C. III. 2 Buchst. a). Danach bedürfen Eingriffe in das Grundrecht auf informationelle Selbstbestimmung u. a. einer gesetzlichen Grundlage,

> „aus der sich die Voraussetzungen und der Umfang der Beschränkungen für Rechtsanwender und Betroffene klar ergeben und die dem Grundsatz der Verhältnismäßigkeit Rechnung trägt.“ (Urteil a. a. O.)

Hinzu kommt ein systematisches Argument für eine enge Auslegung: Der Begriff der öffentlichen Sicherheit steht in Satz 1 der Vorschrift in alternativer Beziehung zur freiheitlichen demokratischen Grundordnung und damit qualitativ auf einer Stufe mit ihr. Der Begriff ist nicht der Generalklausel des Polizeigesetzes gleichzusetzen. Die öffentliche Sicherheit müsste daher konkret und erheblich gefährdet, hochwertige Rechtsgüter müssten konkret bedroht sein, um eine Datenverarbeitung durch das LfV auf dieser Rechtsgrundlage zu diesem Zweck zu rechtfertigen. Dies war nicht der Fall. Im Rahmen des Akkreditierungsverfahrens erfolgte die Übermittlung personenbezogener Daten nicht aufgrund einer konkreten Gefährdungslage. Weder war die

freiheitliche demokratische Grundordnung konkret gefährdet, noch waren konkrete Gefahren für die öffentliche Sicherheit erkennbar. Der vom SMI dargestellte Zweck der „Minimierung von personellen Gefährdungspotentialen“ war nicht geeignet, eine Übermittlung zu legitimieren. Zu berücksichtigen war ferner, dass die Polizei - hier das Bundeskriminalamt als „single point of contact“ und Informationen bündelnde und an das Organisationskomitee weiterleitende Stelle - personenbezogene Daten erlangt, die es ansonsten von den mitwirkenden Verfassungsschutzbehörden nicht erhalten hätte. Damit kommt auch wieder der spezifisch sächsischen Ausprägung des Trennungsgebotes zwischen Polizei und Nachrichtendienst in Art. 83 Abs. 3 SächsVerf und der dazu ergangenen Rechtsprechung des Verfassungsgerichtshofes des Freistaates Sachsen Bedeutung zu. Das Argument des SMI, dass alle übrigen Landesämter an diesem Akkreditierungsverfahren mitwirkten, wird so relativiert.

Aufmerksamkeit verdienten auch die sonstigen Sicherheitsmaßnahmen im Zusammenhang mit diesem Milliardengeschäft der Unterhaltungsindustrie. Ein auf einen Beschluss der Innenministerkonferenz zurückgehender Erlass des Landes Sachsen-Anhalt sah etwa vor, dass die Genehmigung zur Errichtung von sog. Public-Viewing-Bereichen, also öffentlichen Großbildschirmen, nur erteilt werden solle, wenn sich die Veranstalter verpflichteten, im Rahmen des privaten Hausrechts eine Videoüberwachung vorzunehmen, auf die die Polizei unmittelbar zugreifen durfte. Dies wäre mit den gesetzlichen Voraussetzungen zur Videoüberwachung durch die Polizei nicht erreichbar gewesen. So wurden die Befugnisse, die der Gesetzgeber der Polizei zur Einschränkung von Freiheitsrechten zugestanden hat, systematisch und unter Umgehung des Gesetzgebers durch polizeiliches „Outsourcing“ umgangen. Es ist Aufgabe des Gesetzgebers, seinen Gesetzen Geltung zu verschaffen und derartige Umgehungen zu unterbinden.

Die Polizeiabteilung des SMI hat mittlerweile einen ersten Entwurf einer gesetzlichen Regelung der Zuverlässigkeitsüberprüfungen durch die Polizei vorgelegt.

Ich wäre dankbar, wenn ich vom Verfassungsschutz Ähnliches erfahren dürfte.

5.11 Landessystemkonzept/Landesnetz

In diesem Jahr nicht belegt.

5.12 Ausländerwesen

5.12.1 Mitteilung der Heiratsabsicht und Ersuchen um Übersendung der vollständigen Ausländerakte durch Standesämter bei Eheschließungen

Ein durch mich kontrolliertes Standesamt nahm die Vorlage des Ehefähigkeitszeugnisses durch ausländische Staatsangehörige zum Anlass, in jedem Fall die vollständige Ausländerakte des Betroffenen bei der Ausländerbehörde anzufordern. Die Anforderung wurde mit der Mitteilung an die Ausländerbehörde verbunden, dass der Ausländer beabsichtige, eine Ehe zu schließen.

Das Standesamt hat mir gegenüber dieses Verfahren wie folgt begründet: Der Standesbeamte sei verpflichtet zu prüfen, ob der Eheschließung ein Ehehindernis entgegensteht. Häufig gäben Ausländer in aufenthaltsrechtlichen oder Asylverfahren an, verheiratet zu sein. Der Standesbeamte müsse deshalb die Angaben des Ausländers und den Inhalt des Ehefähigkeitszeugnisses mit dem in der Ausländerakte vermerkten Familienstand vergleichen. Seien die Angaben widersprüchlich, bestünde der Verdacht, dass das Ehefähigkeitszeugnis gefälscht sei. Der Ausländer werde dann aufgefordert, die Widersprüche aufzulösen. Rechtsgrundlage hierfür sei die Prüfpflicht des Standesbeamten nach § 5 Abs. 2 PStG sowie - hinsichtlich der Anforderung der Ausländerakte - die in § 5 Abs. 3 Satz 2 PStG gegebene Befugnis des Standesbeamten, „sich auf andere Weise Gewissheit zu verschaffen“.

Das ist unzutreffend: Weder für das regelmäßige Ersuchen um Übersendung der kompletten Ausländerakte noch für die Mitteilung der Heiratsabsicht an die Ausländerbehörde gibt es eine Rechtsgrundlage.

Das Personenstandsgesetz ist hinsichtlich der Eheschließung vom Beibringungsgrundsatz geprägt. Die Verlobten haben Urkunden vorzulegen; der Standesbeamte darf von den Verlobten weitere Urkunden fordern (vgl. unter anderen § 5 Abs. 2 Satz 2 PStG, § 68a PStG). Auf die Staatsangehörigkeit kommt es insofern nicht an. Eine Erhebung bestimmter, nämlich der erforderlichen, Daten bei Dritten, hier der Ausländerbehörde, wird erst in Betracht kommen können, wenn der Betroffene eingewilligt hat oder tatsächliche Anhaltspunkte für unrichtige Angaben des ausländischen Staatsangehörigen bestehen. Dies ergibt sich aus dem Grundsatz des Vorrangs der Datenerhebung beim Betroffenen (§ 12 Abs. 4 Nr. 2 oder 5 SächsDSG). Die sich aus § 5 Abs. 2 PStG ergebende Prüfpflicht des Standesbeamten vermag die geschilderte Datenerhebung bei Dritten ohne diese Voraussetzungen wegen des Beibringungsgrundsatzes, der Systematik der Vorschrift und der hinsichtlich der Erhe-

bung personenbezogener Daten mangelnden Bestimmtheit der Regelung nicht zu tragen.

Die danach ausnahmsweise zulässige Erhebung von Daten bei Dritten hat sich aus Rechtsgründen auf das Ersuchen um Auskunft, nämlich über den in der Ausländerakte dokumentierten Familienstand des Verlobten, zu beschränken. Dies ergibt sich aus dem Grundsatz der Erforderlichkeit zur Aufgabenerfüllung (§ 12 Abs. 1 SächsDSG). Erforderlich zur Aufgabenerfüllung des Standesbeamten ist nur die Kenntnis über den in der Ausländerakte dokumentierten Familienstand, nicht die Kenntnis auch aller übrigen Angaben in der Ausländerakte.

Hinzu kommt die Pflicht zur Benachrichtigung des Betroffenen nach § 12 Abs. 6 SächsDSG.

Unzulässig ist des Weiteren die Mitteilung des Standesbeamten an die Ausländerbehörde, dass der Ausländer, dessen Akte angefordert wird, beabsichtige zu heiraten. § 87 Abs. 2 AufenthG und § 101 der „Dienstanweisung für die Standesbeamten und ihre Aufsichtsbehörden“ regeln die Übermittlungsbefugnisse des Standesbeamten abschließend. Beide Vorschriften sehen eine Befugnis zur Mitteilung einer Heiratsabsicht an die Ausländerbehörden nicht vor. Dies gilt auch in den Fällen, in denen ausnahmsweise die Erhebung des in der Ausländerakte dokumentierten Familienstandes zulässig wäre (siehe oben).

Auch das Aufenthaltsgesetz enthält keine Rechtsgrundlage für die Übermittlung von personenbezogenen Daten durch Ausländerbehörden an Standesämter zum Zwecke eines Eheschließungsverfahrens. Das Aufenthaltsgesetz als spezielleres Gesetz regelt Übermittlungen an öffentliche Stellen in § 90 abschließend. Allgemeine Regelungen wie § 14 SächsDSG werden dadurch verdrängt und kommen nicht zur Anwendung.

5.12.2 Erhebung personenbezogener Daten im Einbürgerungsverfahren

Die Lebensgefährtin eines ausländischen Staatsangehörigen, der einen Antrag auf Einbürgerung gestellt hatte, wandte sich an mich, weil der Antragsteller von der Einbürgerungsbehörde aufgefordert worden war, ihren Mietvertrag sowie ihre Einkommensnachweise vorzulegen. Der Antragsteller kam dieser Aufforderung nicht nach, so dass es letztlich nicht zur Erhebung der Daten seiner Lebensgefährtin durch die Einbürgerungsbehörde kam.

Ich habe der Einbürgerungsbehörde mitgeteilt, dass es für die beabsichtigte Datenerhebung bezüglich der Lebensgefährtin des Antragstellers keine gesetzliche Grundlage gibt.

Der Antragsteller ist im Einbürgerungsverfahren gemäß § 37 Abs. 1 StAG i. V. m. § 82 AufenthG zur Mitwirkung am Verfahren verpflichtet. Dazu gehört selbstverständlich die Obliegenheit, erforderliche Nachweise über persönliche Verhältnisse sowie sonstige erforderliche Bescheinigungen und Erlaubnisse beizubringen. Auch die Erhebung personenbezogener Daten des Ehegatten ist vom Gesetz gedeckt. Dagegen ist keine gesetzliche Grundlage für die Erhebung von Nachweisen über persönliche Verhältnisse Dritter, z. B. des unverheirateten Lebenspartners, ersichtlich. Eine solche gesetzliche Grundlage ergibt sich auch nicht aus § 26 VwVfG, der im Einbürgerungsverfahren zur Anwendung kommt. Nach § 26 Abs. 3 VwVfG besteht eine Aussagepflicht für Zeugen - Dritte im Einbürgerungsverfahren sind allenfalls Zeugen - nur, wenn sie durch Rechtsvorschrift vorgeschrieben ist. Eine derartige Rechtsvorschrift existiert im Einbürgerungsverfahren nicht. Unterstrichen wird dies durch Punkt 1.5.1 a der VwV-StA des SMI vom 25. Mai 2003, wonach Zeugen nicht zur Aussage verpflichtet sind.

Das Einbürgerungsverfahren ist ein Verfahren zwischen dem ausländischen Antragsteller und der Einbürgerungsbehörde. Dem Antragsteller obliegt es, die geforderten Nachweise über seine persönlichen Verhältnisse zu erbringen. Die Einbürgerungsbehörde darf ihn nicht verpflichten, Nachweise über die persönlichen Verhältnisse Dritter vorzulegen.

Dass das Ansinnen der konkreten Einbürgerungsbehörde unzulässig war, zeigt auch der Blick auf Punkt 2.1.2 der VwV-StA. Danach ist neben dem Antragsteller ggf. auch der Ehegatte über die Verarbeitung seiner personenbezogenen Daten im Einbürgerungsverfahren zu unterrichten. Der Ehegatte hat dies durch seine Unterschrift nachvollziehbar zur Kenntnis zu nehmen. Nichts anderes dürfte für dritte Personen gelten. Ein anderes Vorgehen der Einbürgerungsbehörde verstieße im Übrigen auch gegen den datenschutzrechtlichen Grundsatz der Datenerhebung beim Betroffenen, nämlich dem Antragsteller.

5.12.3 Akteneinsicht in Ausländerakten

Bereits in 11/5.12.1 hatte ich festgestellt, dass Betroffene ein Recht auf Einsicht in die bei der örtlich zuständigen Ausländerbehörde im Rahmen der Zustimmung zur Visumserteilung durch eine deutsche Auslandsvertretung angelegte Akte haben.

Diese Meinung wurde nicht von allen Ausländerbehörden geteilt, wie nachfolgendes Beispiel zeigt.

Im Frühjahr 2005 wandte sich ein in Deutschland lebender türkischer Staatsangehöriger an mich. Er wollte für seine in der Türkei lebende Ehefrau und die Kinder ein Visum zur Einreise nach Deutschland haben. Die Deutsche Botschaft Ankara beteiligte die örtlich zuständige Ausländerbehörde am Wohnort des Petenten im Rahmen der Zustimmungspflicht gemäß § 31 Abs. 1 AufentV. Der Petent begehrte nunmehr Einsicht in die im Rahmen dieses Mitwirkungsverfahrens angelegte und bei der betreffenden sächsischen Ausländerbehörde geführte Akte. Diese wurde ihm mit der Begründung verweigert, dass hierzu das Einvernehmen mit der Deutschen Botschaft notwendig sei, da es sich nicht um ein selbständiges Verwaltungsverfahren handle. Zu Unrecht, wie ich meine.

Ich habe gegenüber der Ausländerbehörde auf Folgendes hingewiesen: Zwar ist richtig, dass die im Visumverfahren einzuholende Zustimmung der örtlich zuständigen Ausländerbehörde keinen eigenständigen Verwaltungsakt im Sinne des § 35 VwVfG darstellt. Gleichwohl wurden für den verfahrensinternen Mitwirkungsakt bei der örtlich zuständigen Ausländerbehörde personenbezogene Daten des Petenten erhoben und verarbeitet. Dieser Umstand begründet für den Petenten bezüglich seiner personenbezogenen Daten das im § 18 Abs. 3 Satz 1 SächsDSG verankerte Recht auf Akteneinsicht. Ob als Ergebnis der verfahrensinternen Mitwirkung ein selbständiger Verwaltungsakt steht oder nicht, ist insoweit unbeachtlich. Entscheidend für die Akteneinsicht gemäß § 18 Abs. 3 Satz 1 SächsDSG ist allein, ob die zur Person des Betroffenen gespeicherten personenbezogenen Daten in Akten gespeichert werden. Nach dem Volkszählungsurteil ist es erforderlich, dass der Betroffene überschauen kann, welche ihn betreffenden Informationen in bestimmten Bereichen bekannt sind und er abzuschätzen vermag, auf welchem Wissen die ihn betreffenden Entscheidungen ergehen.

Durch die nach § 18 SächsDSG zu gewährende Akteneinsicht wird auch nicht die Rechtsstellung des Bundes untergraben. § 2 Abs. 3 Nr. 3 VwVfG regelt nur, dass das Verwaltungsverfahrensgesetz für die Vertretungen des Bundes im Ausland nicht anwendbar ist und somit für das laufende Visumverfahren bei der deutschen Auslandsvertretung keine Akteneinsicht gewährt werden kann. Gleichwohl findet auf die örtlich zuständige Ausländerbehörde in Sachsen das Sächsische Datenschutzgesetz Anwendung. Durch die Einsichtnahme eines Betroffenen in die dortige Mitwirkungsakte wird das Visumverfahren nicht beeinträchtigt. Der Betroffene erhält insbesondere keine Einsicht in die gesamten Verfahrensakten. Die Rechtsposition des

Bundes wird somit nicht berührt, geschweige denn untergraben. Daher war das zunächst für erforderlich gehaltene Einholen des Einvernehmens der deutschen Auslandsvertretung nicht erforderlich.

Im Ergebnis schloss sich die betreffende Ausländerbehörde meiner Position an.

5.13 Wahlrecht

In diesem Jahr nicht belegt.

5.14 Sonstiges

5.14.1 Verfahren der Zuverlässigkeitsüberprüfung nach dem Luftsicherheitsgesetz (LuftSiG)

Zuverlässigkeitsüberprüfungen nach dem Luftsicherheitsgesetz werden in Sachsen zentral durch das Regierungspräsidium Dresden durchgeführt. Auf eigenen Antrag werden danach alle Personen überprüft, die Zutritt zu den nicht allgemein zugänglichen Bereichen eines Flughafens erhalten sollen. Die Neuansiedlung eines großen Frachtunternehmens am Flughafen Halle/Leipzig sowie der Neubau der Start- und Landebahn am Flughafen Dresden lässt - so wurde uns vom Regierungspräsidium erläutert - eine Vielzahl von Überprüfungsanträgen erwarten. Um diese in der gebotenen Zeit bearbeiten zu können und um Mehrfacherfassungen zu vermeiden, beabsichtige es, die Antragsdaten für Zuverlässigkeitsüberprüfungen nach § 7 LuftSiG durch die Betreibergesellschaften der Flughäfen erheben zu lassen. Diese sollten die Daten dann elektronisch an das Regierungspräsidium übermitteln.

Ich habe deutlich gemacht, dass die Betreibergesellschaften der Flughäfen durch das Luftsicherheitsgesetz nicht ermächtigt worden sind, personenbezogene Daten der Antragsteller zum Zweck der Zuverlässigkeitsüberprüfung zu erheben. In Betracht käme lediglich, dass die Betreibergesellschaften der Flughäfen Daten der Antragsteller im Wege der Auftragsdatenverarbeitung als Auftragnehmer des Regierungspräsidiums nach § 7 SächsDSG erheben und übermitteln. Das Regierungspräsidium bliebe für die Einhaltung der datenschutzrechtlichen Vorschriften verantwortlich und hätte die Betreibergesellschaften der Flughäfen als Auftragnehmer entsprechend anzuweisen und zu beaufsichtigen. Insbesondere müsste festgelegt werden, welche personellen, technischen und organisatorischen Maßnahmen nach § 9 SächsDSG zu treffen sind, um das Recht der Betroffenen auf informationelle Selbstbestimmung zu wahren. Es müsste praktisch ausgeschlossen sein, dass die Betreibergesellschaften der Flughäfen die „interessanten“ Antragstellerdaten aus der Zuverlässigkeitsüberprüfung für eigene Geschäftszwecke, z. B. zur Minimierung von Krankheitskosten,

verarbeiten könnten. Dies gälte insbesondere im Hinblick auf die Verarbeitung von Daten eigener Beschäftigter der Betreibergesellschaften der Flughäfen (Arbeitnehmerdaten).

Das Regierungspräsidium hatte mich frühzeitig beteiligt. Derzeit befinde ich mich noch in einem durchaus konstruktiven Austausch mit dieser Behörde; die weitere Entwicklung bleibt abzuwarten.

6 Finanzen

6.1 Datenverarbeitung bei der Stundung von Kommunalabgaben

Im Zusammenhang mit Stundungsanträgen erreichten mich im letzten Berichtszeitraum vereinzelt Bürgerbeschwerden mit ähnlichem Inhalt. Das Sächsische Kommunalabgabengesetz erklärt die Abgabenordnung für anwendbar. Demnach hat eine Behörde zu prüfen, ob es eine erhebliche Härte für den Antragsteller bedeutet, wenn dieser eine Abgabe, Gebühr oder einen Beitrag mit Fälligkeit zu begleichen hat. Regelmäßig verwenden die Behörden für die Prüfung Formulare, die den Betroffenen als Erhebungsbogen vorgelegt werden. Hiergegen ist nichts einzuwenden, denn dies dient einer gleichmäßigen Datenverarbeitung im Hinblick auf deren Umfang, Tiefe und Ausmaß. Zu empfehlen ist auch, dass sich die Behörden eigene Richtlinien für das Stundungsverfahren auferlegen. Zulässig ist es hierbei, soziale Gesichtspunkte einzubeziehen. So wird man einen Alleinstehenden anders behandeln können, als denjenigen, der Familienmitglieder zu versorgen hat. Vermieden werden sollte dennoch, dass Dritte, die nicht Abgabenschuldner sind, in die Datenverarbeitung einbezogen werden. So ist zum Beispiel die Mit-Erhebung von Einkommensangaben eines Verwandten, der nicht Schuldner ist, nicht ohne weiteres zulässig. Eine Erhebung der Daten von Dritten dürfte dem Grunde nach nur mit deren Wissen und Wollen erfolgen. Sofern zum Beispiel eine getrennte steuerliche Veranlagung von Ehepartnern stattfindet, wäre der Antragsteller z. B. darauf angewiesen, dass die dem Steuergeheimnis unterliegenden Einkommensdaten des Ehepartners für die Nutzung durch die die Stundung gewährende Behörde von diesem freigegeben werden, um sie vortragen zu können. Das Beiziehen solcher Angaben sehe ich als zu weitgehend und nicht mehr als verhältnismäßig an. Darüber hinaus empfehle ich auch generell, datensparsam vorzugehen. Eine Gesamtaufstellung der Vermögensverhältnisse sollte seitens der Behörde nicht intendiert werden. Sofern Erhebungsformulare Verwendung finden, sollte man sich möglichst auf eine Liquiditätsaufstellung beschränken. Darüber hinaus hat die Datenverarbeitung im Hinblick auf Umfang, Tiefe und Ausmaß, gemessen an der Abgabenschuld - auch bei Stundungen, auf die kein Anspruch bestehen mag - zumutbar zu bleiben.

6.2 Datenverarbeitung in der Steuerverwaltung - Ausblick

Kein anderer Bereich der öffentlichen Verwaltung betreibt eine derart offensive Automatisierung von Verfahren wie die deutsche Steuerverwaltung. Zentrale Informationssysteme, bundesweite Verbunddateien und Übermittlungsverfahren bilden hierbei einen in der Öffentlichkeit wahrgenommenen Schwerpunkt.

Zum Teil wird zugunsten einer Automatisierung auf datenschutzorganisatorisch zureichende Informationsschritte verzichtet wie beim ELSTER-Verfahren, bei dem Steuererklärungen ohne Signatur und ohne Unterschrift automatisiert übermittelt werden können. Ich bedaure das, denn Steuerverfahren haben meiner Ansicht nach in besonderer Weise datenschutzgerechten Standards zu genügen.

Die zentrale bundesweite Verarbeitung der Steuer-Identifikationsnummer durch das neu geschaffene Bundeszentralamt für Steuern und die Registrierung der Steuernummer in Meldedatensätzen stellen eine beginnende fach- und ressortübergreifende Vernetzung von personenbezogenen Daten der Steuerpflichtigen in bisher nie da gewesener Weise dar. In besonderem Maße besorgt bin ich, wenn Datenbestände nicht zweckgebunden allein zu Steuerzwecken verarbeitet werden sollen, wie z. B. bei den zentral für die Verwaltung vorgehaltenen Kontostammdaten, die auch für Behörden außerhalb der Steuerverwaltung zugänglich sein sollen. Bei der zentralen Steuer-Identifikationsnummer-Datenbank befürchte ich eine ähnliche Entwicklung (vgl. 16.2.28).

Nachtrag zu einer Entscheidung nach Ende des Berichtszeitraums: Das Bundesverfassungsgericht hat in seiner Entscheidung vom 13. Juni 2007 (1 BvR 1550/03, 1 BvR 2357/04, 1 BvR 603/05) die Kontenabfragemöglichkeit nach § 24 c Abs. 3 Satz 1 Nr. 2 KWG und die Eingriffsermächtigung des § 93 Abs. 7 AO und des § 93 Abs. 8 AO in sozialrechtlichen Angelegenheiten für als mit dem Grundgesetz vereinbar angesehen. Dem Bestimmtheitsgrundsatz genügt § 93 Abs. 8 AO allerdings nach der Entscheidung insoweit nicht, als dass der Kreis der Behörden und die Aufgaben, denen der Abruf dienen soll, nicht hinreichend bestimmt sind. Ein Antrag auf einstweilige Anordnung zum Streitgegenstand war nicht erfolgreich. Die Abrufverfahren konnten zwischenzeitlich betrieben werden. Eine Kontrolle zu einer datenschutzgerechten Verfahrenspraxis Stammdaten abrufender sächsischer Behörden steht meinerseits noch aus (vgl. 12/6.3).

6.3 Einzugsermächtigungsverfahren bei der Kraftfahrzeugsteuer

Im letzten Berichtszeitraum ist die Verordnung der sächsischen Staatsregierung über die Mitwirkung der Zulassungsbehörden bei der Verwaltung der Kraftfahrzeugsteuer (MZulKraftStVO) in Kraft getreten.

Hierbei hat die Staatsregierung von der Möglichkeit des § 13 Abs. 1 Satz 2 und Abs. 1a Satz 1 bis 7 KraftStG Gebrauch und die Zulassung von Kraftfahrzeugen von der Erteilung einer Einzugsermächtigung durch den Fahrzeughalter abhängig gemacht.

Ich habe mich gegen die Beschränkung der Wahlmöglichkeiten der Betroffenen bei ihren Bezahlmöglichkeiten gewandt. Die Staatsregierung ist dem nicht gefolgt.

Die Verordnung enthält darüber hinaus eine Prüfbefugnis für die Kraftfahrzeugzulassungsbehörden bei Kraftfahrzeugsteuerrückständen. Die Zulassungsbehörde ist danach befugt, entsprechende Auskünfte bei der sächsischen Finanzverwaltung einzuholen.

6.4 Datenverarbeitung bei der Erhebung einer Zweitwohnungssteuer

Im letzten Berichtszeitraum wurde in der Landeshauptstadt Dresden eine Zweitwohnungssteuer eingeführt, die zu häufigen Nachfragen bei meiner Behörde führte. Man bat mich um Prüfung, inwieweit eine Erklärung zur Zweitwohnungssteuer einen unzulässigen Eingriff in das Persönlichkeitsrecht darstellen würde. Unter anderem wurden präzise Angaben zum Mietverhältnis und zur genutzten Wohnsituation abverlangt. Darüber hinaus war die Landeshauptstadt auch an einen Betreiber von Studentenwohnheimen zur Datenerhebung herangetreten.

Grundsätzlich ist die Erhebung einer Zweitwohnungssteuer auf der Grundlage der §§ 1f und 7 SächsKAG durch Satzung erlaubt. Ich habe auch die Erhebung der Daten in Umfang, Tiefe und Ausmaß selbst als verhältnismäßig angesehen. Hingegen ist die Frage, ob ein weitgehend undifferenziertes Anknüpfen der Steuer an eine Nebenwohnung anhand der Meldedaten bei Studenten steuerrechtlich zulässig ist, keine datenschutzrechtliche Frage mehr gewesen, sondern eine rein steuerrechtliche (vgl. OVG Koblenz vom 29. Januar 2007 - 6 B 11579/06).

Der Versuch auf Dritte zur Datenerhebung zurückzugreifen, war mangels gesetzlicher Voraussetzungen allerdings nicht zulässig gewesen. § 3 SächsKAG bestimmt für das Verwaltungsverfahren sinngemäß die Anwendung der Abgabenordnung. Nach § 93 Abs. 1 AO soll sich die Finanzbehörde grundsätzlich zunächst an den Beteiligten - das wäre der jeweilige Student gewesen - wenden, um die erforderlichen Auskünfte zu erhalten. Andere natürliche und juristische Personen als der Beteiligte sollen erst dann zur Auskunft herangezogen werden, wenn die Sachverhaltsaufklärung durch den Beteiligten nicht zum Ziel führt oder keinen Erfolg verspricht. Insofern war es Aufgabe des Steueramtes der Landeshauptstadt Dresden, die erforderlichen Daten zu erheben und zum Beispiel mit Hilfe des Melderegisters die infrage kommenden Bewohner einer Nebenwohnung (hier des Studentenwohnheimes) als eventuelle Beteiligte zu ermitteln und um Auskunft zu bitten. Erst wenn

beispielsweise Zweifel an der Richtigkeit der vom steuerpflichtigen Beteiligten erteilten Auskunft bestehen sollten, hätte das Studentenwerk im Einzelfall unter Angabe des Namens und der Anschrift des Beteiligten zur Datenerhebung einbezogen werden können.

7 Kultus

7.1 SaxSVS - Automatisierte Verarbeitung von Personal- und Schülerdaten

Im letzten Berichtszeitraum hat das SMK in seinem Geschäftsbereich ein umfassendes Informationssystem eingeführt, was ich beratend begleitet habe. Die sächsische Schulverwaltungssoftware „SaxSVS“ soll die Schulleitungen bei der Schülerverwaltung, bei der Planung des Unterrichtseinsatzes der Lehrer und bei statistischen Auswertungen sowie die Schulaufsicht bei der Planung und Verwaltung des Personals unterstützen. Auf der Zugriffs-Ebene der jeweiligen Schule kommt jeweils eine MySQL-Datenbank zum Einsatz. Die Schulaufsicht greift auf eine Oracle-Datenbank (Oracle-RDBMS), einen Gesamtdatenbestand, zurück, der regelmäßig mit den einzelnen Datenbeständen der Schulen abgeglichen wird. Aus der daneben existierenden „Landespersonaldatenbank Kultus“ (LPDK) werden zudem notwendige Lehrerpersonaldaten eingespeist. Insgesamt befinden sich in der Datenbank also Einzelangaben zu Lehrern, Elternsorgeberechtigten und Schülern. Alleine bei den Lehrkräften handelt es sich um fünfstellige Datensatzbestände. Gepflegt und systemtechnisch unterhalten wird die Datenbank beim Landesamt für Statistik.

Zu dem Verfahren besteht ein Datenschutz- und Sicherheitskonzept. Darin enthalten ist ein differenziertes Zugriffsberechtigungskonzept hinsichtlich der jeweiligen Ebenen - Schule, Schulaufsicht - und personell. Den Behörden steht außerdem ein Handbuch zur Verfügung, um Einrichtung und Betrieb des Verfahrens zu gewährleisten. In Bezug auf die Frage, ob die datenschutzorganisatorischen und sicherheitstechnischen Schutzvorkehrungen vollständig ausreichen, möchte ich, in Anbetracht der Tatsache, dass in dem Verfahren erhebliche Datensatzbestände incl. Personaldaten verarbeitet werden, einen gelegentlichen externen - durch eine Fachfirma durchgeführten - Schwachstellen- und Sicherheitstest anempfehlen.

Das federführende SMK hat bei dem Verfahren auch den Anspruch, eine gleichmäßigere Datenverarbeitung an den Schulen zu gewährleisten. Über das Verfahren hinausgehend brachte das SMK auch eine neue Verwaltungsvorschrift auf den Weg, die eine geregeltere Nutzung von dienstlichen personenbezogenen Daten durch die Lehrkräfte, auch auf deren privaten Datenträgern, regeln soll (vgl. 7.2).

Individualdatenbanken, die als automatisierte Verfahren betrieben und über Jahre gepflegt werden, beinhalten ein erhöhtes persönlichkeitsrechtliches Gefährdungspotential. Bei der inhaltlichen Erschließung und Nutzung der Datenbestände gilt es daher

zu vermeiden, dass Amtsträger in die Lage versetzt werden, sich Lebensprofile unter Einbeziehung der Leistungsdaten der Schüler zu erschließen (vgl. 16.2.17).

Im Übrigen halte ich es für überzeugender, nicht jede personenbezogene Beschäftigten-Datenverarbeitung auszulagern, sondern - wie in diesem Fall - als Bereich der öffentlichen Kernverwaltung selbst durchzuführen. Soweit eine Auftragsdatenverarbeitung bei Beschäftigtendaten erfolgen soll, wäre jedoch zu fordern und darauf zu achten, dass der Auftragnehmer, der dann möglichst eine sächsische öffentliche Stelle sein sollte, sich auch auf eine normenklare gesetzliche Aufgabenzuweisung stützen kann (Art. 83 Abs. 1 SächsVerf).

Das Verfahren werde ich fortwährend datenschutzrechtlich begleiten.

7.2 Datenschutzgerechte Datenverarbeitung durch Lehrkräfte im Zuhause-Bereich

Gegen Ende des Berichtszeitraums erließ das SMK eine neue Verwaltungsvorschrift, die den Datenschutz beim Umgang mit personenbezogenen Daten an Schulen regeln soll. Ich wurde bei der Erstellung der Verwaltungsvorschrift angehört (vgl. „Verwaltungsvorschrift des SMK über den Datenschutz beim Umgang mit personenbezogenen Daten an Schulen“ (VwV Schuldatenschutz, MBl. 2007 Nr. 3, S. 26). Obwohl die *Verwaltungsvorschrift des SMK zum Datenschutz an Schulen und Schulaufsichtsbehörden des Freistaates Sachsen* und die *Verwaltungsvorschrift des SMK zur automatisierten Verarbeitung von Schülerdaten in Schulen und Schulaufsichtsbehörden des Freistaates Sachsen* thematisch mit der neuen Verwaltungsvorschrift nicht deckungsgleich gewesen sind, sind sie mit Veröffentlichung der neuen Verwaltungsvorschrift außer Kraft getreten.

Die neue Verwaltungsvorschrift gibt auch Hinweise zur Verarbeitung personenbezogener Daten auf privaten Computern von Beschäftigten an Schulen. Ich begrüße es grundsätzlich, dass sich die oberste Dienstbehörde der Problematik angenommen hat, dass viele personenbezogene Daten im Schulbereich von Lehrkräften Zuhause und mit privaten Datenverarbeitungsanlagen verarbeitet werden. Wünschenswert wäre es, wenn die Verwaltung, die Kenntnis davon hat, dass im privaten und häuslichen Bereich der Mitarbeiter personenbezogene Daten verarbeitet werden, hierfür auch die entsprechende Computerausstattung zur Verfügung stellen würde. Im Schulbereich mit vielen tausend Lehrkräften ist das leider unrealistisch. Die Kultusverwaltung ist hierfür nicht zu gewinnen. In anderen Bereichen der Verwaltung, so zum Beispiel bei Gerichtsvollziehern, im gemeindlichen Vollstreckungsbereich oder bei

Außenprüfern der Finanzbehörden erwarte ich allerdings, dass die Beschäftigungsbehörden auch die notwendige sächliche Ausstattung zur Verfügung stellen.

Die Verwaltungsvorschrift ist auch ein positiver Ansatz, die bisher - häufige - ungeregelte „Heimarbeit“ der Lehrkräfte im Kultusbereich datenschutzorganisatorisch und datenschutzrechtlich abzusichern. Ich hoffe, dass die Umsetzung gelingt. Nach der Verwaltungsvorschrift wird die Datenverarbeitung an Bedingungen geknüpft. Eine Voraussetzung, dass auf Datenverarbeitungsanlagen im privaten Bereich Schülerdaten verarbeitet werden können, ist, dass die Lehrkraft akzeptiert und einwilligt, dass ihr Privat-Computer, auf dem dienstliche Daten verarbeitet werden sollen, im Hinblick auf Datensicherheit, den Umfang der Daten und im Hinblick auf Datenschutz den dienstlichen Regeln unterliegt. Lehrkräfte, die dies nicht wollen, sollten davon Abstand nehmen, außerhalb der Schule selbst personenbezogene Daten ihrer Schüler automatisiert zu verarbeiten. Zu den Datensicherheitsmaßnahmen gehört u. a., dass der Computer, was die dienstlichen Daten angeht, vor unbefugten Zugriffen - auch denen von Familienmitgliedern - geschützt bleibt, Verschlüsselungssysteme genutzt werden und regelmäßig in Bezug auf Fehler und Viren geprüft wird. Was die Schülerdaten selbst angeht, so sollen nur die Daten verarbeitet werden, die erfahrungsgemäß erforderlich sind, um den Lehrbetrieb sicherzustellen. Die Daten sind im Einzelnen vom Umfang her in der Verwaltungsvorschrift beschrieben. Selbstverständlich müssen Datenverarbeitungsanlagen, auf denen dienstliche Daten verarbeitet werden, auch datenschutzrechtlich kontrolliert werden können. Es kann keine kontrollfreien Räume geben. Lehrkräfte, die sich entschließen, dienstliche Daten zu Hause zu verarbeiten, haben gegebenenfalls bei einer Stichprobenkontrolle oder auf Anlass hin, ihren Computer einer Kontrolle durch den Datenschutzbeauftragten der Schule oder den Sächsischen Datenschutzbeauftragten zugänglich zu machen. Nach der Verwaltungsvorschrift sollen die Lehrkräfte eine entsprechende Belehrung bzw. Verpflichtung unterschreiben.

Soweit die Verwaltungsvorschrift in der Praxis erfolgreich umgesetzt werden kann, könnte sie auch für andere Geschäftsbereiche und bei den Kommunen Beispiel sein.

7.3 Genehmigung von Schulen in freier Trägerschaft - Überprüfung von Lehrkräften freier Schulen

Hilfesuchend wandte sich eine Lehrkraft an mich und trug vor, dass das zuständige Regionalschulamt ihr wiederholt die Einsichtnahme in die zu ihrer Person gespeicherten Akten verweigere. Zunächst konnte ich aufgrund der mir durch den

Petenten gegebenen Hinweise dafür Sorge tragen, dass der Betroffene vollständige Akteneinsicht in die zu seiner Person geführten Akten bekam.

Bei meiner Kontrolle musste ich darüber hinaus jedoch feststellen, dass die staatlichen Schulbehörden abseits gesetzlicher Regelungen für sich in Anspruch nahmen, einzelne Personalbesetzungen bei Schulen in freier Trägerschaft zu unterbinden. Die Erhebung von Einzelangaben zu sämtlichen einzelnen Lehrkräften begründete man mit den Genehmigungsbestimmungen in Bezug auf Schulen in freier Trägerschaft im Sinne von § 5 FrTrSchulG, was schon eine Überdehnung der gesetzlichen Grundlage darstellen mag und seitens der betroffenen Schulen z. T. durchaus als Gängelei begriffen wird. Eine Ersatzschule hatte im von mir kontrollierten Einzelfall als Schule in freier Trägerschaft Personalunterlagen zu einzelnen einzustellenden Lehrern übermittelt und daraufhin vom Regionalschulamt eine informelle telefonische Mitteilung erhalten, dass der Petent nicht als Lehrkraft eingesetzt werden könne. Der freie Träger hatte daraufhin das Vertragsverhältnis wieder gelöst und den Betroffenen über die vorgebliche Nichteignung unter Bezugnahme auf Gründe nach § 7 FrTrSchulG in Kenntnis gesetzt. Der Petent war damit aber von Rechtsschutzmöglichkeiten abgeschnitten. Ein ordentliches Verfahren nach § 7 FrTrSchulG wurde durch das Regionalschulamt nicht betrieben.

Die Erklärung seitens des Amtes, dass der freie Träger das Einstellungsvorhaben von sich aus nicht weiter verfolgt habe und die Schulaufsichtsbehörde den Betroffenen aus diesem Grund auch nicht zu bescheiden brauche, war wegen des so gesetzlich nicht vorgesehenen Verfahrens einer Genehmigung einzelner Lehrkräfte nicht vertretbar. Entscheidungen der Schulaufsichtsbehörde nach § 17 FrTrSchulG sind als Verwaltungsakte auszugestalten, damit nach Abschluss eines erfolglosen Widerspruchsverfahrens in einem gerichtlichen Verfahren die Rechtmäßigkeit staatlichen Handelns überprüft werden kann. Adressat des Bescheides nach §17 FrTrSchulG über die Untersagung der Lehrtätigkeit ist stets die Lehrkraft. Der Schulträger hätte lediglich eine Mitteilung von der Untersagung mit Hinweis auf § 17 Abs. 1 Nr. 4 FrTrSchulG erhalten können. Darüber hinaus weist § 7 FrTrSchulG auch mit dem Gesetzeswortlaut „Verhalten zeigen …“ oder „Tatsachen vorliegen, die sie für eine Ausübung einer solchen Tätigkeit ungeeignet erscheinen lassen“. auf die zwingende Notwendigkeit hin, die Geeignetheit von Lehrkräften zu prüfen und die Würdigung seiner Geeignetheit für den Schuldienst nach pflichtgemäßen Ermessen zu bewerten. Diese Bewertung ist dann auch durch einen Verwaltungsakt ordnungsgemäß zu begründen. Die Schulaufsichtsbehörde hatte eine Bewertung nicht durchgeführt, sie hat sich letztlich ausschließlich auf Vorwissen und die Selbstauskunft des Betroffenen aus dem Jahre 1991 gestützt. Unterlagen der BStU hatten nicht einmal vorgelegen.

Nach Vorstellung des SMK sollten im Übrigen die bei Schulen in freier Trägerschaft einzustellenden Lehrkräfte Selbstauskünfte in Bezug auf eine Mitarbeit bei der Stasi oder vergleichbaren Organisationen abgeben. Hierfür gab es auch ein entsprechendes Formular. Dies hätte aber gesetzlich nach dem Stasi-Unterlagen-Gesetz im Ermessen des jeweiligen Arbeitgebers gelegen und hätte nicht staatlicherseits vorgegeben werden können. Ich hatte dies dem zuständigen Staatsministerium mitgeteilt, das gleichwohl nicht zu einer Einsicht zu bringen war. Mit der Novellierung des Stasi-Unterlagen-Gesetzes dürfte eine Grundlage für das Revisionsstreben der Schulbehörden in diesem Bereich aber nunmehr endgültig entfallen sein (vgl. 5.1.3).

7.4 Schulgesundheitspflege - Schulen in freier Trägerschaft

Regelmäßig erhalte ich durch Elternsorgeberechtigte Anfragen zum Tätigwerden von Gesundheitsämtern in Schulen in freier Trägerschaft. § 26a SchulG bestimmt, dass alle schulpflichtigen Kinder verpflichtet sind, sich einer Schulaufnahmeuntersuchung zu unterziehen. Nach § 2 Abs. 2 der Schulgesundheitspflegeverordnung wird festgelegt, dass die Schulaufnahmeuntersuchungen durch das Gesundheitsamt durchgeführt werden. Davon sind letztendlich auch Schüler, die Schulen in freier Trägerschaft besuchen, betroffen. Im Übrigen ist die Schulgesundheitspflegeverordnung nach § 1 nur anwendbar, wenn dies bezüglich der Schulen in freier Trägerschaft ausdrücklich bestimmt ist. Was die weiteren Untersuchungen (Reihenuntersuchungen), zusätzlichen oder schulzahnärztlichen Untersuchungen angeht, ist ein Tätigwerden der Gesundheitsämter in Schulen in freier Trägerschaft nicht vorgesehen. Dennoch erfolgende Datenverarbeitungen der Gesundheitsämter in diesen Schulen finden keine gesetzliche Stütze. Die datenschutzorganisatorisch verantwortlichen Schulleitungen und nicht zuletzt die Gesundheitsämter selbst sollten dem Rechnung tragen (weiterführend zu Schulgesundheitsuntersuchungen unter 12/7.3).

8 Justiz

8.1 Entwurf eines Sächsischen Jugendstrafvollzugsgesetzes

Nach der Föderalismusreform ist die Gesetzgebungszuständigkeit für das Strafvollzugswesen vom Bund auf die Länder übergegangen. Künftig dürfen mithin die Länder über die Ausgestaltung des Strafvollzuges und des Jugendstrafvollzuges bestimmen. Im Hinblick auf den Jugendstrafvollzug stehen die Länder dabei unter dem Druck des Bundesverfassungsgerichts, das in seinem Urteil vom 31. Mai 2006 (2 BvR 1673/04; 2 BvR 2402/04) die Schaffung eigener gesetzlicher Grundlagen für den Jugendstrafvollzug bis Ende 2007 gefordert hat. Das SMJus hat mich frühzeitig über seinen Referentenentwurf unterrichtet, der sich an einen gemeinsamen Entwurf von neun Bundesländern („9-Länder-Entwurf“) anlehnt.

Zu diesem und dem mittlerweile durch die Staatsregierung nicht weiter verfolgten Entwurf eines Sächsischen Strafvollzugsgesetzes habe ich schriftlich und in Besprechungen mit dem SMJus Stellung genommen. Das SMJus hat viele meiner ersten Anregungen zur datenschutzgerechteren Gestaltung beider Referentenentwürfe übernommen. Dafür und für die aufgeschlossene Arbeitsatmosphäre, die eine wahre Diskussion erlaubte und sich positiv von der anderer Häuser der Staatsregierung abhob, danke ich. Gleichwohl sind einige der mir wichtigen Anliegen noch nicht ausreichend berücksichtigt worden. Sie sind in Abstimmung mit dem SMJus dem parlamentarischen Verfahren vorbehalten geblieben.

So ist beispielsweise noch nicht im Entwurf verankert worden, dass das sog. Zugangsgespräch des neu in die Anstalt aufgenommenen Gefangenen mit Anstaltsbediensteten ausnahmslos ohne das Beisein anderer Gefangener stattfinden muss. Im Zugangsgespräch wird namentlich die „gegenwärtige Lebenssituation“ des Gefangenen (z. B. Gesundheitszustand, Suizidabsicht, Beziehungsprobleme, finanzielle Lage etc.) erörtert. Es handelt sich um heikle Daten, die Unbefugten definitiv nicht zur Kenntnis gelangen dürfen. Andere Gefangene sind stets Unbefugte. Sie bieten grundsätzlich keine Gewähr für Verschwiegenheit gegenüber Dritten, in der Regel gegenüber weiteren Gefangenen. Die Anstalt aber ist insofern in einer Garantenstellung: Sie muss dafür sorgen, dass die Informationen aus dem Zugangsgespräch - ebenso wie aus anderen Gesprächen des Gefangenen mit der Anstaltsleitung oder ihren Beauftragten - nicht zur Kenntnis anderer Gefangener gelangen. Die Vertraulichkeit dieses Gesprächs zwischen Gefangenem und Anstaltsleitung oder beauftragten Bediensteten muss ohne Wenn und Aber gewährleistet sein. Diese Forderung kann nicht durch die „Einwilligung“ des Gefangenen in die An- oder Abwesenheit anderer Gefangener beim Zugangsgespräch abgebogen werden. Im Justizvollzug er-

teilte Einwilligungen sind nie ganz freiwillig. Gefangene stehen unter Anpassungsdruck. Sie wollen in bestimmten Situationen Wohlverhalten demonstrieren. Hinzu kommt: Auch „erfahrene“ Gefangene werden die Auswirkung der Anwesenheit anderer Gefangener auf die Vertraulichkeit ihrer Angaben kaum einschätzen können. Unter den Bedingungen des Vollzuges können sich täglich neue Konstellationen ergeben, in denen ein Mitgefangener die im Zugangsgespräch erlangten Kenntnisse zum Nachteil des Gefangenen „verwerten“ kann.

Ein anderer bisher nicht zufrieden stellend gelöster Kritikpunkt betrifft die Möglichkeit der Überwachung von Besuchen mit technischen Mitteln, d. h. mit Videoüberwachungssystemen. Diese Möglichkeit weicht vom o. g. „9-Länder-Entwurf“ ab. Eine Überwachung mit technischen optischen Mitteln (Videokameras) berührte das Recht auf informationelle Selbstbestimmung des Gefangenen und der Besucher in besonderer Weise, da unklar bliebe, ob der Besuch gerade überwacht wird oder nicht. Videoüberwachung führt zu einer Verhaltensänderung der Betroffenen. Dies mag bei Gefangenen, zumal innerhalb der Anstalt, noch hingenommen werden, bei Besuchern in Besuchsräumen ist dies jedoch möglichst zu vermeiden. Ziel der Regelung muss daher die Transparenz der Datenverarbeitung sein, d. h. der Gefangene und mehr noch die Besucher müssen wissen können, ob und wann sie im Einzelfall aktuell überwacht werden. Die Überwachung durch Videokameras muss genauso transparent sein wie die Überwachung durch einen Bediensteten an Ort und Stelle (Äquivalenz). Eine Aufzeichnung darf nicht stattfinden.

Schließlich habe ich gegen die gegenwärtige Entwurfsfassung der Vorschriften über die Errichtung einer Zentralen sächsischen Gefangenendatei und die Einrichtung automatisierter Übermittlungs- und Abrufverfahren schwere Bedenken. Die Vorschrift ist datenschutzrechtlich von besonderer Bedeutung, da sie eine zentrale Speicherung aller Gefangenendaten sowie die Herstellung eines „Verbundes“ mit den Dateien zumindest der anderen beteiligten Länder erlaubte. Die Einrichtung und der Betrieb einer bisher nicht vorhandenen und ohne weiteres auch nicht erforderlichen zentralen Gefangenendatei bedürfen einer normenklaren und bestimmten gesetzlichen Rechtsgrundlage. Insbesondere sind die Zwecke anzugeben, für die eine zentrale Speicherung erforderlich sein soll. Hierfür reicht eine Bezugnahme auf „die Anstalt und die Aufsichtbehörde“ nicht aus, zumal ein Zweck auch in der Herstellung eines „Datenverbundes“ bestehen soll. Des Weiteren ist der Erforderlichkeitsgrundsatz, wonach personenbezogene Daten nur verarbeitet werden dürfen, wenn sie zur Erfüllung einer bestimmten Aufgabe erforderlich sind, zu beachten. Da nicht alle der in den einzelnen Anstalten zu erhebenden Daten auch für die Zwecke anderer Anstalten oder der Aufsichtsbehörde erforderlich sein können, kann ich derzeit die Erforder-

lichkeit einer zentralen Datei, die sämtliche Daten aller Gefangenen enthält, noch nicht erkennen. Soweit eine solche zentrale Datei insbesondere für Zwecke der Evaluation oder der kriminologischen Forschung erforderlich sein sollte, müssen diese Zwecke ausdrücklich bestimmt werden. Dabei wäre der Grundsatz der Datenvermeidung und Datensparsamkeit (§ 9 Abs. 1 Satz 2 SächsDSG) - eventuell durch Pseudonymisierung oder Anonymisierung, sobald dies möglich ist - zu beachten. Hinzu kommt, dass die Erforderlichkeit einer zentralen Datei derzeit nicht ausreichend begründet erscheint. In der Begründung des Referentenentwurfs wird zwar ausgeführt, dass es „unerlässlich“ sei, „vergleichbare Daten unabhängig vom Ort der Inhaftierung zu erlangen“. Der Strafvollzug hat jedoch bisher ohne zentrale landesweite Vollzugsdatei funktioniert.

Einige weitere Kritikpunkte werde ich im parlamentarischen Verfahren noch vortragen.

8.2 Anlassunabhängige datenschutzrechtliche Kontrollen von Staatsanwaltschaften

Seit 1993 unterziehe ich die Justiz- und Sicherheitsbehörden immer wieder anlassunabhängigen angekündigten datenschutzrechtlichen Querschnittskontrollen. Ich bin davon überzeugt, dass die kontrollierten Stellen selbst am besten wissen, wie sie eventuelle Defizite im Grundrechtsschutz ausgleichen können. Hierzu gebe ich mit meinen Kontrollen Anlass nachzudenken. Daneben geht es natürlich auch um konkrete datenschutzrechtliche Verstöße. Mein Ziel ist es, diese aufzudecken und daran mitzuwirken, ihnen abzuhelfen.

Im August 2006 habe ich mit anlassunabhängigen angekündigten Querschnittskontrollen der sächsischen Staatsanwaltschaften begonnen. Die bisherigen Ergebnisse aus drei Staatsanwaltschaften stimmen mich positiv. Die kontrollierten Staatsanwaltschaften hatten sich intensiv auf meine Kontrolle vorbereitet, sie offen und zuvorkommend unterstützt und kompetent begleitet. Hierfür sei nochmals ausdrücklich gedankt. Daneben gilt mein Dank auch der Generalstaatsanwaltschaft Dresden sowie dem SMJus für die gute Zusammenarbeit.

Schwerpunktmäßig habe ich die Bereiche Telekommunikationsüberwachung, die retrograde Erfassung von DNA-Identifizierungsmustern, die Führung von Handakten, Löschfristen, die Poststelle/Posteingangsverwaltung, die Bescheidung von Anzeigeerstattern, die Zusammenarbeit mit der Polizei, Anfragen bei der Bundesanstalt für Finanzdienstleistungen, Auskünfte an und Akteneinsicht durch Dritte, die Büro-

kommunikation, den Schutz besonders heikler Daten in Verfahrensakten sowie diverse technisch-organisatorische Vorkehrungen (u. a. Hausordnung, Videotechnikeinsatz, Papierentsorgung, Verpflichtung nach § 6 SächsDSG, Personalaktenaufbewahrung) kontrolliert.

In keiner der kontrollierten Staatsanwaltschaften habe ich schwerwiegende datenschutzrechtliche Mängel feststellen müssen. Ich erhielt den Eindruck von Strafverfolgungsbehörden, die das Grundrecht aller Betroffenen - von Opfern, Zeugen, Beschuldigten oder anderen Betroffenen - auf informationelle Selbstbestimmung ernst nehmen, die einschlägigen Rechtsvorschriften beachten und die erforderlichen technisch-organisatorischen Vorkehrungen getroffen haben.

Kleinere Mängel betrafen den in der Praxis nicht immer ausreichend beachteten Vorrang der Erteilung von Auskünften gegenüber der Akteneinsicht, die besondere Aufbewahrung von Aktenteilen mit besonders heiklen Daten im Aktengeheft (etwa Krankengeschichten in einem „Kunstfehlerverfahren“ gegen einen Arzt, Lichtbildmappen in Leichensachen oder bei strafbaren pornographischen Handlungen), die Benachrichtigung der Betroffenen über bereits durchgeführte Telekommunikationsüberwachungsmaßnahmen oder Personalaktenfragen. Nur beispielhaft sei etwa der Fall einer retrograden Erfassung des DNA-Identifizierungsmusters genannt: Drei Mittäter waren in einem Verfahren angeklagt und verurteilt worden. In allen drei Fällen bat die Staatsanwaltschaft die Polizei zunächst darum, die Speicherung des DNA-Identifizierungsmusters der Täter in der DNA-Analyse-Datei des BKA zu veranlassen. Zwei der Betroffenen verweigerten zunächst die Einwilligung. Auf die Anregung der Polizei hin, einen richterlichen Beschluss zu beantragen, stellte die Staatsanwaltschaft nach neuerlicher Prüfung fest, dass keine Negativprognose gestellt werden könne. Grund hierfür war, dass die Tat lange zurücklag und seither die Betroffenen nicht wieder in Erscheinung getreten waren. Ob diese Feststellung der Polizei mitgeteilt worden war, ließ sich aus der Akte nicht ersehen. Die DNA-Identifizierungsmuster dieser zwei Betroffenen wurden dementsprechend nicht beim BKA erfasst. Der dritte Betroffene, der ebenfalls vor und nach der Tat strafrechtlich nicht weiter aufgefallen war, erklärte vermutlich der Polizei seine Einwilligung. Die Polizei teilte daraufhin der Staatsanwaltschaft mit, dass die Erfassung beim BKA veranlasst worden sei. Da bei allen drei Betroffenen dieselben Umstände gegeben sind, also auch zum dritten Betroffenen keine Negativprognose gestellt werden konnte, habe ich angeregt, die Polizei nachträglich zu bitten, die Erfassung des dritten Betroffenen beim BKA rückgängig zu machen bzw. das DNA-Identifizierungsmuster dieses Betroffenen mangels Negativprognose nachträglich zu löschen. Die eventuell

gegenüber der Polizei erklärte Einwilligung des Betroffenen ersetzt nicht die erforderliche Negativprognose.

Meine anlassunabhängigen Kontrollen werde ich fortführen.

8.3 Reihengentest nach § 81h StPO in Dresden und Umgebung zur Suche nach einem Sexualverbrecher

Der größte Massentest der deutschen Kriminalgeschichte findet derzeit in Dresden und einigen nördlich angrenzenden Gemeinden statt: Mehr als 120.000 Männer, die bestimmte, auf einen gesuchten Täter vermutlich zutreffende Kriterien erfüllen (hier: Körpergröße, Wohnort, Alter) werden seit Mitte Juli 2006 durch die Polizei um die freiwillige Abgabe einer Speichelprobe ersucht. Diese wird anschließend molekulargenetisch untersucht und mit der Täter-DNA aus zwei Sexualverbrechen abgeglichen. Diese Maßnahme war von der Staatsanwaltschaft Dresden im Mai und Juni 2006 beantragt und durch das zuständige Amtsgericht beschlossen worden, nachdem die sehr intensiv geführten „konventionellen“ polizeilichen Ermittlungen bis dahin nicht zur Ergreifung des Täters geführt hatten.

Gegen diese Ermittlungsmaßnahme habe ich keine Einwände, was die erforderliche verfassungsgemäße gesetzliche Grundlage angeht. Denn seit dem 1. November 2005 war mit dem in die Strafprozessordnung eingefügten § 81h StPO die von Seiten des Datenschutzes lange zuvor geforderte bereichsspezifische gesetzliche Grundlage für Reihengentests geschaffen worden. Danach dürfen Personen, die bestimmte, auf den Täter vermutlich zutreffende Prüfungsmerkmale erfüllen, mit ihrer schriftlichen Einwilligung Körperzellen entnommen, diese molekulargenetisch untersucht und mit der Täter-DNA abgeglichen werden, soweit dies zur Feststellung erforderlich ist, ob das Spurenmaterial von diesen Personen stammt. Voraussetzung ist des Weiteren eine bestimmte Anlasstat, ein richterlicher Beschluss und die Verhältnismäßigkeit der Maßnahme. Diese Voraussetzungen waren vorliegend erfüllt. Ich gab jedoch zu bedenken, dass es sinnvoll und grundrechtsschonend erscheine, anhand bestimmter Kriterien von vornherein den Reihengentest in „konzentrischen Kreisen“ - nicht unbedingt nur örtlich, sondern auch qualitativ zu verstehen - stattfinden zu lassen. Allerdings ließ der amtsrichterliche Beschluss das von den Ermittlern gewählte Verfahren nach örtlichen Kriterien durchaus zu.

Da für mich das „Ob“ der Maßnahme aufgrund der Gesetzeslage außer Frage stand, konnte ich mich auf die Fragen des „Wie“ konzentrieren: Wie wird die gesetzlich

vorgesehene Freiwilligkeit der Teilnahme der Betroffenen gewährleistet? Und: Wie wird der Datenschutz technisch-organisatorisch gewährleistet?

Mit der Durchführung des Reihengentests wurde das LKA Sachsen beauftragt. Die inzwischen dort angesiedelte Sonderkommission lädt nach und nach jeweils mehrere tausend Betroffene aus bestimmten Postleitzahlenbezirken zunächst schriftlich zur Teilnahme am Reihengentest ein. Dem Anschreiben werden mittlerweile ein Blatt mit häufig gestellten Fragen (FAQ's) sowie ein Einwilligungsformular beigefügt. An der Erstellung dieser Texte war ich beteiligt; meinen Anregungen und Formulierungsvorschlägen ist zunehmend gefolgt worden. Den Betroffenen werden sodann mittels Wattestäbchen Mundschleimhautzellen entnommen. Diese werden durch ein beauftragtes Untersuchungsinstitut in einer Art und Weise, die technisch keinen Abgleich mit der Straftäter-DNA-Datei beim BKA zulässt, molekulargenetisch „verformelt" und sodann im LKA mit der Täter-DNA abgeglichen.

Die gesetzlich vorgesehene Freiwilligkeit der Teilnahme ist ein hohes Gut. § 81h StPO regelt eine Ermittlungsmaßnahme, die sich - mit der eventuellen Ausnahme des Täters - gegen absolut Nicht-Tatverdächtige, gegen *Menschen, gegen die nicht der geringste Verdacht besteht*, richtet. Anders ausgedrückt: Von z. B. 100.000 Teilnehmern haben 99.999 oder möglicherweise sogar 100.000 nichts mit der Tat zu tun. Deshalb ist die absolute Freiwilligkeit das wesentliche Prinzip dieser Maßnahme. Sie ergibt sich aus dem Prinzip, dass niemand staatlichen Zwangsmaßnahmen unterzogen werden darf, der hierfür nicht Anlass gegeben hat. Die Freiwilligkeit der Teilnahme ist jedoch tatsächlich in zweierlei Hinsicht gefährdet:

Zum einen darf durch die bloße „Verweigerung" der Teilnahme keinerlei Verdacht entstehen. Wer ernstlich erklärt hat, nicht teilnehmen zu wollen, braucht sich keinem auch noch so sanftem Druck ausgesetzt sehen. Damit unvereinbar ist die Erzeugung öffentlichen Drucks auf „Verweigerer" durch Äußerungen in der Boulevardpresse, die sinngemäß lauteten: „Wer nicht teilnimmt, den werden wir besuchen, Ihre Polizei". Damit unvereinbar sind missverständliche Hinweise auf die mögliche Erwirkung von Gerichtsbeschlüssen zur zwangsweisen Durchsetzung der Entnahme von Körperzellen nach anderen strafprozessualen Vorschriften. Damit unvereinbar sind schließlich im Einzelfall wegen ihrer Lästigkeit schon zwangsähnliche, wiederkehrende telefonische oder mündliche polizeiliche Aufforderungen zur Teilnahme. Zu alldem hat der BGH zur früheren Rechtsgrundlage von Reihengentests bereits vor Jahren festgestellt: Die Weigerung, an einem Reihengentest teilzunehmen, darf nicht als belastendes Beweisanzeichen gewertet werden (BGHSt 49, 56 = NStZ 2004, 392). Nur durch die Nichtteilnahme darf keinerlei Verdacht entstehen - ein Prinzip, das zu

akzeptieren manchem Staatsanwalt oder Polizisten möglicherweise schwerfallen mag. Der Reihengentest muss aber ein Ausschlussverfahren, kein Verfahren zur Erzeugung von Verdachtsmomenten sein.

Zum anderen muss jeder Teilnehmer genau wissen, in was er einwilligt. Nur wer alle Konsequenzen seiner Teilnahme kennt, kann selbstbestimmt entscheiden und „informiert“ einwilligen. Deshalb habe ich von Anfang an großen Wert auf die Formulierung der Einwilligungserklärung und die sonstigen Maßnahmen zur Unterrichtung der Betroffenen gelegt. Nachdem das LKA zur ersten Reihengentest-Veranstaltung schriftlich eingeladen hatte, zeigten sich Betroffene darüber verwundert, dass nicht auf die absolute Freiwilligkeit der Abgabe der Speichelprobe hingewiesen worden sei. Dies kritisierte ich gegenüber den Strafverfolgungsbehörden. In der Folge habe ich gemeinsam mit der Staatsanwaltschaft Dresden und dem LKA einen Katalog von häufig gestellten Fragen samt Antworten („FAQ“-Katalog) zum technischen Verfahren, zu Konsequenzen von Teilnahme oder Nichtteilnahme sowie einer möglichen Belastung von Verwandten, die ein mit der Täter-DNA in Teilen identisches DNA-Muster aufweisen, erarbeitet. Dieser sollte künftigen Einladungsschreiben beigefügt werden. Leider verwendete das LKA für die Einladung zu Ersatzterminen der ersten Großveranstaltung zunächst die bereits von mir kritisierten Schreiben und unterließ wiederum, auf die Freiwilligkeit der Maßnahme hinzuweisen. Dies veranlasste mich zu verstärkter Kritik. Die danach für die folgenden Veranstaltungen verwendeten Einladungsschreiben waren schließlich nicht mehr zu beanstanden. Sie bestanden aus einem Anschreiben, das deutlich auf die Freiwilligkeit des Tests hinwies, aus Erläuterungen, die dem FAQ-Katalog entnommen worden waren und dem Hinweis auf die Homepage des Landeskriminalamtes (www.lka.sachsen.de), auf der nach wie vor weitere Hinweise zum Verfahren und der gesamte FAQ-Katalog eingesehen werden können. Derzeit habe ich nichts gegen das verwendete Anschreiben, den FAQ-Katalog und die Einwilligungserklärung einzuwenden.

Außerdem legte ich Wert darauf, dass das konkrete Verfahren der Polizei in technisch-organisatorischer Hinsicht möglichst datenschutzgerecht gestaltet wurde. Die molekulargenetische Untersuchung wird durch ein beauftragtes Untersuchungsinstitut durchgeführt. Das Verfahren erscheint derzeit datenschutzgerecht. Die entnommenen Körperzellen werden ausschließlich für diesen Reihengentest verwendet und unmittelbar nach der „Verformelung“ vernichtet. Die Verformelung kann aus technischen Gründen - wegen des verwendeten Verfahrens - nicht mit der DNA-Datenbank des BKA, die ausschließlich Täterdaten bzw. Tatspuren enthält, abgeglichen werden. Sie wird nicht für andere oder künftige Strafverfahren verarbeitet. Die im Reihengentest erhobenen personenbezogenen Daten werden in einer separaten, von

anderen polizeilichen Informationssystemen getrennten Datenbank gespeichert. Sie sind nach Abschluss des Verfahrens unverzüglich zu löschen. Von dem datenschutzgerechten Ablauf der Untersuchung der Speichelprobe sowie des Abgleichs und der Verarbeitung der personenbezogenen Daten der Betroffenen in einer separaten Datenbank konnte ich mich bei Besuchen im LKA überzeugen.

Durch die ermittlungsführende Staatsanwaltschaft Dresden und das LKA Sachsen wurde ich früh informiert und mit einbezogen. Dafür danke ich. Ich werde den Reihengentest, der derzeit noch keine 10% der Betroffenen erfasst hat, die nächsten Jahre aufmerksam weiter begleiten, ist er doch sowohl hinsichtlich der Risiken und Möglichkeiten der Methode als auch der Verfahrensweise für zukünftige Massentests wegweisend.

8.4 Akten aus dem Staatsarchiv in der Hauptverhandlung - Ein Verstoß gegen § 51 BZRG

Ein Vertreter einer sächsischen Staatsanwaltschaft hatte in einer Hauptverhandlung im Jahr 2006 dem zuständigen Amtsgericht Unterlagen über Verurteilungen des Angeklagten aus den Jahren 1979 und 1984 (!) vorgelegt, die laut Hauptverhandlungsprotokoll in das Verfahren eingeführt wurden. Die Staatsanwaltschaft bestritt eine formelle Einführung der Akten in das Verfahren und teilte mit, der Angeklagte habe auf Frage ihres Vertreters die früheren Verurteilungen eingeräumt. Die Unterlagen stammten aus dem Staatsarchiv. Der aktuelle Bundeszentralregisterauszug des Angeklagten enthielt die Verurteilungen aus den Jahren 1979 und 1984 nicht mehr.

Das Vorgehen der Staatsanwaltschaft verstieß gegen § 51 BZRG, wonach dem Betroffenen eine frühere Tat und die Verurteilung im Rechtsverkehr nicht mehr vorgehalten und zu seinem Nachteil nicht mehr verwertet werden darf, wenn die Eintragung der Verurteilung im Bundeszentralregister getilgt wurde oder zu tilgen ist. In der datenschutzrechtlichen Terminologie verbietet § 51 Abs. 1 BZRG mithin das Nutzen oder Übermitteln der Einzelangaben über Verurteilungen ab dem im Bundeszentralregistergesetz näher bestimmten Zeitpunkt. Irrelevant ist dabei, in welcher Form entsprechende Informationen verwertet werden. Es ist ohne Bedeutung, ob Akten zu früheren, im Bundeszentralregister getilgten Verfahren gemäß § 249 StPO formell in das Verfahren eingeführt werden oder nicht. Vorliegend wies das Hauptverhandlungsprotokoll eine Einführung der alten Verfahren in das aktuelle Verfahren aus, die Staatsanwaltschaft bestritt dagegen eine formelle Einführung nach § 249 StPO. Fraglich, aber letztlich unmaßgeblich ist, ob nicht bereits die - wie auch immer formulierte - Frage nach früheren, inhaltlich dem aktuellen vergleichbaren Verfahren

ein Vorhalten im Sinne von § 51 Abs. 1 BZRG ist. Die Erwähnung früherer Verfahren in der Hauptverhandlung sowie die Übergabe der Verfahrensakten an das Gericht stellten jedenfalls eine Verwertung im Sinne von § 51 Abs. 1 BZRG dar.

Den Verstoß gegen § 51 BZRG habe ich gegenüber dem SMJus beanstandet.

8.5 Behandlung von unfrankierten, nicht gekennzeichneten Briefen in öffentlichen Stellen

Ein Petent teilte mir mit, dass ein von ihm verfasster und an eine Stelle außerhalb Sachsens adressierter Brief in der Poststelle eines Gerichts geöffnet worden sei. Der zum Sachverhalt befragte Mitarbeiter der Poststelle teilte mit, dass der Briefumschlag keinen Absender habe erkennen lassen und unfrankiert gewesen sei, als er auf dem Tresen der Poststelle aufgefunden worden sei. Der Umschlag sei schließlich geöffnet worden, um Hinweise auf den Absender zu erhalten. Das Schreiben selbst sei nicht gelesen worden. Mehrere Versuche der Poststelle, Kontakt mit dem Absender aufzunehmen, wären fehlgeschlagen, so dass letztlich der Brief durch die Poststelle an den Absender zurückgeschickt worden sei.

Datenschutzrechtlich bewerte ich den Sachverhalt wie folgt: Das Öffnen eines Briefes, dessen Absender oder Adressat nicht die öffentliche Stelle ist, in deren Poststelle sich der Brief befindet, greift in das Briefgeheimnis ein (Art. 10 GG; Art. 27 SächsVerf). Ist die Stelle nicht offenkundig die Stelle, zu deren Kenntnis der Brief bestimmt ist, darf sie den Brief nicht öffnen, sofern sie nicht anderweitig befugt ist. Der über die Kenntnisnahme Bestimmende ist der Verschließende, bei Sendungen wird der Adressat Bestimmender, sobald die Sendung in seinen Gewahrsam gelangt ist (vgl. § 202 StGB). Im vorliegenden Fall sah ich keine gesetzliche Befugnis der Poststelle, den Brief, der ersichtlich an eine andere Stelle adressiert war, zu öffnen. Angesichts der guten Absicht der Poststelle, durch das Öffnen des Briefes den Absender zu erkennen und diesen zu informieren, und dem behaupteten Umstand, dass das Schreiben nicht gelesen worden sei, habe ich von einer Beanstandung abgesehen.

Ich empfehle, derartige Schreiben künftig als „Fundsache“ zu behandeln und ungeöffnet in einer Ablage aufzubewahren. Eine solche Behandlung führt weder zu zusätzlichen Kosten noch setze sie die Mitarbeiter der Gefahr aus, sich nach § 202 StGB (Verletzung des Briefgeheimnisses) strafbar zu machen.

8.6 Auskünfte an den Anzeigeerstatter, der auch Nebenkläger ist

Ein Petent teilte mir mit, dass er ein im Rahmen eines Ermittlungsverfahrens gegen ihn erstelltes Schreiben einer Staatsanwaltschaft an einen Dritten in einem Internetforum eingescannt vorgefunden habe. In dem Schreiben hätte die Staatsanwaltschaft dem Dritten die Auskunft erteilt, dass er, der Petent, sich „z. Z. in stationär medizinischer Behandlung“ befände und „in einer anderen Sache (…) ein Gutachten zur Klärung der Schuldfähigkeit angefordert (worden sei)“. Es müsse abgewartet werden, „wie die Ermittlungen mit seiner Erkrankung zu vereinbaren“ seien.

Meine Kontrolle ergab Folgendes: In dem gegen den Petenten geführten Ermittlungsverfahren war der Dritte der Anzeigeerstatter. Dieser hatte zugleich gegenüber der Staatsanwaltschaft erklärt, sich dem Verfahren als Nebenkläger anzuschließen. Die Abgabe einer solchen Anschlusserklärung ist in jeder Lage des Verfahrens zulässig, § 395 Abs. 4 und § 396 Abs. 1 StPO. Wegen dieser Anschlusserklärung des Anzeigeerstatters richtete sich sein Recht auf Auskunft aus dem Ermittlungsverfahren gegen den Beschuldigten (den Petenten) nach § 406e Abs. 1 und 5 StPO. Danach hat der Nebenkläger einen Anspruch auf Erteilung von Auskünften aus der Ermittlungsakte, ohne dass er hierzu ein besonderes Interesse darlegen muss. Grund hierfür ist, dass die Strafprozessordnung dem Verletzten, der zugleich als Nebenkläger auftritt, allgemein gleiche Befugnisse wie den übrigen Prozessbeteiligten einräumt. Allerdings verpflichtet § 406e Abs. 2 StPO die Staatsanwaltschaft zu prüfen, ob Versagungsgründe vorliegen, welche der Auskunftserteilung entgegenstehen. Als Versagungsgrund sieht die Strafprozessordnung besondere schutzwürdige Interessen des Beschuldigten oder anderer Personen vor.

Grundsätzlich konnten dem Dritten daher Auskünfte aus dem Ermittlungsverfahren erteilt werden. Gleichwohl lag in der erfolgten Weitergabe ein datenschutzrechtlicher Verstoß vor. Es war nicht dokumentiert, ob und unter Einbeziehung welcher Tatsachen geprüft wurde, ob schutzwürdige Interessen des Beschuldigten oder Anderer entgegenstehen. Nach dem Grundsatz der Aktenvollständigkeit musste ich daher davon ausgehen, dass diese Prüfung nicht erfolgt war.

Die betreffende Staatsanwaltschaft hat den Fehler eingeräumt und will sicherstellen, dass sich solche Fehler nicht wiederholen.

Allgemein empfehle ich in Fällen, in welchen Informationen an Dritte herausgegeben werden sollen, die Betroffenen zuvor anzuhören. Der hiermit verbundene Aufwand ist minimal und sichert die Rechte der Betroffenen.

8.7 Aussonderung, Ablieferung und Vernichtung von Schriftgut in der Justiz

Meine im Berichtszeitraum begonnenen anlassunabhängigen Kontrollen sächsischer Staatsanwaltschaften haben u. a. ergeben, dass im Freistaat Sachsen keine wirksame Regelung für die Aufbewahrung und Aussonderung von Schriftgut der Justiz besteht.

Die ursprünglich vorhandene Verwaltungsvorschrift „VwV Aufbewahrung und Aussonderung“ vom 2. Februar 1999, geändert durch Verwaltungsvorschrift vom 14. Dezember 1999, war durch Zeitablauf außer Kraft getreten. Eine neue war nicht erlassen worden. Dieser Zustand war unhaltbar und rechtswidrig.

Ich hatte mich deswegen an das SMJus mit der Bitte um Abhilfe gewandt.

Auch dieses hatte die Unhaltbarkeit des bestehenden Zustandes erkannt und am 4. Januar 2007 eine entsprechende Verwaltungsvorschrift erlassen.

Ziel aller Bestrebungen muss jedoch eine bundeseinheitliche gesetzliche Regelung sein.

8.8 Gefängnisbesichtigungen und Gefangene

Eine Petentin wandte sich mit folgendem Vorgang an mich: Sie sei in einer sächsischen Justizvollzugsanstalt inhaftiert gewesen. Zu ihrem Tagesablauf habe unter anderem auch ein Aufenthalt im Freien gehört. Eines Tages habe eine Klasse Auszubildender die Justizvollzugsanstalt besichtigt. Zum Besichtigungsprogramm habe auch der Bereich im Freien, in dem sich die Gefangenen aufhielten, gehört, so dass die Gefangenen von den Besuchern hätten beobachtet werden können.

Ich habe der Petentin mitgeteilt, dass aus Sicht des Datenschutzes nichts gegen eine auch den Freibereich umfassende Besichtigung durch Klassen einzuwenden ist. Die damit an die Teilnehmer der Besichtigung zwangsläufig einhergehende Übermittlung des Umstandes, dass eine bestimmte Person Gefangener ist, ist durch das Strafvollzugsgesetz gedeckt. § 180 Abs. 1 Satz 1 StVollzG erlaubt der Justizvollzugsanstalt die Verarbeitung und Nutzung personenbezogener Daten von Gefangenen, wenn dies für den Vollzug der Freiheitsstrafe, gemeint ist der Vollzug von Haft im Allgemeinen, erforderlich ist.

Was für den Vollzug der Haft erforderlich ist, ergibt sich aus den §§ 2 ff. StVollzG und aus dem sich unmittelbar aus Art. 1 GG ergebenden Gebot eines menschen-

würdigen Justizvollzuges. Gerade zur Gewährleistung des letztgenannten Gesichtspunktes ist die Transparenz des Justizvollzuges nach innen und nach außen notwendig. Hierzu zählt auch die Möglichkeit, der Öffentlichkeit Eindrücke von der Vollzugsgestaltung und vom Leben im Vollzug zu vermitteln. Führungen durch die Justizvollzugsanstalt dienen der Schaffung dieses transparenten Justizvollzuges.

Selbstverständlich muss jedoch jede Besichtigung einer Justizvollzugsanstalt angemessen verlaufen. Die Kenntnisnahme von der Vollzugsgestaltung und dem Leben im Vollzug darf nicht in Voyeurismus ausarten. Deswegen darf keine Justizvollzugsanstalt es ermöglichen, dass Gefangene gegen ihren Willen gezielt über einen längeren Zeitraum bei ihrer Beschäftigung beobachtet werden, zumal dies zur Erreichung des Zieles eines nach Außen transparenten Vollzugs nicht erforderlich wäre.

Festzustellen bleibt anhand dieses Beispiels: Das Datenschutzrecht soll nicht verhindern, dass überhaupt personenbezogene Daten verarbeitet werden. Vielmehr soll der Einzelne und sein Recht auf informationelle Selbstbestimmung nach den Maßstäben des Bundesverfassungsgerichts durchaus eingeschränkt werden dürfen, wenn dies im überwiegenden Allgemeininteresse liegt, eine klare gesetzliche und in sich verfassungsgemäße Grundlage vorhanden und technisch-organisatorische Vorkehrungen zum Schutz des Grundrechts auf Datenschutz getroffen worden sind.

8.9 Datenschutz in der Zwangsvollstreckung - Zustellungen durch Gerichtsvollzieher

Ein Schuldner in einem zivilrechtlichen Verfahren wandte sich an mich, weil er mit der Art und Weise der Zustellung eines Gerichtsbeschlusses durch den zuständigen Gerichtsvollzieher nicht einverstanden war.

Der Gerichtsvollzieher hatte eine beglaubigte Abschrift des Gerichtsbeschlusses im Wege der Ersatzzustellung offen ohne Umschlag an einen Angestellten des Drittschuldners, seines Arbeitgebers, ausgehändigt. Angeblich seien gerade keine Umschläge verfügbar gewesen.

Die ersatzweise Zustellung an den Angestellten des Drittschuldners war gemäß § 178 Abs. 1 Nr. 2 ZPO, §§ 29 Nr. 1, 30 Nr. 2 GVGA zulässig. Im Falle einer solchen Ersatzzustellung bedarf es keiner schriftlichen Vollmacht der im Geschäft des Drittschuldners beschäftigten Person.

Unzulässig ist dagegen die offene Übergabe der Abschrift des Gerichtsbeschlusses. Zwar ist nach § 36 Abs. 3 Satz 4 GVGA eine offene Übergabe des zuzustellenden

Schriftstücks zulässig, wenn die Ersatzzustellung mit der Aufforderung zur Abgabe der Erklärung nach § 840 Abs. 1 ZPO (Drittschuldnererklärung) verbunden wird *und* der Ersatzempfänger zur Abgabe der Erklärung bereit ist oder sich an die Zustellung sofort eine Vollstreckungshandlung anschließt; hier jedoch hat solch eine Konstellation nicht vorgelegen. Eine Person, der ersatzweise zugestellt wird, die aber - wie vorliegend der Angestellte des Drittschuldners - nicht gesondert bevollmächtigt oder vertretungsberechtigt ist, verfügt regelmäßig weder über die für die Abgabe der Erklärung notwendigen Kenntnisse noch über die Befugnis, für den Drittschuldner eine Erklärung nach § 840 ZPO abzugeben. Unter diesen Umständen hätte die beglaubigte Abschrift des Gerichtsbeschlusses gemäß § 36 Abs. 3 Satz 1 GVGA zwingend in einem verschlossenen Umschlag übergeben werden müssen, so dass eine Einsichtnahme ohne Öffnung nicht möglich gewesen wäre. Es geht den Ersatzempfänger in diesen Fällen eben gerade nichts an, welchen Inhalt die zuzustellenden Schriftstücke haben. Er soll diese lediglich an den Zustellungsadressaten weiterleiten. Dieses Vorgehen dient nicht zuletzt dem Schutz des Rechts der Verfahrensbeteiligten auf informationelle Selbstbestimmung. Es gehört zu den Dienstpflichten von Gerichtsvollziehern, Briefumschläge oder anderes Material vorrätig zu halten, um eine gesetzmäßige Aufgabenerfüllung zu gewährleisten.

Das zuständige Amtsgericht teilte meine Auffassung. Es wertete den Sachverhalt gemeinsam mit dem Gerichtsvollzieher aus und belehrte diesen, die datenschutzrechtlichen Bestimmungen auch im Rahmen der Zwangsvollstreckung künftig einzuhalten. Aufgrund dessen habe ich von einer Beanstandung abgesehen.

8.10 Verwendung von Verteidigerpost im Maßregelvollzug ohne Einverständnis des Patienten

Ein Petent im Maßregelvollzug teilte mir mit, dass die Klinik gegenüber dem zuständigen Gericht aus einem an ihn gerichteten Schreiben seines Verteidigers zitiert habe. Weder er selbst noch sein Verteidiger seien durch die Klinik davon in Kenntnis gesetzt worden, dass diese über das Verteidigerschreiben verfügt hätte.

Die Klinik teilte mit, dass der Petent eigenhändig Korrespondenz offen im Abfall der Station entsorgt habe, ohne diese vorher - etwa durch Zerreißen - unleserlich gemacht zu haben. Ein anderer Patient habe die Unterlagen gefunden und dem Personal übergeben. Das Schreiben sei zur Akte des Petenten genommen und für die Stellungnahme verwendet worden. Man sei davon ausgegangen, dass dies rechtmäßig gewesen sei und datenschutzrechtliche Vorschriften nicht verletzt worden seien.

Dies trifft nicht zu. Grundsätzlich darf der Schriftwechsel des Patienten mit seinem Verteidiger nach § 26 SächsPsychKG nicht überwacht werden. In dieser Hinsicht ist der Patient im Maßregelvollzug einem Strafgefangenen gleichgestellt. Das Vertrauensverhältnis zwischen dem im Maßregelvollzug untergebrachten Patienten und seinem Verteidiger ist gesetzlich besonders geschützt, um ein faires, rechtsstaatliches Verfahren zu gewährleisten. Dies drückt sich auch in der Dienstanweisung „Datenschutz im Maßregelvollzug“ des SMS aus. Danach darf „Schriftwechsel des Patienten (…) grundsätzlich nicht gelesen und angehalten werden, es sei denn, es liegen die Voraussetzungen von § 26 Abs. 4 SächsPsychKG vor“. Es sei „nicht zulässig, die Korrespondenz des Patienten, Ablichtungen von ihr oder Vermerke über diese für die Krankenunterlagen zu nehmen, es sei denn, der Patient stimmt dem zu oder es liegen die Voraussetzungen von § 26 Abs. 4 Satz 3 SächsPsychKG vor. Die Weitergabe von Erkenntnissen aus dem Schriftwechsel ist grundsätzlich verboten. Ausnahme hiervon ist eine Verwertung der Erkenntnisse, wenn die Voraussetzungen von § 28 SächsPsychKG vorliegen“. Zum Verhältnis von Schweigepflicht und Übermittlung von Patientendaten äußert sich die Dienstanweisung dahingehend, dass die Schweigepflicht auch für Stellungnahmen und Gutachten gegenüber der vollstreckenden Staatsanwaltschaft und der Strafvollstreckungskammer gilt. Erfordere eine sachgerechte Stellungnahme die Offenbarung eines Patientengeheimnisses, ist Voraussetzung, dass der Patient den Gutachter insoweit von der Schweigepflicht entbunden hat.

Die gesetzlich vorgesehenen Ausnahmefälle, in denen Verteidigerpost überwacht und darin enthaltene Informationen verarbeitet werden dürfen, sind gegeben, wenn tatsächliche Anhaltspunkte für eine erhebliche Gefährdung der Sicherheit oder Ordnung des Krankenhauses oder der Allgemeinheit vorliegen. Dies war vorliegend - auch nach Auffassung der Klinik - nicht der Fall.

Nachdem ich die Klinik auf die Rechtslage, insbesondere auf die einschlägige Dienstanweisung, die den handelnden Bediensteten offenbar nicht geläufig war, hingewiesen hatte, räumte sie ein, dass die Verarbeitung des Verteidigerschreibens rechtswidrig gewesen sei. Der Leiter der Einrichtung ging davon aus, dass der Vorfall ein einmaliges Ereignis bleibe. Er habe den Eindruck, dass den Bediensteten in hohem Maße bewusst sei, dass das Verhältnis zwischen Verteidiger und Patient einem besonderen Schutz unterliege und sicherte zu, dass sich ein solcher Vorgang unter seiner Leitung der Klinik so nicht wiederholen werde. Von einer förmlichen Beanstandung habe ich daher gerade noch abgesehen.

8.11 Kontrolle von Abgeordnetenpost im Justizvollzug

Von einem Staatsanwalt wurde ich gefragt, unter welchen Voraussetzungen die Post eines Abgeordneten an einen Untersuchungsgefangenen zu Überwachungszwecken geöffnet werden dürfte.

Der Schriftwechsel zwischen Gefangenen und Volksvertretungen des Bundes und der Länder sowie deren Mitgliedern, dem Europäischen Parlament und dessen Mitgliedern, den Datenschutzbeauftragten des Bundes und der Länder und einigen anderen Stellen wird nach § 29 Abs. 2 StVollzG nicht überwacht. Dieser Grundsatz gilt auch für die Post von Untersuchungsgefangenen. Nach § 119 Abs. 3 StPO dürfen dem Verhafteten nur solche Beschränkungen auferlegt werden, die der Zweck der Untersuchungshaft oder die Ordnung in der Vollzugsanstalt erfordert. Nach Nr. 30 Abs. 2 der Untersuchungshaftvollzugsordnung dürfen Schreiben der Gefangenen an die Mitglieder der o. g. Volksvertretungen nicht überwacht werden, wenn die Schreiben an die Anschriften der Volksvertretungen gerichtet sind und den Absender zutreffend angeben. Auch wenn in der Untersuchungshaftvollzugsordnung nicht - wie im Strafvollzugsgesetz - ausdrücklich geregelt ist, dass auch Schreiben von Abgeordneten an den Untersuchungsgefangenen nicht kontrolliert werden dürfen, ist kein Grund ersichtlich, die in den Justizvollzugsanstalten eingehende Post von Mitgliedern der o. g. Volksvertretungen an Gefangene in Untersuchungshaft anders als an Gefangene in Straf- oder einer anderen Haft zu beurteilen.

8.12 Übermittlung von Gesundheitsdaten Gefangener durch die JVA an ein Gericht zum Schutz der Justizbediensteten

Darf eine Justizvollzugsanstalt der Polizei oder Justizbediensteten, die einen Gefangenen z. B. zur Vorführung bei Gericht übernehmen, offenbaren, dass der Gefangene an einer gefährlichen Krankheit (z. B. Tuberkulose, Hepatitis oder AIDS) leidet? Oder stehen die Schweigepflicht des Anstaltsarztes oder praktische Erwägungen einer Offenbarung entgegen? Ich habe mehreren Justizangehörigen auf deren Fragen wie folgt geantwortet:

Das Recht des Gefangenen auf informationelle Selbstbestimmung, das sich u. a. in der ärztlichen Schweigepflicht ausdrückt, genießt keinen Vorrang vor dem Recht der Justizbediensteten oder anderer Dritter auf körperliche Unversehrtheit. Vielmehr sind beide Grundrechte in einen sinnvollen Ausgleich zu bringen. Der Bundesgesetzgeber hat in dem derzeit in Sachsen noch geltenden Strafvollzugsgesetz dafür mit den §§ 179 ff. StVollzG einen verfassungsrechtlich unbedenklichen Rahmen geschaffen.

Nach § 182 Abs. 3 StVollzG ist die zweckändernde Übermittlung von Gesundheitsdaten Gefangener durch die JVA an das Gericht sowohl im Hinblick auf Informationen, die der ärztlichen, zahnärztlichen, apothekerlichen etc. Schweigepflicht unterfallen, als auch im Hinblick auf Informationen, die der Gefangene dem Vollzugspersonal selbst mitgeteilt hat oder die offenkundig sind, zulässig, wenn

- dies zur Abwehr von erheblichen Gefahren für Leib oder Leben eines Dritten (z. B. eines Justizbediensteten) *erforderlich* ist,

- es im Einzelfall tatsächliche Anhaltspunkte für eine erhebliche Gefahr für Leib oder Leben eines Dritten (z. B. eines Justizbediensteten) gibt,

- die Übermittlung im Einzelfall auf das zur Abwehr der Gefahr Erforderliche, d. h. in der Regel auf die Mitteilung der erforderlichen Schutzmaßnahmen, beschränkt wird und

- technisch-organisatorische Vorkehrungen zum Schutz des Grundrechts auf informationelle Selbstbestimmung, hier insbesondere zum Schutz gegen zweckändernde Weiterverarbeitungen, getroffen worden sind.

Im Einzelnen:

Hat der Anstaltsleiter Kenntnis von der Krankheit eines Gefangenen durch nach § 203 Abs. 1 Nr. 1, 2 oder 5 StGB schweigepflichtige Personen (z. B. dem Anstaltsarzt) erlangt, so darf er oder ein durch ihn bestimmter Bediensteter die Gesundheitsdaten wiederum nur unter den Voraussetzungen des § 182 Abs. 3 StVollzG an Dritte, z. B. Gerichte, offenbaren. Danach ist die Offenbarung durch den Anstaltsleiter unter denselben Voraussetzungen zulässig, unter denen ein nach § 203 Abs. 1 Nr. 1, 2 oder 5 StGB Schweigepflichtiger hierzu befugt wäre. Eine solche Befugnis wäre nach § 182 Abs. 2 Satz 2 bis 4 StVollzG u. a. dann gegeben, wenn die Offenbarung „zur Abwehr von erheblichen Gefahren für Leib oder Leben (…) Dritter“ *erforderlich* ist. Erforderlich in diesem Sinne heißt, dass die Aufgabe, hier die Abwehr von erheblichen Gefahren für Leib oder Leben Dritter, ansonsten nicht, nicht rechtzeitig oder nicht vollständig erfüllt werden könnte. Die Offenbarungsbefugnis des Anstaltsleiters oder eines durch ihn bestimmten Bediensteten ergibt sich mithin unmittelbar aus § 182 Abs. 3 StVollzG, da diese Vorschrift im Hinblick auf den gefährdeten „Dritten“ nicht danach unterscheidet, ob es sich um einen Bediensteten der JVA oder eine andere Person, z. B. einen Justizbediensteten, handelt.

Nach der Kommentarliteratur darf ein Anstaltsleiter, wenn ein infizierter Gefangener an eine Polizeidienststelle übergeben wird, die Tatsache der Infektion der ihn übernehmenden Polizeidienststelle bekannt geben. Dabei brauche bei ansteckenden Krankheiten wie AIDS oder Hepatitis im Regelfall nicht die Art der Infektion oder Erkrankung des Gefangenen bekannt gegeben zu werden. Es müsse lediglich auf die Übertragungsgefahr einer ansteckenden Krankheit durch den Vermerk „Blutkontakt vermeiden“ an deutlich sichtbarer Stelle im Innern der Akte oder auf der Rückseite des Transportscheins hingewiesen werden. Der Stempelaufdruck „Blutkontakt vermeiden“ in Akten oder Transportpapieren setze nach OLG Koblenz NStZ 1988, 480 = ZfStrVO 1989, 121 voraus, dass der Gefangene tatsächlich infektiös erkrankt ist (Schmid in: Hans-Dieter Schwind/Alexander Böhm, Strafvollzugsgesetz, Kommentar, 3. Aufl. 1999, § 182, Rdnr. 19). Im Hinblick auf die mit der Vorführung des Gefangenen zu gerichtlichen Terminen betrauten Justizbediensteten wird vertreten, dass der Anstaltsarzt zur Offenbarung einer ansteckenden Krankheit verpflichtet sei (Schmid in: Hans-Dieter Schwind/Alexander Böhm, Strafvollzugsgesetz, Kommentar, 3. Aufl. 1999, § 182, Rdnr. 12).

Auf § 180 Abs. 2 Nr. 3 StVollzG kommt es nicht an. Doch selbst wenn man die Offenbarung von Gesundheitsdaten eines Gefangenen durch den Anstaltsleiter an das Gericht zum Zwecke der Abwehr von erheblichen Gefahren für Leib oder Leben der Justizbediensteten als Änderung des ursprünglichen Zwecks der Offenbarung ansähe, käme man über § 180 Abs. 2 Nr. 3 StVollzG zu keinem anderen als dem o. g. Ergebnis. Denn zu den Rechten einer anderen Person im Sinne von § 180 Abs. 2 Nr. 3 StVollzG zählt u. a. das Recht auf körperliche Unversehrtheit, wobei für eine schwere Beeinträchtigung dieses Rechts konkrete Anhaltspunkte vorliegen müssen, Schmid in: Hans-Dieter Schwind/Alexander Böhm, Strafvollzugsgesetz, Kommentar, 3. Auflage 1999, § 180, Rdnr. 15.

Gesundheitsdaten von Gefangenen, die ursprünglich nicht der ärztlichen Schweigepflicht unterliegen - etwa da der Gefangene außerhalb eines Arzt-Patienten-Gesprächs seine Mitgefangenen oder die Vollzugsbediensteten über eine Erkrankung unterrichtet oder gar damit gedroht hat - dürfen unter den Voraussetzungen von § 180 Abs. 2 Nr. 3 StVollzG an Dritte, z. B. ein Gericht, übermittelt werden, soweit dies „zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte einer anderen Person“ erforderlich ist. Dazu, dass zu den Rechten einer anderen Person im Sinne von § 180 Abs. 2 Nr. 3 StVollzG u. a. auch deren Recht auf körperliche Unversehrtheit zählt, siehe oben.

Ob durch den konkreten Gefangenen eine erhebliche Gefahr für Leib oder Leben eines Justizbediensteten oder eine schwerwiegende Beeinträchtigung der Rechte eines Justizbediensteten drohen, hat der Anstaltsleiter oder ein durch ihn bestimmter Bediensteter nach den Umständen des Einzelfalles zu entscheiden. Unzulässig wäre die routinemäßige Übermittlung von Erkenntnissen über den Gesundheitszustand von Gefangenen, bei denen keine tatsächlichen Anhaltspunkte für eine Gefahr im Einzelfall bestehen. Solche *tatsächlichen Anhaltspunkte* können u. a. frühere Verhaltensweisen, Ankündigungen oder Drohungen des konkreten Gefangenen oder vollzugliche Erfahrungen, deren Wiederholungswahrscheinlichkeit an Sicherheit grenzt, sein. *Erheblich* sind Gefahren, die zu schwerwiegenden Erkrankungen der Justizbediensteten führen können. Ein grippaler Infekt des Gefangenen wird im Regelfall nicht ausreichen, wohl aber eine Tuberkulose-, Hepatitis- oder AIDS-Infektion oder eine schwerwiegende psychische Störung.

Inwieweit Gesundheitsdaten des Gefangenen offenbart werden dürfen, bemisst sich danach, welche Informationen die übernehmenden Justizbediensteten benötigen, um sich zu schützen. So darf im Regelfall nicht die konkrete Erkrankung, sondern nur die zu ergreifende spezifische Schutzmaßnahme mitgeteilt werden. Also nicht: „Tbc-Erkrankung“, sondern nur: Vorsicht vor dem Anhusten, Anspucken etc, generell vor einer Tröpfcheninfektion“. Oder: Nicht „AIDS-infiziert“, sondern nur: „Vorsicht vor Bissen, Kratzern, etc., generell vor dem Kontakt mit Körperflüssigkeiten“.

Falls eine Offenbarung von Gesundheitsdaten von Gefangenen nach diesen Maßstäben zulässig wäre, unterlägen sie bei Gericht einer strikten Zweckbindung. Die weitere oder unzulässige Verarbeitung der Gesundheitsdaten könnte den Straftatbestand des unbefugten Offenbarens nach § 203 Abs. 2 StGB erfüllen.

Generell zu bedenken ist - und hierauf machte das SMJus aufmerksam -, dass mit der Übermittlung von Gesundheitsdaten ein trügerisches Sicherheitsgefühl bei den Justizbediensteten entstehen kann. Dies ist ein tatsächliches, kein rechtliches Argument gegen eine Übermittlung, dem ich mich nicht ganz verschließen kann. In der Praxis könnte die Gefahr entstehen, dass Justizbedienstete den notwendig unvollständigen Informationen der Anstalt (es werden keine Reihenuntersuchungen in Gefängnissen durchgeführt) über den Gesundheitszustand eines Gefangenen derart vertrauen, dass sie erforderliche Schutzmaßnahmen ansonsten unterlassen oder zu lax handhaben.

Auch das künftige Sächsische Strafvollzugsgesetz wird nach derzeitigem Entwurfsstand keine anderen Regelungen schaffen.

8.13 Medikamentenausgabe im Justizvollzug

Die Erforderlichkeit von Daten zur Aufgabenerfüllung ist ein tragendes Prinzip des Datenschutzes. Nur wenn ohne die Kenntnis eines Datums die gesetzliche Aufgabe nicht, nicht vollständig oder nicht rechtzeitig erfüllt werden könnte, darf die öffentliche Gewalt etwas über den einzelnen Betroffenen wissen. Dies gilt in besonderer Weise unter den besonderen Bedingungen des Justizvollzuges auch für Gefangene. Sind Gefangene krank und bedürfen der Medikamentierung, so stellt sich daher die Frage, wie die Medikamentenausgabe organisiert ist. Datenschutzrechtlich problematisch könnte eine Beteiligung von allgemeinen Vollzugsbediensteten sein, wenn diese Kenntnis von konkreten Erkrankungen erhielten oder aus der Art der Medikamente entsprechende Rückschlüsse ziehen könnten, obwohl das Arztgeheimnis auch im Strafvollzug gilt.

Das SMJus teilte mir mit, dass Stationsbedienstete dann an der Medikamentenausgabe beteiligt würden, wenn diese nicht direkt durch den Arzt erfolge, Pflegepersonal nicht im Dienst sei oder aufgrund der spezifischen Problematik des verordneten Medikamentes oder des betroffenen Gefangenen die sofortige Einnahme unter Aufsicht erforderlich sei. Hierzu würden Medikamentenspender verwendet, die entsprechend der ärztlichen Verordnung durch das Pflegepersonal bestückt und an die jeweiligen Stationsbediensteten weitergeleitet würden. In den meisten sächsischen Justizvollzugsanstalten enthielten diese Medikamentenspender lediglich den Namen des Gefangenen, die Haftraumnummer sowie Datum und Uhrzeit der Einnahme, nicht jedoch die Bezeichnung des Medikamentes. In drei sächsischen Justizvollzugsanstalten seien dagegen die Medikamentenspender zusätzlich mit der konkreten Bezeichnung des Medikamentes versehen.

Letzteres halte ich für problematisch. Denn die Kenntnis der konkreten Erkrankung eines Gefangenen ist zur Aufgabenerfüllung des Vollzugspersonals nicht erforderlich. Der Gefangene ist in der Regel durch den Arztbesuch selbst informiert. Die korrekte Einnahme kann durch sorgfältige Bestückung gegebenenfalls mehrerer Medikamentenspender und deren unmissverständlicher Beschriftung bezüglich der Einnahmezeitpunkte sichergestellt werden. Dass eine derartige datenschutzgerechte Praxis möglich ist, zeigt zudem die Vorgehensweise in der überwiegenden Zahl der sächsischen Justizvollzugsanstalten. Der im Strafvollzug mögliche und durch § 182 StVollzG garantierte Grad des Schutzes gesundheitlicher Daten wird nicht unterschritten, wenn bei Verhinderung des Arztes oder des Pflegepersonals Stationsbedienstete Medikamente aus bereits bestückten Medikamentenspendern, auf denen der Name des Gefangenen, die Haftraumnummer sowie Datum und Uhrzeit der Ein-

nahme des Medikamentes, nicht aber dessen konkrete Bezeichnung vermerkt sind, an die Gefangenen ausgeben.

Das SMJus hat daraufhin die Justizvollzugsvollzugsanstalten gebeten, künftig - soweit allgemeine Vollzugsbedienstete an der Ausgabe beteiligt sind - ausschließlich Medikamentenspender zu verwenden, auf denen nicht der Name des Medikamentes vermerkt ist.

9 Wirtschaft und Arbeit

9.1 Straßenverkehrswesen

9.1.1 Kontrolle von Personal durch Aufsichtsbehörden nach dem Fahrpersonalgesetz

Ein Fuhrunternehmer fragte bei mir an, ob das Regierungspräsidium Chemnitz für eine Kontrolle berechtigt sei, unter anderem umfangreiche Personaldaten, einschließlich Anschrift und Geburtsdatum seines Fahrpersonals sowie bei Aushilfsfahrern auch das Erstarbeitsverhältnis mit lückenlosen Zeitnachweisen bei ihm zu erheben.

Anlass zur Prüfung von Unterlagen auf Einhaltung der Sozialvorschriften für das Fahrpersonal im Straßenverkehr des Fuhrbetriebes war die Ordnungswidrigkeitenanzeige einer Polizeidirektion gewesen, wie ich aus der Stellungnahme des Regierungspräsidiums Chemnitz erfuhr.

Ich habe dem Fuhrunternehmer mitgeteilt, dass die Aufsicht über die Ausführung der VO (EWG) Nr. 3820/95 und VO (EWG) Nr. 3821/85, des „Europäischen Übereinkommens über die Arbeit des im internationalen Straßenverkehrs beschäftigten Fahrpersonals“ (AETR) sowie des Fahrpersonalgesetzes und der aufgrund dieses Gesetzes erlassenen Rechtsverordnungen den von den Landesregierungen bestimmten Behörden/Aufsichtsbehörden (§ 4 Abs. 1 FPersG) obliegt. In Sachsen ist das Regierungspräsidium Chemnitz, Abt. Arbeitsschutz als Aufsichtsbehörde benannt (Verordnung der Sächsischen Staatsregierung über die Zuständigkeiten auf dem Gebiet des sozialen und medizinischen Arbeitsschutzes - SmAsZuVO vom 8. Juli 1993). In Ausübung dieser Aufsicht zur Durchführung des Gesetzes über das Fahrpersonal von Kraftfahrzeugen und Straßenbahnen (FPersG) fordert die Behörde auf der Grundlage des § 4 Abs. 3 FPersG Unterlagen zur Prüfung an. Dazu ist ebenfalls die Erteilung entsprechender Auskünfte (auch in schriftlicher Form) meist zwingend erforderlich. Die Verpflichtung zur Vorlage oder Einsendung von Unterlagen fällt nicht unter die Bestimmungen des § 4 Abs. 4 FPersG - Aussage- und Zeugnisverweigerungsrecht. Der Unternehmer, der Fahrzeughalter und die Mitglieder des Fahrpersonals, sowie die für dessen Einsatz in einem Unternehmen Verantwortlichen sind auskunftspflichtig, soweit dies erforderlich ist, um die Einhaltung der Sozialvorschriften zu überwachen (§ 4 Abs. 3 Satz 1 FPersG).

Zur Ausübung der Aufsichts- und Kontrollpflicht ist es erforderlich, einen lückenlosen Nachweis (fortlaufende Kilometerstände, detaillierte, personenbezogene Angaben zu den Arbeitszeiten der Kraftfahrer, Arbeitszeit-Urlaub-Krankheit usw.) der zu prüfenden Fahrer und Fahrzeuge von den Firmen zu erhalten. Ohne ausreichende

Identitätsangaben ist eine effektive Kontrolle der Sozialvorschriften nicht möglich (OLG Köln vom 29. November 1994, Ss478/94 (B)).

Eine Regelung für die datenschutzrechtliche Behandlung von Ordnungswidrigkeiten nach dem Fahrpersonalgesetz erfolgt durch § 10 FPersG. Dabei werden die zuständigen Behörden der Länder und das Bundesamt für Güterverkehr durch den Verweis auf § 9 in die Regelung mit einbezogen. Ohne Erhebung, Verarbeitung und Nutzung personenbezogener Daten wäre die notwendige Überwachung der Einhaltung der in § 2 FPersG genannten fahrpersonalrechtlichen Vorschriften nicht oder nicht im ausreichenden Maße möglich. Die Vorschrift wurde durch das Gesetz zur Änderung fahrpersonalrechtlicher Vorschriften vom 18. August 1997 (BGBl. I S. 2075) eingeführt.

Zu den von der Aufsichtsbehörde zulässig zu erhebenden und zu verarbeitenden personenbezogenen Daten gehören zum Beispiel Name, Anschrift und Geburtsdatum des betroffenen Fahrers sowie Arbeitgeber, Stellung im Betrieb sowie eventuell rechtskräftig geahndete Vorverstöße. Die zuständige Bußgeldbehörde darf die genannten Daten insoweit verarbeiten, als dies für die Erfüllung ihrer Aufgaben oder für die Zwecke der Beurteilung der Zuverlässigkeit des Unternehmens, bei dem der Betroffene angestellt ist, erforderlich ist.

Zur Erfüllung der Aufgaben einer Bußgeldbehörde ist der Rückgriff auf personenbezogene Daten auch erforderlich, um festzustellen, ob der Betroffene wiederholt in Erscheinung getreten ist. Ein Unternehmen hat nach Art. 14 Abs. 2 VO (EWG) Nr. 3821/85 (Kontrollgerät) die Schaublätter nach der Benutzung mindestens ein Jahr lang gut geordnet aufzubewahren. Gemäß Art. 15 Abs. 2 VO (EWG) 3820/85 sind die Unternehmer verpflichtet, die Originalschaublätter der Kraftfahrer in regelmäßigen Abständen zu kontrollieren. Zur Überprüfung des Verhaltens der Fahrer muss das Unternehmen die Schaublätter alsbald nach Beendigung der Fahrt auswerten. Die Schaublätter sind jedem Kontrollbeamten auf Verlangen vorzulegen oder auszuhändigen. Im Verweigerungsfall der Vorlage von entsprechenden Unterlagen hat die Behörde das Recht, gegen den Betroffenen ein Bußgeldverfahren einzuleiten. Nur durch einen lückenlosen Nachweis im Hinblick auf Kilometerstände der Fahrzeuge, aber auch der Arbeitszeiten von Kraftfahrern, ist der Aufsichtsbehörde die Überwachung der in Rede stehenden Sozialvorschriften, die eine Untersuchung von Tätigkeitsnachweisen weiter zurückliegender und längerer Zeiträume (anders bei Kontrollen auf der Straße) einschließt, beim Unternehmen möglich.

Zusammenfassend habe ich dem Fuhrunternehmer mitgeteilt, dass ich eine Verletzung datenschutzrechtlicher Bestimmungen nicht feststellen konnte. Die Datenerhebung und -verarbeitung durch das Regierungspräsidium Chemnitz war zulässig, sie erfolgte nach gesetzlichen Vorgaben, war formal in Ordnung.

Gleichwohl habe ich Verständnis für den anfragenden Unternehmer, der über Umfang, Tiefe und Ausmaß der Datenverarbeitung erstaunt war. Der Staat nötigt Bürgern und Unternehmen im Zuge einer allgemein zu beobachtenden Überregulierung im EU-Raum in vielen Ordnungsbereichen zunehmend Daten ab.

9.1.2 Der Geburtsname der Mutter ist keine Pflichtangabe gemäß § 111 OWiG

Ein Petent erkundigte sich, ob er verpflichtet sei, in einem Ordnungswidrigkeitenverfahren im Anhörungsbogen bei den Pflichtangaben („Angaben zu Ihrer Person“) auch das Feld für den Geburtsnamen seiner Mutter auszufüllen.

Ich habe ihm mitgeteilt, dass es dafür keine gesetzliche Grundlage gibt. Der Geburtsname der Mutter zählt insbesondere nicht zu den Pflichtangaben nach § 111 OWiG. Er ist in Ordnungswidrigkeitenverfahren zur Identifizierung überflüssig und eben gerade nicht erforderlich. In anderen Verwaltungsverfahren - etwa in bestimmten Antragsverfahren oder in Zuverlässigkeitsüberprüfungsverfahren - mag dies anders sein.

Die beteiligte Behörde habe ich aufgefordert, Anhörungsbögen, die das Feld „Geburtsname der Mutter“ im Bereich der Pflichtangaben enthalten, entweder nicht mehr zu verwenden oder deutlich darauf hinzuweisen, dass dieses Feld durch den Betroffenen nicht auszufüllen ist. Die Behörde sagte daraufhin zu, derartige (veraltete) Anhörungsbögen nicht mehr zu verwenden.

9.1.3 Lichtbilderabgleich in der Passbehörde

In einem Landratsamt war ein Ordnungswidrigkeitenverfahren wegen einer Geschwindigkeitsübertretung durch einen bis dahin unbekannten männlichen Fahrer, welcher auf einem Beweismittelfoto abgebildet war, anhängig. Die eingetragene Halterin des Tatfahrzeuges, die wegen ihres Geschlechts offensichtlich als Täterin ausschied, erkannte auf dem Foto einen Verwandten und machte von ihrem Zeugnisverweigerungsrecht Gebrauch.

Im Zuge der weiteren Ermittlungen wandte sich das Landratsamt an die Meldestelle, welche zugleich Passstelle war, und ließ sich die Daten nebst Passfotos der in Frage

kommenden männlichen Personen aus dem Umfeld der Halterin - Mitbewohner und Verwandte - übermitteln. Die so erhobenen Daten, insbesondere aber der Abgleich der übermittelten Passbilder mit der auf dem Beweisfoto abgebildeten Person, führte das Landratsamt zum Sohn der Halterin. Gegen ihn wurde das Ordnungswidrigkeitenverfahren weitergeführt und er wurde als Betroffener vernommen.

Ich habe das Landratsamt wegen Verstoßes gegen den Grundsatz des Vorrangs der Datenerhebung beim Betroffenen (§ 12 Abs. 2 Satz 1 SächsDSG), der Nichtbeachtung eines Erlasses des SMI und des Gebotes der sparsamen Datenerhebung aus folgenden näheren Gründen beanstandet.

Zwar war das Landratsamt als für die Verfolgung von Ordnungswidrigkeiten zuständige Behörde nach § 46 Abs. 1 OWiG i. V. m. § 161 Abs. 1 StPO berechtigt, personenbezogene Daten zu erheben, soweit dies zu seiner Aufgabenerfüllung erforderlich war. Diese Befugnis umfasste auch die Erhebung von Daten zu Mitbewohnern und Verwandten der Halterin aus dem örtlichen Melderegister. Davon zu unterscheiden waren jedoch die in den Pass- oder Personalausweisregistern des Landratsamtes darüber hinaus gespeicherten personenbezogenen Daten der in Betracht kommenden Betroffenen (§ 22 Abs. 2 Satz 3 PaßG und § 2b Abs. 2 Satz 3 PAuswG). Diese weiteren Daten hätten einer ersuchenden Stelle nur unter den Voraussetzungen des § 22 Abs. 2 Nr. 1 bis 3 PaßG oder § 2 Abs. 2 Nr. 1 bis 3 PAuswG übermittelt werden dürfen. Voraussetzungen und Verfahrensweise eines Abrufs personenbezogener Daten bei Personalausweisbehörden durch Bußgeldbehörden sind durch Erlass des SMI zur Einsichtnahme des Polizeivollzugsdienstes und der Bußgeldbehörden in das Personalausweis- oder Passregister vom 1. Juli 2005 (Az. 31-055/114) eindeutig und klar geregelt:

> „Sofern der Halter keine Angaben zu der Person des Fahrers oder von seinem Zeugnisverweigerungsrecht oder Auskunftsverweigerungsrecht gemäß §§ 52-55 StPO Gebrauch macht und die ggf. eingeräumte Möglichkeit, im Verwarnungsgeldverfahren das Verwarnungsgeld zu zahlen, ungenutzt verstrichen ist, können anhand des Melderegisters der Meldebehörde die Namen und Anschriften von Familienmitgliedern des Halters erhoben werden, *ohne zunächst das Beweisfoto mit deren im Pass- und Personalausweisregister hinterlegten Fotos abzugleichen*. Diesen Personen kann dann ein Zeugenfragebogen zugesandt werden. Der Zeugenfragebogen ist mit folgendem Zusatz zu versehen:
>
> ‘*Hinweis: Nach dem gegenwärtigen Stand der Ermittlungen sind Sie Zeuge und möglicher Betroffener im Verfahren wegen o. g. Ordnungswidrigkeit. Sofern Sie*

innerhalb einer Frist von einer Woche keine Angaben zum verantwortlichen Fahrzeugführer machen, kann das Beweisfoto mit Ihrem im Pass- und Personalausweisregister hinterlegtem Foto verglichen werden.'

Auch hier kann der Zeugenfragebogen im Verwarnungsgeldverfahren die Möglichkeit beinhalten, das Verfahren durch Zahlung des Verwarnungsgeldes zu beenden. Nach Ablauf der eingeräumten Frist kann auch hier der Bildabgleich stattfinden.“

Das Landratsamt hätte also zunächst die in Betracht kommenden Familienmitglieder anschreiben und ihnen einen Zeugenfragebogen vorlegen müssen. Das wäre zwar etwas aufwendiger, dafür aber rechtmäßig gewesen. Denn die öffentliche Gewalt, auch Bußgeldbehörden, dürfen nicht ohne weiteres hinter dem Rücken von Betroffenen Daten zu ihrer Person erheben. Dies ist nur in engen Ausnahmefällen gestattet, etwa wenn Anhaltspunkte dafür vorhanden sind, dass ein Betroffener die Unwahrheit gesagt hat. Im Regelfall muss die öffentliche Gewalt zunächst die Daten beim Betroffenen zu erheben versuchen. Dies stellt einen der tragenden Grundsätze des Datenschutzrechts dar und hat u. a. in § 12 Abs. 2 Satz 1 SächsDSG Ausdruck gefunden. Auch der Erlass des SMI, den das Landratsamt nicht beachtet hat, beruht darauf.

In meiner Beanstandung habe ich gefordert, dafür Sorge zu tragen, dass der Erlass des SMI vom 1. Juli 2005 künftig ausnahmslos und exakt beachtet wird.

9.2 Gewerberecht

In diesem Jahr nicht belegt.

9.3 Industrie- und Handelskammern; Handwerkskammern

9.3.1 IHK - Unternehmensdatenbank

Eine Industrie- und Handelskammer wandte sich an mich, da sie beabsichtigte, ihre bestehende Internetplattform zur Förderung von Geschäftsabschlüssen um eine vollständige Unternehmensdatenbank aller Kammerangehörigen zu erweitern und bat um Auskunft, ob dagegen datenschutzrechtliche Bedenken geltend gemacht werden können.

Grundsätzlich gestattet § 9 Abs. 4 IHK-G eine Übermittlung von Name, Firma, Anschrift und Wirtschaftszweig der Kammerangehörigen an nicht-öffentliche Stellen durch die IHK zur Förderung von Geschäftsabschlüssen und dem Wirtschaftsverkehr

dienenden Zwecken. Das Gesetz fordert allerdings eine Einwilligung des Kammerzugehörigen, wenn zusätzlich Angaben über die von ihm angebotenen Waren und Dienstleistungen sowie die Betriebsklassengröße übermittelt werden sollen.

Die von der IHK vorgesehene Vorgehensweise bei der Ergänzung und dem weiteren Aufbau der Datenbank auf ihrer bestehenden Internetplattform konnte ich als datenschutzkonform bestätigen. Danach war vorgesehen, bei Handelsregister-Neueintragungen oder -Änderungen unter Beachtung der Regelungen zum Einholen der Einwilligungserklärung (§ 4 Abs. 3 bis 5 SächsDSG) zuvor eine Einwilligungserklärung bei der betroffenen Firma zur Veröffentlichung der Angaben auf der Internetpräsenz einzuholen. Bei der Einbeziehung der bereits im Handelregister eingetragenen Firmen in die Internetplattform war auch zu beachten, dass diese Firmen durch ein geeignetes Anschreiben der IHK unter Bezugnahme auf § 9 Abs. 4 IHK-G die Möglichkeit erhalten mussten, vor der ersten Veröffentlichung ihrer Daten zu widersprechen. Gleichzeitig war darauf hinzuweisen, dass neben der Möglichkeit des sofortigen Widerspruchs (hier erschien eine 4-Wochen-Frist angemessen) ein späterer Widerspruch zur Veröffentlichung jederzeit möglich ist. Andere Gewerbetreibende, die nicht in öffentlichen Registern - wie im Handelsregister - eingetragen sind (das Gewerberegister ist so ein nicht öffentlich zugängliches Register), könnten ohnehin nur auf Einwilligungsgrundlage in die Unternehmensdatenbank aufgenommen werden.

Hingewiesen habe ich die IHK auf das Erfordernis, beim Betreiben der Datenbank Maßnahmen zur Gewährleistung des Datenschutzes nach § 9 SächsDSG, insbesondere zur Integrität und Authentizität der Daten zu treffen. Bei der Absicht, Firmen die Möglichkeit einzuräumen, eigene Firmenangaben zu ergänzen, muss beispielsweise ein Zugriff auf die fixen Firmendaten der Unternehmensdatenbank verwehrt sein, um verfälschende oder unberechtigte Änderungen zu unterbinden.

9.4 Offene Vermögensfragen

9.4.1 Datenaustausch zwischen Vermögensämtern und Lastenausgleichsämtern

Infolge der - noch keineswegs abgeschlossenen - Tätigkeit der Ämter zur Regelung offener Vermögensfragen (in den neuen Bundesländern) haben auch die Lastenausgleichsämter (in den alten Bundesländern) wieder Arbeit bekommen, (wobei beide Behörden vielfach zusammenwirken müssen, weil Lastenausgleichsleistungen und Rückübertragungs- bzw. Entschädigungsleistungen für denselben Vermögens-

wert nicht doppelt geleistet werden sollen.) Das schlägt sich auch datenschutzrechtlich nieder, wie folgender Fall zeigt:

Ein Ehepaar aus Hessen, die Miterben nach einer Frau M., hat sich an mich gewandt. Frau M. war aus dem Erzgebirge nach Westdeutschland gegangen und hatte dort später wegen des Verlustes des zurückgelassenen, ihr dann weggenommenen Vermögens einen Antrag auf sog. *Lastenausgleich* nach dem Lastenausgleichsgesetz gestellt, also demjenigen Gesetzeswerk, das in der ‚Alt-Bundesrepublik' der „Abgeltung von Schäden und Verlusten, die sich infolge der Vertreibungen und Zerstörungen der Kriegs- und Nachkriegszeit ergeben haben", von Einbußen durch die Währungsreform (§ 15 LAG) sowie, als sog. *Zonenschäden* (§ 15a LAG), auch der Vermögensverluste infolge der Wegnahme von Vermögenswerten in der Sowjetischen Besatzungszone bzw. der DDR, einschließlich Ost-Berlin (nach dem sog. Beweissicherungs- und Feststellungsgesetz, BGBl. I 1965, 425), insbesondere als Folge einer Übersiedlung nach Westdeutschland, gewidmet gewesen ist und mit dem man in begrenztem Ausmaß zwischen denjenigen, die der Krieg und seine mittelbaren Folgen an Vermögenswerten stärker getroffen hatte, und denjenigen, die er eher verschont hatte oder die durch die Währungsreform sogar begünstigt worden waren, einen finanziellen Ausgleich geschaffen hat.

Für den Verlust eines Hauses waren Frau M. 1977 Leistungen nach diesem Gesetz in Höhe von rund 40.000 DM gezahlt worden. Nachdem das Wohnhaus im Jahr 1992 an Frau M. nach dem Gesetz zur Regelung offener Vermögensfragen zurückgegeben worden war, forderte die seinerzeit tätig gewesene Lastenausgleichsbehörde die damals erbrachten Lastenausgleichszahlungen zurück, weil durch die Rückübertragung die Voraussetzungen für einen diesbezüglichen Lastenausgleich nachträglich entfallen waren. Da Frau M. inzwischen verstorben war, ging der Rückforderungsbescheid der Lastenausgleichsbehörde an ihre Erben, eben die Petenten. Sie stellten einen Stundungsantrag und wurden dabei gewahr, dass das zuständige Amt zur Regelung offener Vermögensfragen (ARoV) dem Lastenausgleichsamt mitgeteilt hatte, dass nicht nur das eine Haus, sondern auch weitere (ebenfalls im Zuständigkeitsbereich dieses ARoV belegene) Vermögenswerte rückübertragen worden waren. Die Petenten hielten diese Datenübermittlungen für unzulässig und baten mich um Prüfung (wobei ich genau genommen nur die Verarbeitungshandlungen der beteiligten sächsischen Stelle, also des ARoV, zu beurteilen hatte).

Dazu habe ich die Akten zum Restitutionsvorgang angefordert und nach Studieren der sieben dicken Ordner den datenschutzrechtlich relevanten Sachverhalt herausarbeiten und feststellen können, dass die in dem Schriftverkehr zwischen den beiden

Ämtern vorgenommene Verarbeitung personenbezogener Daten rechtmäßig gewesen ist, nämlich die nötige gesetzliche Erlaubnisgrundlage gehabt hat:

(1) In einem ersten Schreiben im August 2005 hat die Lastenausgleichsbehörde das ARoV davon unterrichtet, dass Frau M. für ein bestimmtes Grundstück Lastenausgleich erhalten hatte. Zudem hat das Lastenausgleichsamt das ARoV um Mitteilung gebeten, ob für dieses Grundstück ein Antrag auf Rückübertragung (nach dem Gesetz zur Regelung offener Vermögensfragen - kurz *Vermögensgesetz* bzw. *VermG*, BGBl. II 1990 S. 889) bzw. Entschädigung (nach dem Gesetz über die Entschädigung nach dem Gesetz zur Regelung offener Vermögensfragen - kurz *Entschädigungsgesetz* bzw. *EntschG*, BGBl. I 1994, S. 2624) vorliege bzw. bereits beschieden worden sei.

Bei diesem Schreiben hat es sich um eine Weitergabe personenbezogener Daten Frau M.s gehandelt, die auf der Rechtsgrundlage des *§ 317 Abs. 2 LAG* hat erfolgen können: Danach übermittelt die Ausgleichsverwaltung der für die Rückgabe oder Entschädigung zuständigen Stelle - hier dem ARoV - die Angaben zur Ermittlung derjenigen Vermögenswerte, für die sog. Hauptentschädigung nach dem Lastenausgleichsgesetz gewährt worden ist (in diesem Fall wegen *Wegnahme von Wirtschaftsgütern* durch Behörden im Zusammenhang mit den nach der Besetzung durch sowjetische Truppen entstandenen politischen Verhältnissen, § 3 Abs. 1 Beweissicherungs- und Feststellungsgesetz). Das ARoV ist also zu der mit diesem Mitteilungsvorgang verbundenen Datenerhebung berechtigt gewesen (und die Lastenausgleichsbehörde zu der betreffenden Datenübermittlung).

(2) Noch im August 2005 hat das ARoV auf diese Anfrage der Lastenausgleichsbehörde hin dieser die Umstände der Rückübertragung des Grundstückes im Jahre 1992 mitgeteilt. Zugleich hat das ARoV das Lastenausgleichsamt gebeten, mitzuteilen, ob für weitere Vermögenswerte Leistungen nach dem Lastenausgleichsgesetz an Frau M. gewährt worden waren. Ferner hat das ARoV das Lastenausgleichsamt davon unterrichtet, dass für weitere Vermögenswerte Rückübertragungsentscheidungen nach dem Vermögensgesetz ergangen bzw. Entschädigungen nach dem Entschädigungsgesetz zuerkannt worden waren.

Die in diesem Schreiben weitergegebenen personenbezogenen Daten durfte das ARoV gemäß *§ 27 Abs. 2 Satz 1 und Satz 3 VermG* an das Lastenausgleichsamt übermitteln. Nach dieser Vorschrift darf das ARoV dem zuständigen Lastenausgleichsamt eine Abschrift seiner Entscheidungen nach dem Vermögensgesetz sowie weitere zum Zweck der Rückforderung von Ausgleichsleistungen erforderliche Angaben übermitteln.

Diese Befugnis zur Übermittlung des gesamten Rückübertragungsbescheides umfasst zwingend auch die Übermittlung der demgegenüber zurückbleibenden Angabe, dass überhaupt eine bestimmte Person Vermögenswerte rückübertragen bekommen hat oder für sie entschädigt worden ist.

(Zusätzlich könnte man diese Übermittlung der Angabe, dass auch für weitere Vermögenswerte, neben dem besagten Haus, positive Rückübertragungs- bzw. Entschädigungsleistungs-Entscheidungen getroffen worden sind, auf folgende Rechtsgrundlage stellen:

Es hat sich dabei um eine als Amtshilfeersuchen zu verstehende Mitteilung des ARoV zur Vorbereitung etwaiger Rücknahmebescheide gehandelt; grundsätzlich hat das ARoV ja bei Entscheidungen über Entschädigungsleistungen nach § 8 Abs. 1 Satz 1 EntschG einen von der Lastenausgleichsverwaltung bestandskräftig festgesetzten Rückforderungsbetrag abzuziehen. Da das ARoV erst nach Beendigung der Entschädigungsverfahren Anhaltspunkte dafür erhalten hatte, dass von den gezahlten Entschädigungen möglicherweise nach dieser Vorschrift des § 8 Abs. 1 EntschG eine bereits gezahlte Hauptentschädigung nach Lastenausgleichsgesetz abzuziehen gewesen wäre, hat es Ermittlungen anzustellen gehabt, um darüber entscheiden zu können, ob es seinen Entschädigungsbescheid gegebenenfalls zurücknehmen und durch einen berichtigten zu ersetzen hätte. Die dafür notwendige Erhebungsbefugnis betreffend die für eine solche Entscheidung erforderlichen personenbezogenen Daten (bestandskräftig festgesetzter Rückforderungsbetrag nach Leistung von Hauptentschädigung?) ergibt sich aus § 12 Abs. 1 SächsDSG, zumindest i. V. m. Abs. 4 Nr. 1 SächsDSG, i. V. m. § 8 Abs. 1 Satz 1 (vgl. auch Satz 2!) EntschG. In dieser Erhebungsbefugnis des ARoV enthalten ist auch die Befugnis zur Übermittlung derjenigen Daten, die zur Konkretisierung der die Datenerhebung ermöglichenden Frage, also der an die Lastenausgleichsbehörde gerichteten Frage, erforderlich sind.)

(3) Im Oktober 2006 hat dann das Lastenausgleichsamt das ARoV davon benachrichtigt, dass es beabsichtige, den Antrag der Petenten auf Stundung der Rückzahlungsforderung wegen der verschiedenen Rückübertragungen abzulehnen, und für die etwaige Eintragung von Sicherungshypotheken (zur Sicherung des Rückzahlungsanspruches) um Übersendung der entsprechenden Bescheide über Rückübertragungen und zuerkannte Entschädigungen gebeten.

(4) Die angeforderten Bescheide hat das ARoV übersandt - auf der Grundlage des schon genannten *§ 27 Abs. 2 Satz 1 VermG*.

Es hat sich dabei um zwei bestandskräftige Entschädigungsbescheide sowie einen weiteren Rückübertragungsbescheid über zwei Grundstücke gehandelt.

(5) Von einer - grundsätzlich möglichen - Rücknahme seiner Bescheide hat das ARoV jedoch abgesehen, nachdem das Lastenausgleichsamt ihm mitgeteilt hatte, dass es seinerseits Rückforderungsansprüche geltend machen werde und für etwaige Sicherungshypotheken und Verrechnungserklärungen entsprechende Bescheide des ARoV benötige. Diese Datenerhebung konnte das Ausgleichsamt auf § 317 Abs. 1 LAG stützen. Die mit der Übersendung der Bescheide verbundene Datenübermittlung durch das ARoV an das Ausgleichsamt hat ebenfalls § 317 Abs. 1 LAG zur Grundlage gehabt: Nach dieser Vorschrift haben alle Behörden den Lastenausgleichsämtern Auskünfte zu erteilen und Akteneinsicht zu gewähren, soweit dies zur Durchführung des Lastenausgleichsgesetzes erforderlich ist. Zusätzliche Rechtsgrundlage war § 27 Abs. 2 Satz 1 und 3 VermG.

Über das Ergebnis dieser Kontrolle haben sich die Petenten nicht freuen können, da der eigentliche Hintergrund ihrer Anfrage - wie in sehr vielen anderen Fällen auch - weniger datenschutzrechtlicher sondern finanzieller Natur war: Sie hatten sich offenbar erhofft, dass wegen Verstößen gegen Datenschutzrecht ihr Stundungsantrag positiv würde beschieden werden müssen.

10 Gesundheit und Soziales

10.1 Gesundheitswesen

10.1.1 Umsetzung der Testmaßnahme zur Einführung der elektronischen Gesundheitskarte (eGK)

Die Einführung der eGK sowie die Pilotphasen in den Testregionen werden von mir bezüglich der Umsetzung der datenschutzrechtlichen Belange bereits seit 2004 fortlaufend begleitet. Bereits in 12/10.1.2 berichtete ich ausführlich zum Stand der Einführung der eGK in Sachsen. Die in meinem Beitrag veröffentlichten Anforderungen an eine datenschutzgerechte Gestaltung der eGK sind nach wie vor gültig. Gemeinsam mit den Datenschutzbeauftragten des Bundes und der Länder berate ich die mit der Umsetzung des Projektes beauftragten Unternehmungen zur Anwendung und Umsetzung der Datenschutzforderungen.

Vor diesem Hintergrund befasst sich der Beitrag mit den datenschutzrechtlichen Anforderungen an die eGK in der ersten Teststufe und zeigt, wie sie datenschutzgerecht und verbraucherfreundlich gestaltet werden kann.

Einführung

Vor der bundesweiten Einführung der eGK sollen in sieben ausgewählten Testregionen die vier Funktionsabschnitte der Telematikinfrastruktur erprobt werden. In Sachsen wird seit dem 22. Dezember 2006 im Landkreis Löbau-Zittau die Einführung der eGK getestet.

Im Rahmen der Planung der eGK sollen wichtige Voraussetzungen geschaffen werden, damit bestehende Informationssysteme in Arztpraxen, Apotheken und Krankenhäusern untereinander (über sichere Netze) kommunizieren können. „*Durch dieses Projekt wird nach Aussage der Sächsischen Staatsministerin für Soziales die bundesweit einheitliche technische Infrastruktur in Form von Karten, sicheren Netzen und notwendigen Verbindungen geschaffen. Im Freistaat Sachsen entsteht ein Gesundheitsnetzwerk mit den ca. 4,3 Mio. Bürgern, ca. 12.500 Ärzten, ca. 3.260 Zahnärzten, 86 Krankenhäusern, 950 Apotheken und den in Sachsen vertretenen Krankenkassen*."[1]

Am Projekt beteiligt sind alle Leistungserbringer und Kostenträger. Die Projektleitung für den Feldtest wird durch die AOK Sachsen und die Projektsteuerung durch

[1] SaxMediCard - Projektziel, Projektansatz, Projektmanagement und Stand der Einführung der elektronischen Gesundheitskarte in der Testregion Löbau-Zittau, ■ R. Seibt , L. Kleinholz, R. Schlautmann, U. Bethge, R. Rösler, P. Oesch.

die healthpartner consulting GmbH wahrgenommen. Die regionale Projektleitung wurde der Managementgesellschaft Gesundheitszentrum Löbau-Zittau übertragen.

Testmaßnahme für die Einführung der eGK

Der Test wird stufenweise in jeweils vier Funktionsabschnitten durchgeführt. Der Leistungsumfang wurde in der *Verordnung über Testmaßnahmen für die Einführung der elektronischen Gesundheitskarte*[2] vom 10. Oktober 2006 festgelegt. In der ersten Testphase wurden Anwendertests in einer zentralen Musterumgebung der *gematik* Berlin mit Testdaten durchgeführt. Das elektronische Rezept (eRezept) ist die erste Anwendung, die auf der Basis der eGK erprobt wurde. Getestet wurde das Lesen und Schreiben der Versichertenstammdaten und eRezepte auf bzw. von der eGK im Testlabor. Diese ersten Labortests der eGK in einer Musterumgebung können noch keine Rückschlüsse auf die Praktikabilität und Akzeptanz der Telematikinfrastruktur liefern und zeigen noch nicht, ob sich die Karte in den Arzt- und Klinikalltag integrieren lässt.

In einer zweiten Teststufe (Release 1) wird der Transport des eRezeptes über die eGK ohne Netzzugang (*offline*) getestet und zusätzlich das Schreiben und Lesen der Versichertenstammdaten und der Notfalldaten auf die eGK.

Der Leistungsumfang für Release 2 beinhaltet die Testung der elektronischen Gesundheitskarte mit Netzzugang (*online*). Für die Übermittlung der ärztlichen Verordnungen für apothekenpflichtige Arzneimittel (*Verordnungsdaten* - gemäß § 291a Abs. 2 Satz 1 SGB V), für den Abgleich der *Versichertenstammdaten* und für die Anwendungen *Daten für die Notfallversorgung* wird ein Netzzugang geschaffen und die Übermittlung der Arzneimittelverordnungen über die Telematikinfrastruktur getestet. Die Gültigkeit der Versichertendaten können über den Netzzugang (online) überprüft und nach Onlineabgleich mit der Krankenkasse auf der Karte aktualisiert werden.[3]

Im dritten Abschnitt soll die Übermittlung der Verordnungen technikoffen getestet werden.

Ab dem vierten Abschnitt werden die Anwendungen gemäß § 291a Abs. 3 Satz 1 Nr. 1 und 3 SGB V sowie weitere Verordnungen (z. B. Heil- und Hilfsmittel) getestet.

Datenschutzrechtliche Anforderungen an die Karten

[2] „Verordnung über Testmaßnahmen für die Einführung der elektronischen Gesundheitskarte“ in der Fassung der Bekanntmachung vom 5. Oktober 2006 (BGBl. I vom 10. Oktober 2006, Seite 2199 ff.).
[3] Vgl. Fußn. 2.

Grundsätzlich sollen alle medizinischen Daten für den Transport und für die Speicherung verschlüsselt werden. Die Daten müssen mit dem elektronischen Schlüssel der eGK des Patienten verschlüsselt werden.

Die Datenschutzbeauftragten haben eine datenschutzgerechte Protokollierung der Zugriffe auf die Gesundheitsdaten verlangt. Im Konzept der eGK ist deshalb jetzt vorgesehen, die letzten 50 Zugriffe auf die Karte zu protokollieren und nur für den Versicherten selbst einsehbar zu gestalten.

Eine datenschutzgerechte Umsetzung setzt voraus, dass nur konkrete Fachärzte einen Zugang zu den freiwilligen Daten (z. B. die elektronische Patientenakten (EPA) und Arzneimittel-Historie) über die eGK eröffnet bekommen.

Als weitere datenschutzseitige Schwerpunkte sollen hier kurz erwähnt werden:

- die differenzierte Vergabe der Zugriffsrechte,
- das Verfahren im Fall des Verlustes oder der Beschädigung der Karte,
- der Schutz der Datenübertragung und verschlüsselte Datenspeicherung.

Zum Aufbau der Telematikinfrastruktur und zur Einführung der eGK wurde die Gesellschaft *gematik GmbH* gegründet. Aufgabe der *gematik* ist es u. a., die technischen Vorgaben einschließlich Datenschutz- und Datensicherheitskonzept zu erstellen, Inhalt und Struktur der Datensätze festzulegen sowie alle Test- und Zertifizierungsmaßnahmen sicherzustellen.[4] Dieses Datenschutz- und Datensicherheitskonzept musste durch die Datenschutzbeauftragten mehrfach eingefordert werden. Die *gematik* hat leider erst im April 2007 das längere Zeit angekündigte Datensicherheitskonzept zur Kommentierung freigegeben.

Im Berichtszeitraum konnte u. a. erreicht werden, dass spezielle Kommandos und Funktionen des Kartenbetriebssystems in die Konzeption der eGK aufgenommen und aktiviert wurden, um die Patientenrechte auch wirksam anwenden zu können.

Entwicklung in der Testregion Sachsen

In der Testregion Sachsen nehmen bisher 22 niedergelassene Ärzte, 30 Apotheken und das Klinikum Löbau-Zittau am Test teil.

Testbeginn für die Gesundheitskarte - Lesen der Versichertendaten - war in der Testregion Sachsen der 22. Dezember 2006. Seit dem offiziellen Testbeginn in Sachsen

[4] Vgl. § 291b SGB V.

wurden über 1.100 Karten eingelesen, von denen insgesamt (lt. Angaben der Projektleitung) 40 Karten nicht gelesen oder verarbeitet werden konnten.[5]

Im ersten Testabschnitt wurde das Schreiben des eRezeptes auf die eGK getestet. Aus Sicherheitsgründen soll das Auslesen der eGK nur mit einer freigeschalteten und aktiven HPC/HBA (health personal Card/Heilberufeausweis) möglich sein. Nur wenn HBA und eGK in den Kartenleser gesteckt und geprüft wurden, kann ein Rezept auf die Karte gespeichert werden. In allen Testregionen wird der gleiche Funktionsumfang getestet. Bisher wird offline in einem Testlabor gearbeitet und die Abfrage des Versichertenstatus nur simuliert.

Im Testlabor Löbau-Zittau konnten jeweils nur acht Medikamente (Verordnungen) auf einer Gesundheitskarte gespeichert werden. Zusätzlich kann der Arzt jetzt einen Notfalldatensatz auf der Karte anlegen. Der Arzt oder Heilberufler muss jede Verordnung (eRezept) mit einer qualifizierten elektronischen Signatur und PIN-Eingabe bestätigen. Auch im Testlabor musste jede Verordnung - also jedes Medikament - einzeln vom Arzt signiert und mit der PIN bestätigt werden. Diese Umstrukturierung der Abläufe und die notwendige angepasste technische Ausrüstung greifen stark in die Abläufe in der Arztpraxis ein.

Die Telematikinfrastruktur soll es ermöglichen, dass der Patient die Rechte zur Steuerung des Zugriffs auf die gespeicherten Informationen seiner eGK selbst wahrnimmt. Nach der derzeit vorliegenden Lösungsarchitektur soll der Karteninhaber seine Rezepte, Verordnungen oder andere über die Karte gespeicherten Informationen (z. B. EPA) auf der Karte verbergen und im Weiteren nur bestimmten Leistungserbringern zugänglich machen (freigeben) können. Dadurch erhält der Patient die Möglichkeit, auch einzelne Rezepte in einer Apotheke einzulösen und alle weiteren Rezepte vor dem Apotheker zu verbergen. Rezepte seiner Wahl kann er dann bei einer Apotheke seines Vertrauens oder einer Versandapotheke einlösen. Zur Durchführung der Patientenrechte werden so genannte e-Kioske (Patiententerminals) benötigt, an denen der Patient die auf seiner Karte gespeicherten Daten freigeben, verbergen oder löschen kann.

Um den Patienten zu ermöglichen, dass sie auch unabhängig und außerhalb einer Arztpraxis oder Apotheke ihre Kartendaten einsehen und auf die Auswahlmöglichkeiten zugreifen können, sollen die eKioske in geschützten Bereichen, z. B. einer Arztpraxis oder Apotheke aufgestellt werden. Allerdings gibt es in der Testregion Sachsen bisher noch keinen einzigen eKiosk an denen die Patienten ihre Datenhoheit

[5] Internetpräsentation Projektbüro SaxMediCard; http://www.saxmedicard.de/aktuelles.php.

testen könnten, da die einzelnen technischen Komponenten an die Testregion nur mit erheblicher Verspätung geliefert bzw. freigegeben werden. Zusätzlich soll den Versicherten von zu Hause - über das Internet - die Möglichkeit eingeräumt werden, auf die Kartendaten zuzugreifen. Wie die konkrete Ausgestaltung der eKioske und der Homezugänge ausgestaltet werden und welcher Funktionsumfang realisiert wird, ist noch abschließend festzulegen.

Die technische Umsetzung dieses Konzeptes wurde nur möglich durch die Aktivierung des Kommandos „Deactivate Record“ des Kartenbetriebssystems. Die Datenschutzbeauftragten der Länder haben schon frühzeitig auf die Umsetzung dieser Technik gedrängt, um die Einhaltung der Datenschutzvorgaben und des damit verbundenen Selbstbestimmungsrechts der Patienten zu gewährleisten.

Wann die Wahrnehmung der Versichertenrechte eindeutiger Bestandteil für die Testregionen und somit für den Gesamttest wird und wann diese Testphase beginnen wird, ist unbestimmt, da diesbezüglich noch konkrete technische Realisierungsvorgaben fehlen.

Unabhängig von meiner Beteiligung im Lenkungssauschuss des Projektes SaxMediCard habe ich im Rahmen einer Kontrolle im Juni dieses Jahres die Einhaltung des Datenschutzes bei der technischen Umsetzung und Durchführung des Projektes in Löbau-Zittau überprüft.

Einwilligung, Lichtbild

Ich konnte auf die Gestaltung der Einwilligungserklärung der sächsischen gesetzlichen Krankenkassen zu Testzwecken wesentlichen Einfluss nehmen. Die Testteilnehmer in Sachsen haben die Möglichkeit, differenziert in die Erhebung und Verarbeitung ihrer Daten einzuwilligen. Das betrifft zum einen die Lichtbilddaten, die beim Testverfahren Verwendung finden sollen und die auch, soweit es der Einwilligende möchte, von der Krankenkasse weiterverwendet werden dürfen, als auch die übrigen Testdaten, zu denen insbesondere die nach dem Gesetz obligatorischen Angaben nach § 291 Abs. 2 SGB V, e-Rezept-Funktion nach § 291a Abs. 2 SGB V und freiwillige Angaben im Sinne von § 291a Abs. 3 SGB V, wie Notfall- und Arzneimitteldaten gehören. Sobald der Testteilnehmer seine Einwilligung widerruft, sind die Daten zu löschen und können nicht weiterverwendet werden.

Voraussetzung einer zureichenden Einwilligung ist eine bestmögliche Information der Einwilligenden. Ich lege daher Wert darauf, dass bei der Fortschreibung des Testverfahrens die Einwilligenden fortwährend informiert bleiben. Im Hinblick auf die

datenschutzrechtlichen Kernpunkte habe ich mich mit dem Projektbüro dahingehend geeinigt, dass diese auch auf der Internetpräsenz veröffentlicht werden. Die perspektivische Datenverarbeitung, die Datenflüsse im Einzelnen bis hin zu der einfachen Frage, wer eigentlich die Daten verarbeitenden Stellen sind, waren bis zum Ende des Berichtszeitraums unklar, was keinesfalls am sächsischen Projektbüro gelegen hat, sondern an Verantwortlichen an anderer Stelle, die auch im Bundesregierungsbereich angesiedelt sein mögen. Unter anderem wegen der zahlreichen „Unbekannten“ in dem Verfahren habe ich eine Beteiligung von nicht persönlich einwilligungsfähigen Personen als nicht zulässig angesehen.

Ausblick

Die eGK zieht eine Reihe von technischen und organisatorischen Maßnahmen nach sich. Bereits bei der ersten Anwendung im Testgebiet sind auch Nebenwirkungen ersichtlich. Die Umsetzung der geplanten EPA erfordert bei weitem höhere Ansprüche an die Technik, wobei die Diskussion über Inhalt und Zweck der EPA noch nicht abgeschlossen ist.

Ich werde mich auch weiterhin dafür einsetzen, dass die Einführung der eGK und Telematikinfrastruktur, auch unter der Gefahr wachsenden Zeitdruckes, unter Wahrung der Belange des Datenschutzes umgesetzt wird. Eine datenschutzrechtlich nachprüfbare Verfahrensbeschreibung, ein Datenschutz- und Datensicherheitskonzept für den Testbetrieb in der Testregion Löbau-Zittau wurde bis zum Ende des Berichtszeitraums nicht vorgelegt. Allein mit Verordnungen über Testmaßnahmen[6] und Staatsministerankündigungen ist es eben nicht getan. Das macht es mir schwer.

10.1.2 Aktenführung und Einsichtnahmerecht bei einem für ein gerichtliches Gutachten beteiligten universitären Institut einer Klinik

Ein Petent, der Vater eines Kindes, das bei einem an einer Universitätsklinik angegliederten Institut begutachtet worden war, wandte sich mit der Bitte um Unterstützung zur Einsichtnahme in die bei dem Institut zu seiner Person verarbeiteten personenbezogenen Daten an mich. Das Institut erarbeitet psychiatrische und psychologische Gutachten und wird von Familiengerichten regelmäßig zur Entscheidungsfindung in Anspruch genommen. Bei der Begutachtung von Kindern, die anhand von Gesprächen erfolgen, werden von dem Institut üblicherweise Videoaufzeichnungen angefertigt. Auf den Videoaufzeichnungen sind die Kinder im Gespräch zu sehen und - wenn mit den Eltern (zumeist getrennte) Gespräche durchgeführt wurden - auch die

[6] Vgl. die Verordnung über Testmaßnahmen für die Einführung der elektronischen Gesundheitskarte vom 2. November 2005 (BGBl. I S. 3128).

Eltern. Der Petent begehrte die Einsichtnahme in die ihn betreffenden Videoaufzeichnungen, die ihm zunächst verwehrt wurde.

Ich forderte das Institut auf, die Einsichtnahme zu gestatten. Hierbei waren für mich nachstehende Überlegungen ausschlaggebend.

Die Gerichte unterliegen der Kontrolle des Sächsischen Datenschutzbeauftragten nach § 27 Abs. 4 SächsDSG nur, soweit sie in Justizverwaltungsangelegenheiten tätig werden. Insofern war ich nicht berechtigt Datenverarbeitungsvorgänge zu kontrollieren, die im gerichtlichen Verfahren gerichtlicherseits durchgeführt oder unterbunden werden. Allerdings sind die bei dem Klinikinstitut verbleibenden und gespeicherten Daten Gegenstand meiner Kontrolle öffentlicher Stellen. Das Institut selbst hat die Videoaufzeichnungen als Hilfsmittel zum Gutachten betrachtet, die eigenständig verwahrt wurden und im Besitz und Eigentum des Klinikinstituts verblieben. Die Videobänder habe ich daher als Akten im Sinne von § 3 Abs. 6 SächsDSG angesehen, wenn sie nicht bereits Krankenakten im Sinne des Sächsischen Krankenhausgesetzes gewesen sein sollten. Nach § 32 Abs. 5 SächsKHG, § 18 Abs. 3 SächsDSG steht Betroffenen ein Einsichtnahmerecht in zu ihnen geführten Akten zu, so dass diesen auf Verlangen auch Einsicht in die Akten (die Videobänder) zu ihrer Person zu gewähren ist. Darüber hinaus stand den Elternsorgeberechtigten in Bezug auf den Sohn ein Einsichtnahmerecht, das gemeinsam geltend zu machen gewesen wäre, zu, da die Elternsorgeberechtigten bei noch nicht über die Einsicht verfügenden minderjährigen Kindern das Grundrecht auf informationelle Selbstbestimmung ausüben. Zu den Daten mit Doppelbezug zu seiner jeweiligen Person war auch ein Elternsorgeberechtigter auskunftsbefugt. Da keine gesetzlich normierten Ausschlussgründe nach § 32 Abs. 5 SächsKHG, § 18 SächsDSG einschlägig waren, war dem Petenten Einsicht in die entsprechenden Videoaufzeichnungen zu gewähren. Entsprechendes galt für textliche Aufzeichnungen, die in der Klinik zu dem Vorgang geführt wurden. Das Institut folgte meinen Hinweisen.

10.1.3 Datenverarbeitung durch den Rettungsdienst

Mehrfach erhielt ich Anfragen von Beschäftigten im Rettungsdienst, die sich besorgt über die Verarbeitung von Patientendaten bei Rettungsdiensteinsätzen äußerten. In diesem Zusammenhang habe ich auf die bereits im Jahr 2004 mit dem Gesetz über den Brandschutz, Rettungsdienst und Katastrophenschutz (SächsBRKG) begonnene Neuordnung dieses Bereiches im Freistaat Sachsen hingewiesen.

Mit der Sächsischen Landesrettungsdienstplanverordnung (SächsLRettDPVO) vom 5. Dezember 2006 wurde das Rettungsdienstwesen neu geregelt und der bis dahin gültige Landesrettungsdienstplan (SächsLRettDP) außer Kraft gesetzt. Im Rahmen meiner Beteiligung im Verordnungsgebungsverfahren konnte ich Empfehlungen geben, die Berücksichtigung in der Sächsischen Landesrettungsdienstplanverordnung fanden.

Die vorgenommenen Änderungen bei der Verarbeitung personenbezogener Daten beziehen sich vor allem auf mehr Transparenz und auf eine Datenübermittlung, die sich auf das erforderliche Maß beschränkt. So ist durch individuelle Gestaltung des Notarztprotokolls die Datenübermittlung für den jeweiligen Adressaten, Kostenträger, Notarzt, Ärztlicher Leiter Rettungsdienst und das aufnehmende Krankenhaus neu geregelt worden.

Der Ärztliche Leiter Rettungsdienst erhält beispielsweise für die ihm übertragenen Aufgaben der Kontrolle über den Rettungsdienst hinsichtlich Effektivität und Effizienz der präklinischen notfallmedizinischen Patientenversorgung und Patientenbetreuung alle organisatorischen wie medizinischen Daten des Rettungsdiensteinsatzes. Ausgenommen sind die für seine Aufgabenerfüllung nicht erforderlichen personenbezogenen Daten des Versicherten. Vorgeschrieben ist, das Exemplar des Notarztprotokolls zur Weitergabe an das aufnehmende Krankenhaus umgehend zu vernichten, wenn eine Einlieferung des Patienten in ein Krankenhaus nicht erfolgt.

Den Kostenträgern, den gesetzlichen Krankenkassen, werden außer den zu Abrechnungszwecken gemäß § 295 Abs. 2 Satz 1 SGB V vorgesehenen Versichertendaten einschließlich des ärztlichen Diagnoseschlüssels keine weiteren Daten übermittelt.

Nebenbei: Im Falle der zugelassenen mobilelektronischen Dokumentation des Rettungsdiensteinsatzes und Datenübermittlung sind die datenschutzorganisatorischen Bestimmungen des § 9 Abs. 2 SächsDSG einzuhalten.

10.1.4 Einsichtnahme in Krankenhaus-Patientenakten

Nach § 33 Abs. 5 SächsKHG ist dem Patienten Einsicht in seine Krankenakten zu gewähren. Die Auskunfts- und Einsichtsrechte können im Interesse der Gesundheit des Patienten begrenzt oder durch berechtigte Geheimhaltungsinteressen Dritter eingeschränkt werden. Es handelt sich hierbei aber um gesetzliche Ausnahmen. In der Praxis wird Patienten jedoch *uneingeschränkt* Einsichtnahme in ihre Patientenakten in Krankenhäusern zu gewähren sein.

Gleichwohl ist es kein Einzelfall, dass sächsische Krankenhäuser Akteneinsichtnahmen zunächst abzuwehren versuchen, nur sehr zögerlich die Akteneinsichtnahme zulassen oder bei einer Einsichtnahme beanspruchen, die „persönlichen Aufzeichnungen“ von Ärzten vorzuenthalten. Häufig wird dabei auch unterstützend argumentiert, dass der Betroffene die Unterlagen ohne Erläuterung eines medizinisch Fachkundigen ja nicht begreifen und verstehen könne und dass die wertenden oder „subjektiven“ Einschätzungen oder Wahrnehmungen des Arztes nicht Gegenstand der Einsichtnahme sein könnten, da sie Eigentum des Mediziners seien oder dem betroffenen Patienten ja nichts nützten. Das ist eine veraltete Vorstellung in Bezug auf Patientenrechte, der ich natürlich entgegentrete. Wer so argumentiert, hat das Sächsische Krankenhausgesetz offenbar noch nicht richtig gelesen und nicht verinnerlicht, dass es um die Gewährleistung eines Grundrechts geht. Eine Beschränkung der Einsicht gibt es nur in den gesetzlich genannten Fällen. Nicht zu differenzieren ist zwischen „objektiven“ und „subjektiven“ Unterlagen. Die Krankenhaus-Akte ist als Ganzes zu begreifen. „Persönliche Aufzeichnungen“ oder „Notizen“ etwa gibt es juristisch nicht. Es handelt sich um Akten des Krankenhauses und nicht einzelner Ärzte. Auch spielen etwaige Persönlichkeitsrechte der Ärzte keine Rolle. Die behandelnden Ärzte stellen im Zusammenhang mit den Krankenhaus-Patientenakten keine Grundrechtsträger dar. Sie sind vielmehr in einer Amtsträgerrolle, wenn durch sie oder ihr Zutun Patientenangaben in die Akte gelangen. Dasselbe gilt auch für das Krankenhauspersonal. Etwaige handschriftliche Notizen etwa, die für den Mediziner bei Einsicht durch den Betroffenen nachteilig sein können, weil sie z. B. den Patienten abwerten, bekommt dieser daher genauso zu sehen, wie Untersuchungsbefunde, eingegangene Berichte anderer Ärzte und alle anderen ihn betreffenden Krankenunterlagen. Einschränkungen, die das Gesetz nennt, können lediglich in den Fällen bestehen, in denen aus einer objektivierten Sicht heraus die Prognose gemacht werden kann, dass eine Offenbarung die Gesundheit des Patienten beschädigt, was nur in ganz seltenen Konstellationen - nimmt man den Psychiatriebereich aus - der Fall und daher kaum in der Praxis relevant sein dürfte. Geheimhaltungsinteressen Dritter könnten hingegen u. a. dann bestehen, wenn z. B. in den Akten Befunde zum Vergleich zu weiteren Patienten auftauchen, z. B. bei einem epidemielogischen Ereignis. Aber auch in den Fällen, in denen die Ausnahmen greifen, ist der Akteneinsichtnahmeanspruch bestmöglich zu erfüllen und das heißt, dass er nicht wegen zu verschweigender einzelner Schriftstücke oder Angaben gänzlich entfällt, sondern dass nur die problematischen Stellen von einer Einsichtnahme ausgenommen werden können.

Auch das Verfahren der Akteneinsicht ist für Betroffene z. T. belastend. In einem Fall wurde eine gebrechliche Patientin wegen ihres Wunschs auf Akteneinsicht mit

dem Justitiariat der Klinik konfrontiert. Die Akteneinsicht fand an einem an den Bürotisch des Justitiars angefügten Besprechungstisch in dessen Anwesenheit statt. Wie man mir gegenüber mitteilte, habe es sich hierbei um eine übliche Beteiligung des Justitiariats gehandelt. Man kann so etwas aber auch aus Betroffenensicht als Einschüchterungsmethode begreifen. Einsichtnahmen müssen als Betroffenenrecht, ohne dass sich der Einsichtnehmende einer irgendwie produzierten Drucksituation ausgesetzt sieht, gewährleistet werden. Dazu gehört auch, dass man dem Einsichtnehmenden eine Räumlichkeit und unaufdringliches Personal für etwaige Nachfragen zur Aktenführung zur Verfügung stellt. Selbstverständlich hat auch der Patient einen Anspruch auf Ablichtungen, für die er allerdings die Kosten zu tragen hat.

Das Bundesverfassungsgericht hat im Übrigen in einem Beschluss vom 9. Januar 2006 (2 BvR 443/02) die Rechte der Patienten weiter verfestigt. In den Gründen der Entscheidung wird unter anderem festgestellt, dass in das Grundrecht auf informationelle Selbstbestimmung, das die Befugnis des Einzelnen gewährleistet, über die Verwendung seiner persönlichen Daten grundsätzlich selbst zu bestimmen, nur auf gesetzlicher Grundlage eingegriffen werden dürfe. Die gesetzliche Grundlage müsse dem Grundsatz der Verhältnismäßigkeit entsprechen und dürfe nicht weiter reichen, als zum Schutz öffentlicher Interessen unerlässlich. In Bezug auf die Frage der Akteneinsicht komme bei der notwendigen Abwägung dem Informationsinteresse des Patienten erhebliches Gewicht zu. Ärztliche Krankenunterlagen beträfen den Patienten unmittelbar in seiner Privatsphäre. Deshalb und wegen der möglichen erheblichen Bedeutung der in den Unterlagen enthaltenen Informationen für den Patienten habe dieser generell ein geschütztes Interesse daran zu erfahren, wie mit seiner Gesundheit umgegangen wurde. Dies gelte in gesteigertem Maße für Informationen über die psychische Verfassung. Die Entscheidung wird bei der Auslegung der Ausnahmeregeln des § 33 Abs. 5 SächsKHG zu berücksichtigen sein.

Die gesetzliche Bestimmung in Sachsen ist datenschutzrechtlich gelungen und für Akteneinsichtsuchende positiv. In der Umsetzung gibt es z. T. Verbesserungsbedarf. Perspektivisch rechne ich bei der Verfassungsgerichtsrechtsprechung mit einer weiteren Stärkung der Patientenrechte, hin zu einem - bis auf notstandsähnliche Ausnahmen - uneingeschränkten Akteneinsichtnahmerecht, wie die Bestimmung des § 33 Abs. 5 SächsKHG sie darstellt. Die Berufsordnungen jedenfalls werden dem modernen Grundrechtsverständnis, was das informationelle Selbstbestimmungsrecht angeht, noch nicht vollständig gerecht.

10.2 Sozialwesen

10.2.1 Datenschutzkontrollzuständigkeit für die SGB II-ARGEn: SMS und Sächsischer Datenschutzbeauftragter zusammen auf einem sächsischen Sonderweg

In 12/10.2.16 (auf S. 249 bis 251 oben) habe ich schon näher dargelegt, dass sich seinerzeit den einschlägigen Regelungen des SGB X im Hinblick auf die besondere Konstruktion der im SGB II vorgesehenen *Arbeitsgemeinschaften nach § 44b SGB II* nicht eindeutig hat entnehmen lassen, inwieweit die Datenschutzkontrollzuständigkeit dem Bundes- oder aber dem Landesdatenschutzbeauftragten zugewiesen gewesen ist.

Wegen dieser Uneindeutigkeit der rechtlichen Regelung habe ich keine Grundlage dafür gesehen, von der seinerzeit gemeinsam von Landesdatenschutzbeauftragten und Bundesdatenschutzbeauftragtem gefundenen „pragmatischen“ Lösung abzuweichen, die darauf hinausgelaufen ist, dass zwar von Hause aus der LfD zuständig, für die zentralen Vorgaben, welche die Bundesagentur für Arbeit (BA) den SGB II-ARGEn macht, jedoch der BfDI zuständig sein sollte.

(A) Dieser - weder rechtlich noch auch praktisch wirklich befriedigenden - Praxis hat dann jedoch im Sommer 2006 der Gesetzgeber die Grundlage entzogen.

Rechtlich und aus diesem Grunde auch tatsächlich unbefriedigend war diese Praxis insofern, als vielfach die ARGEn sich als verlängerten Arm der BA und damit einer Bundesbehörde verstanden und sich deswegen gegen Datenschutzkontrollen durch die Landesdatenschutzbeauftragten gesperrt haben; in der milderen Form, die auch in Sachsen vorgekommen ist, haben die ARGEn datenschutzrechtliche Fragen nicht selbst beantwortet, sondern deren Beantwortung der BA überlassen. Es war deshalb auch nicht übertrieben, wenn einer meiner von dem Abwehrverhalten der ARGEn besonders betroffener Kollege von einem System der Verantwortungslosigkeit gesprochen hat. (Dies war auch die Zeit, als der Schlussbericht des Hartz-IV-Ombudsrates, unter Beteiligung des früheren sächsischen Ministerpräsidenten Prof. Biedenkopf, die unselbständige Organisation der Arbeitsgemeinschaften für untauglich erklärt und klare Weisungsverhältnisse gefordert hat.)

Mit dem Gesetz zur Fortentwicklung der Grundsicherung für Arbeitsuchende vom 20. Juli 2006 (BGBl. I S.1706) hat dann der Gesetzgeber mit Wirkung ab dem 1. August 2006 in § 50 n. F. SGB II Folgendes bestimmt:

> Soweit Arbeitsgemeinschaften die Aufgaben der Agenturen für Arbeit wahrnehmen (§ 44b Abs. 3 Satz 1), ist die Bundesagentur verantwortliche Stelle nach § 67 Abs. 9 des Zehnten Buches.

(B) Daraufhin habe ich mit Schreiben vom 4. August 2006 dem BfDI sowie meinen Kollegen in den anderen Bundesländern mitgeteilt, dass ich aufgrund einer genaueren Untersuchung der nunmehr geltenden Fassung des SGB II, unter Einbeziehung der im Gesetzgebungsverfahren vorgenommenen Änderungen des Entwurfs der Koalitionsfraktionen, zu dem Ergebnis käme, dass für die Datenschutzkontrolle der Tätigkeit der Arbeitsgemeinschaften nach § 44b SGB II, *soweit sie die Aufgaben der Agenturen für Arbeit (Bundesagentur für Arbeit) wahrnehmen, ausschließlich der Bundesdatenschutzbeauftragte zuständig ist*.

(C) Ich habe mich zunächst darauf beschränkt, diese Auffassung unter den Datenschutzbeauftragten von Bund und Ländern zur Diskussion zu stellen, und zugleich angekündigt, dass ich mich bemühen wollte, Stellen, die auf die Bundesgesetzgebung Einfluss haben, auf das Problem aufmerksam und damit ‚bösgläubig' zu machen. Außerdem habe ich angekündigt, dass ich, sofern ich nicht mit besseren Argumenten von der Unrichtigkeit meiner Auffassung überzeugt würde, nach Ablauf einer angemessenen Frist von ca. einem dreiviertel Jahr meine Datenschutzkontrolle, was die Tätigkeit der SGB II-ARGEn in Erfüllung der Aufgaben der BA betrifft, auslaufen zu lassen, mich bis dahin aber an die bis dahin geübte faktische Arbeitsteilung zu halten. Weil Vereinbarungen unter Datenschutzkontrollbehörden (LfDen, BfDI) keine Datenschutzkontrollzuständigkeit begründen könnten, habe ich dazu aufgefordert, auf den Gesetzgeber einzuwirken, eine befriedigende Lösung herbeizuführen.

Hintergrund der von mir genannten Frist war die Erwartung, dass im Frühjahr 2007 das Bundesverfassungsgericht aufgrund der bei ihm zu den Aktenzeichen 2 BvR 2433/04 und 2434/04 anhängigen Verfassungsbeschwerden von elf Landkreisen, darunter neben fünf bayerischen immerhin vier sächsische, eine Klärung verschiedener die Beteiligung der Kommunen an der Ausführung des SGB II betreffender verfassungsrechtlicher Fragen herbeiführen werde.

Im Oktober 2006 habe ich dann auf der 72. Konferenz der Datenschutzbeauftragten des Bundes und der Länder zusammen mit meinen Kollegen aus Brandenburg und Nordrhein-Westfalen diese Position bei der Diskussion zur Datenschutzkontrollzuständigkeit dezidiert zum Ausdruck gebracht.

(D) Nachdem ich in der Zuständigkeitsfrage aber zunächst insbesondere auch in Sachsen nichts weiter unternommen und insbesondere auch nicht dem SMS meine

Überlegungen zu erkennen gegeben hatte, teilte mir das Staatsministerium Ende Oktober mit, dass es beabsichtige, auf einen von der Linkfraktion.PDS unter LT-DS-Nr.: 4/6592 Ende September 2006 eingebrachten Antrag, die Staatsregierung durch Landtagsbeschluss zu ersuchen, sich gegenüber der Bundesregierung und im Bundesrat dafür einzusetzen, dass *die umfassende und uneingeschränkte datenschutzrechtliche Kontrolle der Verarbeitung von Sozialdaten durch die nach § 44 SGB II errichteten Arbeitsgemeinschaften durch die Datenschutzbeauftragten der jeweiligen Bundesländer gewährleistet werde*, zu antworten, dass sie der Auffassung sei, dass nach der Novellierung des SGB II gemäß dessen § 50 Abs. 2 die BA verantwortliche Stelle im Sinne von § 67 Abs. 9 SGB X sei, soweit die ARGEn die Aufgaben der Agenturen für Arbeit wahrnehmen, und dass deswegen, weil die BA eine öffentliche Stelle des Bundes sei, gemäß § 80 Abs. 6 Satz 1 SGB X i. V. m. § 24 Abs. 1 Satz 1 BDSG der BfDI insoweit für die Datenschutzkontrolle zuständig sei, weswegen nach dieser kürzlich erfolgten gesetzlichen Klarstellung die Staatsregierung eine erneute Gesetzesinitiative zum Sachverhalt weder für notwendig noch für aussichtsreich halte. Das SMS war also - ich betone es noch einmal - völlig unabhängig von mir zu demselben rechtlichen Ergebnis gekommen!

Nachdem das SMS diese Antwort unter dem Datum des 6. November 2006 (Az: 43-0141.53-06/131, zu LT-DS-Nr. 4/6592) öffentlich erteilt hatte und nachdem aus Anfragen einzelner ARGEn zu meiner datenschutzrechtlichen Kontrollzuständigkeit in diesen Wochen zu erkennen gewesen war, dass der Antrag in einigen ARGEn in Sachsen wohl bekannt gewesen ist, habe ich dem BfDI mitgeteilt, dass ich mich im Hinblick darauf, dass diese Stellungnahme der Sächsischen Staatsregierung auch den sächsischen ARGEn notwendig bekannt werde, nicht in der Lage sähe, der Staatsregierung zu widersprechen und meine Kontrolltätigkeit betreffend die sächsischen SGB II-ARGEn bis März 2007 fortzuführen. Zugleich habe ich dem BfDI angekündigt, eine solche Änderung meiner Praxis in Sachsen demnächst bekannt zu machen und die dann nötigen Abgrenzungen der Zuständigkeit für die künftige Bearbeitung von Eingaben sowie bei Kontrollen im Bereich der SGB II-ARGEn zu erarbeiten.

(E) Mit Schreiben vom 7. Dezember 2006 habe ich dann den SGB II-ARGEn des Freistaates Sachsen mitgeteilt, dass meine datenschutzrechtliche Kontrollzuständigkeit nunmehr auf folgende Tätigkeiten der ARGEn beschränkt sei:

Erbringung von Leistungen zur Eingliederungshilfe im Hinblick auf

- die Betreuung minderjähriger oder behinderter Kinder oder die häusliche Pflege von Angehörigen,
- die Schuldnerberatung,
- die psychosoziale Betreuung,
- die Suchtberatung (§ 16 Abs. 2 Satz 1 Nr. 1 bis 4)

sowie

- die Erbringung von Leistungen für Unterkunft und Heizung (§ 22),
- die Leistungen für Erstausstattungen für die Wohnung einschließlich Haushaltsgeräten,
- die Erstausstattung für Bekleidung einschließlich bei Schwangerschaft und Geburt

und

- bei mehrtägigen Klassenfahrten im Rahmen der schulrechtlichen Bestimmungen (§ 23 Abs. 3).

Soweit die Behörden personenbezogene Daten ausschließlich zur Erfüllung dieser Aufgaben verarbeiteten, unterlägen sie unverändert meiner datenschutzrechtlichen Kontrolle.

Daneben gibt es jedoch die der Aufgabenerfüllung beider in der ARGE zusammenarbeitenden Träger zugleich dienende Verarbeitung personenbezogener Daten; dies betrifft beispielsweise alle Grunddaten wie Namen, Anschrift, Einkommen, Vermögen, Mitglieder der Bedarfsgemeinschaft usw. - diese Daten werden von der SGB II-ARGE sowohl zur Erfüllung von Aufgaben der BA als auch in Erfüllung der Aufgaben der kommunalen Träger verarbeitet. Zur Begründung dafür, dass insoweit meiner Auffassung nach nicht der BfDI und der jeweilige LfD gleichermaßen für die Datenschutzkontrolle zuständig seien und dass, zum anderen, die ausschließliche Datenschutz-Zuständigkeit des BfDI insoweit bestehe, habe ich Folgendes ausgeführt:

(1) Eine doppelte Bearbeitung von Anfragen und Kontrollen könnte im Ergebnis auch unterschiedlich ausfallen. Eine solche Doppelbearbeitung wäre jedoch nicht nur ineffizient und widerspräche den Grundsätzen der Datenvermeidung und Datensparsamkeit, sondern sie stellte auch einen Verstoß gegen das Rechtsstaatsgebot dar: Die Tätigkeit des unabhängigen Datenschutzbeauftragten ist nach dem Volkszählungsurteil des BVerfG (BVerfGE 65, 1, 46 unten) als eine Art „vorgezogenen Rechtsschutzes“ anzusehen. Wie bei der eigentlichen Rechtsweggarantie des Art. 19 Abs. 4

GG muss das Ergebnis der Durchführung des zwecks Grundrechtsschutzes zur Klärung der Rechtslage dienenden Verfahrens ein eindeutiges sein. Doppel-Verfahren - also Verfahren betreffend denselben rechtlichen Gegenstand (Verfahrensgegenstand) infolge Doppelzuständigkeit und Doppeldurchführung widersprächen dem.

Daraus folgt, dass auch für den Bereich der Verarbeitung mit Doppel-Zweck die datenschutzrechtliche Kontrolle „aus einer Hand“ gewährleistet werden muss. Bislang haben der BfDI und die LfDen angenommen, dass eine Kontrolle (allein) aus der einen Hand des jeweiligen LfD erfolgt. Diese Auffassung ist jedoch bereits dort an ihre Grenzen gestoßen, wo Datenverarbeitungsprogramme und Vordrucke allein von der BA vorgegeben werden und die BA eine Unterwerfung unter die Vorschriften des Landesdatenschutzgesetzes verneint bzw. eine Kontrolle durch die LfDen insoweit verweigert - wie in Sachsen geschehen - und sich damit einer Kontrolle des LfD entzieht.

Datenschutz aus der einen Hand des LfD kann somit nicht gewährleistet werden. Dies kann nur zur Folge haben, dass sie aus der einen Hand des BfDI erfolgen muss.

(2) Dies ist offenbar auch der Wille des Gesetzgebers, wie folgendes Zitat belegt:

Allgemeiner Teil der Begründung des Entwurfs der Koalitionsfraktionen für das *Gesetz zur Fortentwicklung der Grundsicherung für Arbeitsuchende* (BT-DS 16/1410, vom 9. Mai 2006), Abschnitt „Verbesserung der Verwaltungspraxis“, vierter Spiegelstrich:

> „Im Interesse der Rechtsklarheit sollten die datenschutzrechtlichen Zuständigkeiten eindeutig zugeordnet werden. Die Bundesagentur für Arbeit soll die datenschutzrechtlich verantwortliche Stelle für die im Rahmen des Zweiten Buches Sozialgesetzbuch erhobenen, verarbeiteten und genutzten Daten sein.“ (Gemeint sind natürlich, wie im § 67 Abs. 9 SGB X, die Verarbeitungshandlungen, nicht die Daten.)

Auch das Gewicht der Aufgabenverteilung der ARGE entspricht diesem Ansatz. Der überwiegende Teil der Aufgaben (Grundsicherung, Förderung, Arbeitsvermittlung) gehört zum Verantwortungsbereich der BA, der kleinere Teil der Kosten der Unterkunft und der Leistungen zur Eingliederungshilfe gehört zu demjenigen der kommunalen Träger. Dieser Schwerpunkt der Aufgabenerfüllung findet sich auch im Gesetz selbst, das vom Grundsatz der Allzuständigkeit der BA in § 6 Abs. 1 Satz 1 Nr. 1 SGB II („soweit Nummer 2 nichts anderes bestimmt“) ausgeht oder etwa in § 51b Abs. 5 SGB II regelt, dass letztlich allein die BA die Befugnis hat, Verwal-

tungsvorschriften zum Umfang der der nach den Absätzen 1-3 der Vorschrift zu erhebenden und zu übermittelnden Daten zu erlassen.

(3) Aus diesen Überlegungen ergibt sich für Eingaben hinsichtlich meiner Kontrollzuständigkeit folgendes Prüfungsschema:

Betrifft die Petition eine Datenverarbeitung der SGB II-ARGE zur Erfüllung der Aufgaben nach § 6 Abs. 1 Satz 1 i. V. m. § 16 Abs. 2 Satz 2 Nr. 1-4, §§ 22, 23 Abs. 3 SGB II?

[1] Wenn ja, volle Kontrolle durch den LfD.

[2] Wenn nein, Abgabe an den BfDI.

[3] Wenn sowohl Aufgaben nach § 6 Abs. 1 Satz 1 Nr. 1 SGB II als auch nach § 6 Abs. 1 Satz 1 i. V. m. § 16 Abs. 2 Satz 2 Nr. 1-4, §§ 22, 23 Abs. 3 SGB II, dann ebenfalls Abgabe an den BfDI.

(F) Von dieser Mitteilung an die sächsischen SGB II-ARGEn habe ich mit Schreiben vom folgenden Tage den BfDI unterrichtet (und dazu ergänzend auf einen Beschluss des Sozialgerichts Leipzig vom 2. August 2006, Az: S 1 AS 411/05 ER, hingewiesen, in welchem die SGB II-Arbeitsgemeinschaft als institutionalisierter Verwaltungshelfer qualifiziert wird, dem die „verwaltungstechnische Abwicklung“ obliege, der sich in vielen Einzelfragen beim eigentlichen Aufgabenträger rückversichere und nicht in dem Sinne passiv legitimiert sei, dass er selbst den materiellen Anspruch auf Leistungen zu erfüllen hätte; in dem Beschluss werde die Unklarheit bzw. Kompliziertheit der gesetzlichen Regelung deutlich).

Der BfDI hat dies widerstrebend zur Kenntnis genommen. Von meinen Kollegen ist keiner mir gefolgt, wenn mir auch der eine oder andere zu verstehen gibt, dass er meinen Standpunkt für den einzig rechtlich richtigen hält. Dieses Geschehen wiederum hat auf Seiten des BMAS zu neuen Aktivitäten geführt.

(G) In diesem Zusammenhang hat das BMAS eine „vollumfängliche datenschutzrechtliche Kontrollzuständigkeit der Landesbeauftragten“ für die SGB II-ARGEn im Wesentlichen auf § 80 Abs. 6 Satz 2 und 3 SGB X zu stützen versucht. Das ist, wie ich geltend gemacht habe, aus mehr als einem Grund nicht richtig:

(1) Zum einen trifft es bereits nicht zu, dass die ARGEn (Sozial-)Daten *nach § 80 Abs. 1 SGB X* im Auftrag für die Agentur für Arbeit (BA) verarbeiten. Eine Auftragsdatenverarbeitung gemäß § 80 SGB X liegt nämlich nur dann vor, wenn sich

eine (speichernde) Stelle eines Dienstleisters bedient, der in vollständiger Abhängigkeit von ihren die Art und den Umfang der Datenverarbeitung betreffenden Vorgaben für sie Sozialdaten verarbeitet. (Der Auftragnehmer ist weitgehend und namentlich in der Hinsicht datenschutzrechtlich als eine Einheit mit der betreffenden Stelle anzusehen, dass die Datenweitergabe zwischen beiden Stellen keine Übermittlung im Sinne des § 67 Abs. 6 SGB X ist.) Wird jedoch auch die zugrundeliegende (gesetzliche) Verwaltungsaufgabe des auftraggebenden Leistungsträgers übertragen, so ist § 80 SGB X nicht anwendbar (Kasseler Kommentar/Scholz, Rdnr. 7 zu § 80 SGB X; Hauck/Noftz/Rombach, Rdnrn. 6, 20, 22 zu § 80 SGB X; v. Wulfen/Roos, Rdnr. 3 zu § 80 SGB X; vgl. auch Simitis/Waltz, Rdnr. 17 zu § 11 BDSG).

Eben eine solche Aufgabenübertragung von den Agenturen für Arbeit auf die ARGEn regelt jedoch § 44b Abs. 3 SGB II, so dass eine Datenverarbeitung im Auftrag nach § 80 SGB X eben tatbestandlich ausgeschlossen ist: Übertragen ist nicht lediglich die Aufgabe der Verarbeitung personenbezogener Daten, sondern das gesamte Verwaltungshandeln, dem diese Verarbeitung dient (sog. Funktionsübertragung, im Allgemeinen, auch im Falle des § 88 SGB X, mit der Folge des vollständigen Überganges aller datenschutzrechtlichen Pflichten, v. Wulfen/Roos a. a. O., m. w. N.).

(2) Dass § 80 SGB X auf dieses Verhältnis zwischen Agentur für Arbeit und ARGEn nicht passt, wird auch dadurch deutlich, dass die Absätze 2 bis 4 der Vorschrift auf eine gesetzliche Aufgabenübertragung, wie sie hier vorliegt, im Wesentlichen nicht sinnvoll anwendbar sind.

(3) Schließlich begründet eine Anwendung des § 80 Abs. 6 SGB X - für den es nach meinem Kenntnisstand kaum praktische Anwendungserfahrungen gibt - nicht diejenige Zuständigkeitsaufteilung, die das BMAS wünscht. Die in § 80 Abs. 1 Satz 1 SGB X dem Auftraggeber übertragene uneingeschränkte datenschutzrechtliche Verantwortlichkeit hat zur Folge, dass der für den Auftraggeber zuständige Datenschutzbeauftragte über diesen diejenigen Verarbeitungshandlungen, die dem Auftragnehmer übertragen worden sind, weitgehend zu kontrollieren hat, mangels unmittelbarer Zuständigkeit für den Auftragnehmer aber eben lediglich nur mittelbar, mit der Folge, dass § 80 Abs. 6 SGB X eine weitgehende Doppelzuständigkeit begründet. Konkret ausgedrückt: Verarbeitet eine Landesstelle weisungsgemäß (rechtswidrig) Sozialdaten im Auftrag einer Bundesstelle, so ist das Recht des Betroffenen, wegen dieser vom Auftraggeber zu verantwortenden (§ 80 Abs. 1 Satz 1 SGB X) Verarbeitung den BfDI anzurufen (§ 81 Abs. 1 Nr. 1 SGB X) durch die durch § 80 Abs. 6 Satz 2 gegebene Möglichkeit des Betroffenen, in Hinblick auf das Tätigwerden des Auftragnehmers auch den Landesdatenschutzbeauftragten anzurufen,

nicht beschränkt (§ 80 Abs. 6 Satz 2 SGB X lässt nicht etwa generell, sondern nur im Hinblick auf die Zuständigkeit für den *Auftragnehmer* den Landesdatenschutzbeauftragten an die Stelle des Bundesdatenschutzbeauftragten treten).

(4) Abgesehen davon war auch der BfDI bis dahin davon ausgegangen, dass es sich *nicht* um einen Fall des § 80 SGB X handelt: Im September 2006 hatte er in der gesetzlichen Konstruktion eine „Konzeption sui generis" gesehen, auf die Regeln für die Datenverarbeitung im Auftrag - lediglich! - „analog" anwendbar seien, weil eine Ähnlichkeit mit der Auftragsdatenverarbeitung bestehe. Im August 2006 hatte der BfDI zuvor sogar betont, dass die BA den ARGEn *keine Weisungen nach § 80 SGB X* erteilen könne.

Der Weg zu einer solchen *Analogie* ist jedoch durch die klare Regelung des § 50 Abs. 2 SGB II versperrt. Diese Spezialregelung (vgl. auch § 37 SGB I) ist so konkret, dass sie es ausschließt, hinsichtlich ihres Regelungsinhaltes ersetzend oder ergänzend auf allgemeinere, ähnliche Regelungen zurückzugreifen. Der Wortlaut des § 50 Abs. 2 SGB II ist insofern eindeutig, dass man ihm gerade nicht entnehmen kann, dass er eine verteilte Verantwortlichkeit zuweise oder sonst vorsehe. Vielmehr enthält § 50 Abs. 2 SGB II eine eindeutige und, wie die Stellung im Gesetz zeigt, gerade in datenschutzrechtlicher Hinsicht maßgebliche Regelung der Verantwortung für die Verarbeitung personenbezogener Daten. Danach ist die BA - die eine - verantwortliche Stelle, soweit die ARGEn die Aufgaben der Agentur für Arbeit wahrnehmen. In diesem Sinne heißt es auch im allgemeinen Teil der Begründung des Entwurfes der Koalitionsfraktionen für das *Gesetz zur Fortentwicklung der Grundsicherung für Arbeitsuchende*, BT-Drs.: 16/1414, vom 9. Mai 2006, im Abschnitt „Verbesserung der Verwaltungspraxis" zum vierten Spiegelstrich: „Im Interesse der Rechtsklarheit sollen die datenschutzrechtlichen Zuständigkeiten eindeutig zugeordnet werden. Die Bundesagentur für Arbeit soll die datenschutzrechtlich verantwortliche Stelle für die im Rahmen des Zweiten Buches Sozialgesetzbuch erhobenen, verarbeiteten und genutzten Daten sein" (gemeint sind natürlich, wie in § 67 Abs. 9 SGB X, die Verarbeitungshandlungen, nicht die Daten).

(5) Soweit schließlich das BMAS (in dem genannten Schreiben vom 14. Dezember 2006) die gemäß § 44b Abs. 3 Satz 4 SGB II bestehende Aufsicht der zuständigen obersten Landesbehörde als Argument für die Datenschutzkontrollzuständigkeit der LfDen bemüht, sei auf die zugleich bestehende Rechts- und Fachaufsicht verwiesen, die das BMAS gemäß § 47 Abs. 1 Satz 1 und 2 SGB II über die BA ausübt, soweit diese Leistungen nach dem SGB II erbringt:

Das BMAS kann Weisungen erteilen und die BA an seine Auffassung binden. Anders verhält es sich bei der Aufsicht der obersten Landesbehörden gemäß § 44b Abs. 3 Satz 4 SGB II. Gemäß § 94 Abs. 2 SGB X, der ausweislich des § 44b Abs. 3 Satz 2, 2. Halbs. SGB II Anwendung findet, gelten die Regelungen der §§ 85, 88, 90, 90a SGB IV entsprechend. Die Rechtsaufsicht der Landesbehörde besteht demzufolge vorrangig aus Informations- und Prüfungsrechten (§ 88 SGB IV). Da § 89 SGB IV, mangels Verweisung, nicht anwendbar ist, sind die Landesbehörden nicht befugt, die ARGEn zu verpflichten, Rechtsverstöße zu beseitigen (siehe dazu Hauck/Noftz/ Luthe, SGB II, § 44b, Rdnr. 17).

In diesem Aufsichtssystem kann eine Tätigkeit des Sächsischen Datenschutzbeauftragten kaum Wirkung entfalten. Selbst wenn von seiner Kontrollzuständigkeit ausgegangen würde, könnte das SMS als Aufsichtsbehörde keine Abhilfe - etwa bei datenschutzrechtlichen Beanstandungen - schaffen. Etwas anderes gilt für das BMAS, welches sogar über die Fachaufsicht verfügt.

(H) Meine Auffassung habe ich dem BVerfG zur Berücksichtigung in den beiden o. g. Verfassungsbeschwerdeverfahren unterbreitet, und ich habe dabei darauf verweisen können, dass ich für meine rechtlichen Überlegungen auch unter ARGE-Praktikern Zustimmung gefunden hätte. Das Gericht hat sie den Verfahrensbeteiligten zur Kenntnis gegeben und in der mündlichen Verhandlung am 24. Mai 2007 neben vielen anderen Problemen, welche die Konstruktion der SGB II-ARGEn mit sich bringt, auch Datenschutz-Fragen angesprochen und sich dabei auf deren „eindrucksvolle Schilderung durch den Sächsischen Datenschutzbeauftragten“ bezogen.

Es bleibt abzuwarten, wie das Gericht entscheiden wird. Man wird nicht erwarten können, dass der Bundesgesetzgeber sich mit der Konstruktion der SGB II-ARGEn beschäftigen wird, bevor diese Entscheidung des Gerichts ergangen sein wird. Bis dahin wird es bei der bisherigen Praxis bleiben, die ja nicht bedeutet, dass ich mit Fragen des SGB II nicht befasst wäre, zumal Sachsen mit den Landkreisen Bautzen, Döbeln, Kamenz, Löbau-Zittau, Meißen und dem Muldentalkreis eine vergleichsweise hohe Anzahl an Options-Kommunen hat (selbstverständlich datenschutzrechtlich Landes-Stellen). Einzelfragen zum SGB II werden entsprechend in Abschnitt 10.2.5 bis 10.2.9 behandelt.

(I) In der Zeit bis zur Entscheidung des Gerichts bzw. zu einer anschließenden Gesetzesänderung bleiben aber auch für die zurzeit außerhalb Sachsen herrschende Praxis noch Streitfragen: Die BA will, so berichten jedenfalls einige Kollegen, in den ARGEn - wohl um die Sache fest in der Hand zu behalten - kein Landesdatenschutz-

recht angewendet wissen, soweit es um die Bestellung behördlicher Datenschutzbeauftragter geht. Das widerspricht wegen § 81 Abs. 4 Satz 3 und 4 SGB X der für eine Zuständigkeit der Landesdatenschutzbeauftragten wegen § 80 Abs. 2 Satz 1 und 2 SGB X notwendigerweise vorzunehmenden Einordnung der ARGEn als *Länder*-Stellen.

10.2.2 Datenerhebung der Krankenkasse für Zwecke der Beitragsberechnung über die vom freiwillig Versicherten getätigten Ausgaben

In der Praxis kommt es immer wieder zu Fällen, in denen freiwillig versicherte Mitglieder ihre beitragspflichtigen Einnahmen derart gering ausweisen, dass sich für die Krankenkasse bei der Beitragsberechnung berechtigterweise die Frage stellt, wovon diese Krankenkassenmitglieder ihren Lebensunterhalt bestreiten, und sich daher der Verdacht aufdrängt, dass das Mitglied unrichtige Angaben zu seinen Einnahmen gemacht hat, letztlich im Hinblick auf seine beitragsrechtliche Einstufung. Die Frage war nun, ob die Krankenkasse zumindest in diesen Fällen berechtigt ist, zur Prüfung der Stimmigkeit der Angaben das Mitglied nicht nur zu seinen *Einnahmen*, sondern auch nach seinen (monatlichen) *Ausgaben* zu befragen.

Ich habe die mir von der Krankenkasse gestellte Frage bejaht, und zwar aus folgenden Gründen:

Als Rahmenbedingung schreibt § 240 Abs. 1 Satz 2 SGB V für die Beitragsberechnung zur freiwilligen Krankenversicherung vor, dass die Beitragsbelastung die gesamte wirtschaftliche Leistungsfähigkeit des freiwilligen Mitglieds berücksichtigen muss. Der Beitragsberechnung dürfen somit nicht pauschal bestimmte Einnahmen zum Lebensunterhalt unterstellt werden, ohne dass die wirtschaftliche Leistungsfähigkeit konkret und individuell geprüft wird. Eine Prüfung der Verhältnisse im Einzelfall hinsichtlich der tatsächlich erzielten Einnahmen ist daher rechtlich erforderlich, und die Krankenkasse ist gemäß § 284 Abs. 1 Nr. 3 SGB V daher auch berechtigt, die für die Beitragsberechnung insoweit erforderlichen Daten zu erheben. Insoweit ist die Krankenkasse auch berechtigt zu prüfen, ob der Beitragssatz nur nach dem Mindesteinkommen zu berechnen ist, das heißt ob die Einnahmen des Versicherten diesen Wert auch tatsächlich nicht überschreiten.

Den Nachweis der wirtschaftlichen Leistungsfähigkeit hat der Versicherte durch die Vorlage von Unterlagen zu erbringen. Gemäß § 206 SGB V ist der Versicherte verpflichtet, der Krankenkasse auf Verlangen über alle für die Feststellung der Versicherungs- und Beitragspflicht und für die Durchführung der der Krankenkasse übertragenen Aufgaben erforderlichen Tatsachen Auskunft zu erteilen. Der Versicherte

hat auf Verlangen der Krankenkasse dieser die Unterlagen, aus denen die Tatsachen oder die Änderungen der Verhältnisse hervorgehen, vorzulegen.

Soweit auch nach Vorlage entsprechender Einkommensnachweise bei der Krankenkasse weiterhin Anlass zu der Vermutung besteht, dass der Versicherte seiner Pflicht, wahrheitsgemäße Angaben bezüglich seines tatsächlichen monatlichen Einkommens zu machen, nicht nachgekommen ist - aber auch erst dann -, halte ich zu Plausibilisierungszwecken eine Datenerhebung bezüglich der monatlich erfolgenden Ausgaben, als *Hilfstatsachen*, für zulässig (vgl. die gleiche Problematik bei der Erhebung von Sollbuchungen im Rahmen von Sozialhilfe und SGB II).

Eine generelle Datenerhebung ohne Vorliegen konkreter Anhaltspunkte, in Gestalt einer Abfrage (mittels Fragebogen) bei sämtlichen Versicherten, halte ich dagegen für nicht erforderlich und damit für unzulässig (vgl. Beschluss des Hessischen Verwaltungsgerichtshofs vom 7. Februar 1995, RDV 1995, 175).

10.2.3 Datenübermittlung durch MDK bzw. Krankenkasse (Pflegekasse) an das Jugendamt bei Verdacht einer Kindeswohlgefährdung

Eine Krankenkasse hatte durch Zusatz-Angaben in einem ihr vom MDK übersandten Gutachtens Kenntnis von gravierenden Mängeln im häuslichen Lebensumfeld eines 13-Jährigen erhalten: Das Gutachten enthielt neben den von der Kasse in Auftrag gegebenen Feststellungen zur Pflegebedürftigkeit (einer anderen Person) auch Hinweise zum Zustand der Wohnung des Jungen (Auszug aus dem Gutachten: „*Im gesamten Wohnbereich verschmutzte Kleidung, Gerümpel, Abfälle etc., Kinderzimmer befindet sich im Erdgeschoss, ungeheizt, nur Betonfußboden mit zwei völlig verdreckten Betten* ...“). Die Krankenkasse wollte von mir wissen, ob sie die vom MDK mitgeteilten Angaben über die Lebensumstände des Jungen an das Jugendamt wegen des Verdachts auf Kindeswohlgefährdung weitergeben dürfe.

Ich bin zu folgender Rechtsauffassung gelangt:

(1) Die Rechtsgrundlage, die für eine Übermittlung von einer unter § 35 Abs. 1 SGB I fallenden Stelle bekannt gewordenen Tatsachen, die den Verdacht einer Kindeswohlgefährdung begründen (Sozialdaten nach § 67 Abs. 1 Satz 1 SGB X), erforderlich ist, ergibt sich im Bereich der *Krankenversicherung* aus § 284 Abs. 3 Satz 1, 2. Halbsatz SGB V, § 69 Abs. 1 Nr. 1, 3. Fall SGB X. Danach ist die Verarbeitung, d. h. also auch die Übermittlung, von Sozialdaten, die ursprünglich für Zwecke der Krankenversicherung erhoben worden sind, auch für andere Zwecke zulässig, soweit dies durch Rechtsvorschriften des Sozialgesetzbuchs angeordnet oder

erlaubt ist. Dies ist insbesondere der Fall, soweit die §§ 67 ff. SGB X die Übermittlung an Dritte zulassen (Kranig in Hauck/Noftz, SGB V, § 284 Rdnr. 41).

Als „gesetzliche Aufgabe nach dem Gesetzbuch“ gemäß § 69 Abs. 1 Nr. 1, 3. Fall SGB X ist jede Aufgabe zu verstehen, die sich aus dem Sozialgesetzbuch insgesamt ergibt (siehe hierzu 12/10.2.10). Die Übermittlung von Sozialdaten ist hier erforderlich, damit ein Jugendamt seine Aufgaben insbesondere nach § 8a SGB VIII, aber auch nach § 27 ff. SGB VIII, erfüllen kann. Gemäß § 8a Abs. 1 Satz 1 SGB VIII hat das Jugendamt bei Vorliegen gewichtiger Anhaltspunkte für eine Kindeswohlgefährdung entsprechend tätig zu werden. Dabei ist das Jugendamt gerade bei seiner Aufgabe nach § 8a SGB VIII in besonderer Weise auf die Mitteilung entsprechender Angaben durch Dritte angewiesen.

Die Erhebungsbefugnis des Jugendamts ergibt sich ungeachtet ungenauer Ausdrucksweise des Gesetzgebers aus § 62 Abs. 3 Nr. 2, Buchst. d SGB VIII.

(2) Die für die Übermittlung erforderliche Befugnis im Bereich der *Pflegeversicherung* ergibt sich für die Pflegekasse aus § 94 Abs. 2 Satz 1 SGB XI i. V. m. § 69 Abs. 1 Nr. 1, 3. Fall SGB X. Im Übrigen gelten die unter 1 gemachten Ausführungen auch für die Pflegekasse.

(3) Die Befugnis zur Datenübermittlung gemäß § 284 Abs. 3 Satz 1, 2. Halbsatz SGB V, § 69 Abs. 1 Nr. 1, 3. Fall SGB X setzt jedoch, wenn der Übermittlung wie hier eine entsprechende Datenerhebung der Krankenkasse vorausgegangen ist, voraus, dass die übermittelnde Stelle die Daten *rechtmäßig* erhoben hat. § 284 Abs. 3 Satz 1 SGB V besagt ausdrücklich, dass die Befugnis der Krankenkasse sich nur auf rechtmäßig erhobene Daten bezieht, die Rechtswidrigkeit der Erhebung macht somit eine weitere Verwendung der Sozialdaten unzulässig (Kranig a. a. O.), selbst dann, wenn eine Übermittlung - wie hier - isoliert betrachtet an sich zulässig wäre (Waschull in Krauskopf, Kommentar, § 284 SGB V Rdnr. 64).

Eine entsprechende ausdrückliche Festlegung auf die Übermittlung lediglich rechtmäßig erhobener Sozialdaten fehlt in § 94 Abs. 2 Satz 1 SGB XI. Jedoch kann meiner Auffassung nach im Bereich des SGB XI nichts Anderes gelten als nach § 284 Abs. 3 Satz 1, 2. Halbsatz SGB V. Auch nach § 94 Abs. 2 Satz 1 SGB XI ist somit Voraussetzung, dass es sich um rechtmäßig erhobene Sozialdaten handelt, die übermittelt werden sollen.

Daran fehlte es jedoch in dem mir geschilderten Fall. Denn es ist keine gesetzliche Regelung ersichtlich, die die Kasse berechtigt, beim MDK die betreffenden Angaben

in Bezug auf die häuslichen Lebensumstände des Kindes, die nun dem Jugendamt übermittelt werden sollen, zu *erheben*.

Wie die Krankenkasse mir gegenüber selbst einräumte, wurden ihr die betreffenden Hinweise und Anmerkungen vom MDK *neben* den üblichen Feststellungen zur Pflegebedürftigkeit mitgeteilt. Diese Angaben hätte die AOK Sachsen jedoch bereits gar nicht vom MDK erheben oder gar speichern dürfen. Die Erhebungsbefugnis der AOK umfasst als Krankenkasse vielmehr nur die in § 284 Nr. 7 SGB V i. V. m. § 277 Abs. 1 SGB V genannten Daten sowie als Pflegekasse die in § 94 Nr. 4 i. V. m. § 18 Abs. 6 SGB XI genannten Daten.

Für den MDK hat keine Befugnis bestanden, die betreffenden Hinweise *an die Krankenkasse* zu *übermitteln*. Mit anderen Worten: Die Krankenkasse hätte die betreffenden Angaben über die Lebensumstände des Kindes bereits gar nicht vom MDK erhalten dürfen. Der MDK hätte vielmehr nur selbst auf der Grundlage des § 69 Abs. 1 Nr. 1, letzter Fall SGB X dem Jugendamt (ohne Speicherung!) einen mündlichen Hinweis geben dürfen.

10.2.4 Zuständigkeitserweiterung im Bereich der Rentenversicherung; Datenweitergabe des Rentenversicherungsprüfdienstes an eine Lohnausgleichskasse im Rahmen einer Betriebsprüfung

(1) Die Landesversicherungsanstalten Thüringen, Sachsen-Anhalt und Sachsen haben sich gemäß § 141 SGB VI zu einem Regionalträger der Deutschen Rentenversicherung vereinigt, wobei sich der Zuständigkeitsbereich des vereinigten Trägers genau auf die Bundesländer Sachsen, Sachsen-Anhalt und Thüringen erstreckt und der Hauptsitz dieses Regionalträgers Leipzig ist. Aufgrund dessen handelt es sich bei der Deutschen Rentenversicherung Mitteldeutschland gemäß Art. 87 Abs. 2 Satz 2 GG um eine landesunmittelbare Körperschaft des öffentlichen Rechts, weil die beteiligten Länder ein einzelnes aufsichtsführendes Land bestimmt haben (vgl. § 90 Abs. 3 SGB IV): Durch Art. 1 Abs. 1 des Staatsvertrages über die Bestimmung aufsichtsführender Länder nach Art. 87 Abs. 2 Satz 2 GG, den alle Bundesländer abgeschlossen haben (GVBl. 1997 S. 107) haben insbesondere auch die drei an dem Zusammenschluss zur Deutschen Rentenversicherung Mitteldeutschland beteiligten Bundesländer bestimmt, dass die Aufsicht über einen sozialen Versicherungsträger, dessen Zuständigkeit sich - wie vorliegend - über das Gebiet eines Landes, aber nicht über mehr als drei Länder hinaus erstreckt, jeweils dasjenige Land führt, in dem der Versicherungsträger seinen Sitz hat. Dem Art. 87 Abs. 2 Satz 2 GG zu entnehmenden Gebot, dass es gerade die konkret beteiligten Länder sein müssen, die das

aufsichtsführende Land bestimmen, ist durch die Möglichkeit abweichender Vereinbarungen der konkret beteiligten Länder (Art. 1 Abs. 2 des Staatsvertrages) sowie durch die Kündigungsmöglichkeit (seines Art. 4) Genüge getan (vgl. Hermes in Dreier, GG, Rdnr. 59 zu Art. 87). Die somit bestehende Aufsichtszuständigkeit des Freistaates Sachsen für die Deutsche Rentenversicherung Mitteldeutschland ist mit der Landes-Zugehörigkeit gleichzusetzen, die im Tatbestand des § 81 Abs. 2 Satz 2 SGB X gemeint ist (*öffentliche Stelle des Landes*). Rechtsfolge ist nach dieser Vorschrift dann die Kontrollzuständigkeit des betreffenden Landesdatenschutzbeauftragten, im vorliegenden Falle also diejenige des Sächsischen Datenschutzbeauftragten. Meine Kollegen in den betroffenen Bundesländern sowie im Bund haben sich diesem Ergebnis uneingeschränkt angeschlossen.

Konkret: Ich bin nunmehr insoweit zusätzlich für Sachsen-Anhalt und Thüringen zuständig.

(2) Ein Prüfdienst der Deutschen Rentenversicherung Mitteldeutschland hatte im Rahmen einer nach § 28p SGB IV durchzuführenden Betriebsprüfung festgestellt, dass der Inhaber des betreffenden Handwerksbetriebes bestimmte Einmalzahlungen einer Sozialkasse, konkret handelte es sich um eine Lohnausgleichskasse, entgegen den einschlägigen gesetzlichen Bestimmungen nicht an seine Arbeitnehmer ausgezahlt hatte. Der Prüfdienst hatte darüber die betroffene Lohnausgleichskasse informiert, die umgehend die nicht ausgezahlten Beiträge vom Arbeitgeber zurückforderte - insgesamt eine Summe von über 60.000 €. Der Steuerberater des geprüften Arbeitgebers sah in der Unterrichtung der Sozialkasse einen erheblichen Datenschutzverstoß und bat mich um rasche Aufklärung des Falls. Das Ergebnis meiner Prüfung fiel allerdings nicht so aus, wie sich dies der Arbeitgeber wohl gerne gewünscht hätte, denn der Prüfdienst hatte sich meiner Rechtsauffassung nach völlig korrekt verhalten:

Die erforderliche Rechtsgrundlage für die Datenübermittlung seitens des Betriebsprüfdienstes an die Lohnausgleichskasse ergab sich, abweichend von den von der Rentenversicherung zu dem Fall geäußerten Vorstellungen, aus § 69 Abs. 1 Nr. 1, 3. Fall i. V. m. § 69 Abs. 2 Nr. 2 SGB X:

(a) Bei der Lohnausgleichskasse handelt es sich nicht um einen Leistungsträger nach § 35 Abs. 1 SGB I, insbesondere nicht um eine der in § 35 Abs. 1 Satz 4 SGB I abschließend genannten Stellen, dort ist im Bereich der Sozialkassen ausschließlich die Künstlersozialkasse genannt. Die Lohnausgleichskassen sind jedoch insoweit nach § 69 Abs. 2 Nr. 2, 1. Fall SGB X i. V. m. § 4 Abs. 2 TVG einem Leistungsträger *gleichgestellt*.

(b) Die erfolgte Datenübermittlung an die Lohnausgleichskasse konnte vorliegend auf § 69 Abs. 1 Nr. 1, 3. Fall SGB X gestützt werden. Denn zu den Aufgaben der Lohnausgleichskasse zählt nicht nur die Auszahlung bestimmter Einmalzahlungen an den Arbeitgeber, sondern ausweislich des nach Auskunft der betroffenen Lohnausgleichskasse derzeit gültigen Tarifvertrags über die Sozialkassenverfahren auch die Prüfung und insbesondere gegebenenfalls die Geltendmachung eines Rückerstattungsanspruches im Falle von Leistungen für Einmalzahlungen, wenn diese wie hier nicht an die Arbeitnehmer weitergegeben worden sind. Für die Geltendmachung solcher Erstattungsansprüche der Lohnausgleichskasse gegen Arbeitgeber benötigt diese daher die Kenntnis von der Nichtweitergabe der geleisteten Zahlungen für ihre Aufgabenerfüllung. Bedenken hinsichtlich der an die Lohnausgleichskasse vorgenommenen Datenübermittlung, mit der der Prüfdienst die erstattungsberechtigte Sozialkasse über die im Rahmen der Betriebsprüfung festgestellte Nichtauszahlung der betreffenden Einmalzahlungen unterrichtet hatte, waren daher nicht begründet.

10.2.5 Grenzen der Zulässigkeit der Verarbeitung von Daten aus Kontoauszügen durch die SGB II-Behörde

Eine Vielzahl von Eingaben betraf die Frage der Zulässigkeit der Anforderung von Kontoauszügen. Ich habe gegenüber den SGB II-Behörden deutlich gemacht, dass die grundsätzlichen Erwägungen, die ich für das Sozialhilferecht bereits in 9/10.2.6 zu dieser Problematik angestellt habe, auch für den Anwendungsbereich des SGB II gelten.

Das Anfordern von Kontoauszügen ist eine Erhebung von Sozialdaten, die nach § 67a Abs. 1 SGB X nur zulässig ist, wenn die Kenntnis dieser Daten zur Erfüllung einer Aufgabe der erhebenden Stelle erforderlich ist. Das Kopieren und Zur-Akte-Nehmen von Kontoauszügen stellt eine Speicherung personenbezogener Daten dar, die gemäß § 67c Abs. 1 Satz 1 SGB X nur statthaft ist, wenn sie zur Erfüllung der in der Zuständigkeit der verantwortlichen Stelle liegenden gesetzlichen Aufgaben nach dem Sozialgesetzbuch erforderlich ist und für die Zwecke erfolgt, für die die Daten erhoben worden sind.

Auf einem Kontoauszug sind neben Angaben über Einnahmen in der Regel auch eine Vielzahl von Daten enthalten, die für die Aufgabenerfüllung der SGB II-Behörde nicht erforderlich sind. Fordert die Behörde Kontoauszüge pauschal an und kopiert sie diese pauschal ohne teilweise Schwärzung, kommt sie ihrer Pflicht zur datenschutzgerechten Verarbeitung personenbezogener Daten nicht nach.

Datenschutzgerecht ist danach ein Vorgehen in drei Schritten: Die Behörde hat zunächst zu prüfen, welche konkreten personenbezogenen Daten sie für ihre Aufgabenüberfüllung benötigt. Nur die danach erforderlichen Unterlagen darf sie sich vorlegen lassen. Nach der Prüfung der vorgelegten Unterlagen ist in einem zweiten Schritt zu überlegen, ob es ausreichend ist, in der Akte zu vermerken, dass und wann der Nachweis vorgelegen hat. Sollte ein solcher Vermerk nicht ausreichend sein, können Ablichtungen gefertigt werden, auf denen die Angaben, die nicht leistungsrelevant sind, geschwärzt werden müssen.

Die meisten der SGB II-Behörden, die die Vorlage und die Speicherung der Kontoauszüge anders gehandhabt hatten, haben inzwischen eine datenschutzgerechte Lösung entwickelt, die ihrer effizienten Aufgabenerfüllung einerseits und dem Sozialdatenschutz andererseits gerecht werden. Als vorbildlich habe ich die Ausgabe eines Merkblattes für Antragsteller angesehen, das über die Vorlage und Speicherung der Kontoauszüge Auskunft gibt. Dieses Merkblatt habe ich nachfolgend unter 16.3.3 abgedruckt. Ich hoffe, damit noch andere SGB II-Behörden zu einem in dieser Hinsicht datenschutzgerechten und transparenten Antragsverfahren bewegen zu können.

10.2.6 Zur-Akte-Nehmen einer Ablichtung des Personalausweises für die Antragsbearbeitung nach dem SGB II

Ebenfalls im Zusammenhang mit einem Antrag auf Leistungen nach dem SGB II hat mich ein Petent darauf aufmerksam gemacht, dass die SGB II-Behörde eine Kopie seines Personalausweises gefertigt habe. Von mir zur Stellungnahme aufgefordert, räumte die Behörde ein, dass sie bei jeder Antragstellung den Personalausweis des Antragstellers kopiere. Begründet wurde dies damit, dass sich anhand des Personalausweises die Identität des Antragstellers prüfen lasse. Zudem seien die Angaben zum Wohnort für die Zuständigkeitsprüfung erforderlich. Ferner könne das Lichtbild für die Leistungsbearbeitung hilfreich sein, beispielsweise wenn der Antragsteller seinen Ausweis bei seinem persönlichen Vorsprechen in der Behörde nicht dabei habe. In diesem Fall wäre der Antragsteller umsonst gekommen und müsste unter Aufwendung von Fahrtkosten noch einmal, mit Personalausweis, wiederkommen.

Die Behörde war, das musste ich ihr zugestehen, erfindungsreich im Zusammenstellen von Gründen, wozu sie die Kopie des Personalausweises benötigte. An den gesetzlichen Vorschriften kam sie dennoch nicht vorbei:

SGB II-Behörden dürfen für die Bearbeitung von Anträgen nach dem SGB II die Daten erheben und speichern, die für eine ordnungsgemäße Erfüllung ihrer Aufgaben

erforderlich sind. Dies regeln die §§ 67a Abs. 1 Satz 1, 67c Abs. 1 Satz 1 SGB X. Das Zur-Akte-nehmen der Ablichtung eines Personalausweises stellt eine Datenspeicherung dar, die das Grundrecht auf informationelle Selbstbestimmung verletzt, wenn sie für ein ordnungsgemäßes Verwaltungsverfahren nicht erforderlich ist. Sie ist es hier, also im Falle der Bearbeitung von Anträgen auf Sozialleistungen.

Zwar ist es richtig, dass anhand des Personalausweises die Identität des Antragstellers geprüft werden kann. Dafür vollkommen ausreichend ist jedoch das bloße Sichzeigen-lassen des Ausweises. Dies gilt ebenso für die Zuständigkeitsprüfung. Auch das Bestreben der Behörde, die Ausweise im Sinne einer effektiven und bürgerfreundlichen Leistungsbearbeitung zu kopieren, rechtfertigt die Speicherung nicht; dieses Bestreben bekommt einen zynischen Grundton, wenn es Rechtfertigung für einen Grundrechtseingriff sein soll.

Ich habe die Behörde deshalb aufgefordert, das Ablichten des Personalausweises bei jeglicher Antragsbearbeitung nach dem SGB II zu unterlassen und die in den vorhandenen Kopien enthaltenen Daten gemäß § 21 Abs. 2 Satz 1 SächsDSG zu sperren. Die Behörde ist dieser Forderung nachgekommen.

Der darüber informierte Petent hat sich in der Folge an die Presse gewandt und das Ergebnis meiner Datenschutzkontrolle veröffentlicht. Dies hatte zur Folge, dass sich weitere Petenten anderer SGB II-Behörden ebenfalls an mich gewandt haben. Auch diese Behörden haben mir eine datenschutzgerechte Antragstellung zugesichert.

Zu einer ähnlichen Problematik vgl. schon 7/10.4.

10.2.7 Personenbezug durch Zusatzwissen

Eine interessante Fragestellung ist mir in einem Fall begegnet, in dem sich ein Schüler - allem Anschein nach mit von einem geschäftsgewandten Elternteil formulierten Schreiben - an mich gewandt hat, der grundsätzlich Anspruch auf Leistungen nach dem SGB II und in diesem Zusammenhang die Übernahme der Kosten für die Teilnahme an einer schulischen Studienfahrt beantragt hatte, woraufhin die SGB II-Behörde Erkundigungen bei der Schule eingeholt hatte, ob die Studienfahrt denn tatsächlich als schulische Veranstaltung stattfinde.

Die SGB II-Behörde hat mir auf meine Anfrage hin mitgeteilt, dass sie bei der Schule angerufen, jedoch nicht den Namen des Schülers genannt, sondern die Erkundigungen nur ganz allgemein, eben ohne konkreten Bezug eingeholt habe. Ich habe dem Schüler mitgeteilt, dass ich diese Aussage nicht widerlegen (ich habe keine

Möglichkeit gesehen, den wahren Inhalt eines Telefongespräches zwischen zwei Personen zu ermitteln, an dem ich nicht beteiligt gewesen bin) und einen Verstoß gegen Datenschutzrecht insoweit nicht feststellen könne. Der Schüler hat demgegenüber eingewandt, dass die Schule auch ohne Nennung seines Namens durch die SGB II-Behörde habe wissen können, dass es sich um seine Person handele, da er (nach seiner Kenntnis) der einzige gewesen sei, der bei dem an der Schule bestehenden Schul-Förderverein einen Antrag auf Förderung seiner Teilnahme an der Studienfahrt gestellt habe. Die Schule habe deshalb vermuten dürfen, dass unter den Teilnehmern der Studienfahrt nur er als möglicher Empfänger von SGB II-Leistungen in Frage komme. (Ein tüchtiger Schulleiter ist erfahrungsgemäß aktiv im Vorstand des Schulfördervereins tätig, und auch unabhängig davon wird ein Schulförderverein sich in solchen Fällen mit hoher Wahrscheinlichkeit bei der Schule vergewissern, so dass diese Überlegung des Schülers sehr viel für sich hatte.)

Hier hat sich demnach die Frage gestellt, ob eine Behörde Erkundigungen zu für sich genommen nicht personenbezogenen Umständen („Findet eine bestimmte Klassenfahrt statt?“) nicht hat einholen dürfen, wenn die um Auskunft gebetene Behörde (Schule) durch ihr Zusatzwissen einen Personenbezug hat herstellen können, so dass die Frage ihrem Inhalt nach zugleich auf eine Übermittlung eines personenbezogenen Datums („Schüler X hat bei der SGB II-Behörde Leistungen beantragt“) an die Schule hinausgelaufen ist.

Im vorliegenden Fall hat die SGB II-Behörde jedoch nicht damit rechnen müssen, dass die Schule über das betreffende Zusatzwissen verfügen könnte. Aus diesem Grund war die von der SGB II-Behörde gestellte Frage im Rechtssinne nicht personenbezogen. Es hat daher dahinstehen können, ob ein lediglich auf einer naheliegenden - möglichen oder tatsächlich angestellten - *Vermutung* beruhender bzw. auf eine bloße *Vermutung* (Wahrscheinlichkeit) hinauslaufender Personenbezug schon einen Personenbezug im Sinne der maßgeblichen rechtlichen Begriffsbestimmungen (§ 67 Abs. 1 Satz 1 SGB X, § 3 Abs. 1 SächsDSG, § 3 Abs. 1 BDSG) dargestellt hat.

10.2.8 Anforderung von Betriebsunterlagen des selbständigen Ehegatten eines ALG II-Empfängers

Eine sehr umfangreiche Korrespondenz über die Erforderlichkeit einer Datenerhebung habe ich mit einer Options-Kommune geführt. Diese hatte eine ALG II-Empfängerin im Rahmen ihres zweiten Folgeantrags aufgefordert, weitere Unterlagen zur selbständigen Tätigkeit ihres Ehemannes vorzulegen. Gefordert worden waren die

Steuerbescheide der vergangenen zwei Jahre einschließlich der dazugehörigen Steuererklärungen, die Jahresabschlüsse (Einnahmen-Ausgaben-Überschussrechnung - „EÜR“), der so genannte Anlagespiegel, die aktuelle betriebswirtschaftliche Auswertung sowie Angaben zu Fördergeldern, Gewerbeanmeldung, Nachweisen zu Kranken- bzw. Rentenversicherungen.

Die Behörde hat ihr Vorgehen mir gegenüber damit begründet, dass sie die Unterlagen auf der Grundlage der §§ 11 SGB II und 15 SGB IV angefordert habe, wonach das Arbeitseinkommen nach den allgemeinen Gewinnermittlungsvorschriften einzelfallabhängig ermittelt werden müsse: Insbesondere könnten sich nicht alle steuerrechtlichen Vorschriften mindernd auf den Gewinn auswirken. Aus diesem Grund sei der Steuerbescheid für die Einkommensermittlung nicht ausreichend.

Ich habe dazu folgende datenschutzrechtliche Bewertung abgegeben:

Maßgeblich für die Frage, welche personenbezogenen Daten bzw. Nachweise die SGB II-Behörde über den Antragsteller nach dem SGB II und mit ihm in Bedarfsgemeinschaft Lebende erheben darf, ist zunächst § 51b Abs. 1 Satz 1 Nr. 1 i. V. m. Abs. 2 Nr. 3 SGB II. Danach darf der zuständige Träger die Art und Höhe des angerechneten Einkommens für einen Leistungsempfänger erheben. Eine Auskunftspflicht des Ehegatten (oder sonstigen Lebenspartners) eines Leistungsempfängers regelt § 60 Abs. 4 SGB II. Der 2. Halbsatz des 1. Satzes beschränkt diese Pflicht jedoch auf Angaben, die zur Durchführung der Aufgaben nach dem SGB II erforderlich sind. Aus dem Zusammenspiel dieser Regelungen ergibt sich, dass nur die Daten erhoben werden dürfen, die zur Erfüllung der gesetzlichen Aufgaben - im konkreten Fall zur Ermittlung des Einkommens des selbständigen Partners in der Bedarfsgemeinschaft - erforderlich sind.

Wie das Einkommen zu ermitteln ist, regelt § 11 SGB II i. V. m. der Verordnung zur Berechnung von Einkommen sowie zur Nichtberücksichtigung von Einkommen und Vermögen bei Arbeitslosengeld II/Sozialgeld (ALG II-V) vom 20. Oktober 2004 (BGBl. I S. 2622). In letzterer ist die Berechnung des Einkommens aus selbständiger Arbeit in § 2a geregelt. Absatz 1 der Vorschrift verweist auf § 15 SGB IV. Danach ist Arbeitseinkommen der nach allgemeinen Gewinnermittlungsvorschriften des Einkommenssteuerrechtes ermittelte Gewinn aus einer selbständigen Tätigkeit. Die von der SGB II-Behörde vertretene Auffassung, dass nicht alle steuerrechtlichen Vorschriften, deren Anwendung im Steuerrecht zur Gewinnminderung führen kann, auch bei der Einkommensermittlung nach dem SGB II zu berücksichtigen seien, kann aufgrund der Formulierung des § 15 SGB IV nicht richtig sein. Auch der Gesetzgeber

hat mit der Regelung des § 15 SGB IV einen vollen Gleichlauf von Einkommenssteuerrecht und Sozialversicherungsrecht erreichen wollen (BR-DS 508/93, zitiert nach Jahn, Rdnr. 2 zu § 15 SGB IV). Dies soll insbesondere in § 2 Abs. 4 ALG II-V deutlich werden, wonach bei der abschließenden Entscheidung als Einkommen der vom Finanzamt für das Berechnungsjahr festgestellte Gewinn zu berücksichtigen ist. Die einzige Besonderheit, die bei der Berechnung des Einkommens nach SGB II zu beachten ist, regelt § 2a Abs. 2 und 3 ALG II-V. Danach ist als Einkommen der Betrag anzusetzen, der auf der Grundlage von früheren Betriebsergebnissen, der im Berechnungsjahr bereits erzielten Einnahmen und geleisteten notwendigen Ausgaben sowie der erwarteten Einnahmen und notwendigen Ausgaben zu errechnen ist.

Auf dieser Grundlage ist die Anforderung des Einkommenssteuerbescheides der letzten zwei bis drei Jahre gerechtfertigt, nicht jedoch die der dazugehörigen Steuererklärungen und Jahresabschlüsse einschließlich der EÜR. Das in § 2a Abs. 3 ALG II-V erwähnte „Betriebsergebnis“ ist im Einkommenssteuerbescheid des Finanzamtes vollständig enthalten, da es das Ergebnis der EÜR vor Steuern und Zinsen abbildet.

Wozu die Vorlage eines Anlagespiegels erforderlich sein soll, war mir ebenfalls nicht ersichtlich. Über das aktuelle Einkommen gibt der Anlagespiegel keine Auskunft, er gibt allenfalls einen Überblick über die Wertentwicklungen der einzelnen Bilanzpositionen des Anlagevermögens. Soweit die Behörde das Anlagevermögen eines Unternehmens als Vermögen i. S. d. § 12 Abs. 3 SGB II berücksichtigen möchte, sei auf § 4 Abs. 1 ALG II-V verwiesen. Das Anlagevermögen eines Unternehmens wird in der Regel für die Erwerbstätigkeit unentbehrlich sein. Im Übrigen sind lediglich Kapitalgesellschaften gemäß § 268 Abs. 2 HGB verpflichtet, einen Anlagespiegel aufzustellen.

Soweit die Kommune eine aktuelle betriebswirtschaftliche Auswertung verlangt, kann dies grundsätzlich auf § 2b Abs. 3 ALG II-V gestützt werden, da diese Auskunft über die im Berechnungsjahr bereits erzielten Einnahmen und geleisteten notwendigen Ausgaben geben könnte. Allerdings kann eine betriebswirtschaftliche Auswertung nur aufgrund einer aktuellen Buchführung ermittelt werden. Da nicht alle Selbständigen der Buchführungspflicht unterliegen, ist zunächst zu ermitteln, ob eine solche Pflicht besteht. In einem zweiten Schritt ist abzuklären, ob eine aktuelle betriebswirtschaftliche Auswertung vorliegt. Ist eine solche nicht vorhanden - es besteht keine gesetzliche Pflicht zur Aufstellung einer solchen Auswertung -, so können die SGB II-Behörden dies vom Lebenspartner eines Antragstellers nur verlangen, wenn erstens eine Feststellung der im Berechnungsjahr bereits erzielten Einnahmen und notwendigen Ausgaben anderweitig - etwa durch Selbstauskunft - nicht möglich

ist und, zweitens, wenn die Behörde die Auskunftspflichtigen auf die Regelungen des § 60 Abs. 4 Satz 2 SGB II hinweist. In der Regel ist eine betriebswirtschaftliche Auswertung mit etlichem finanziellem Aufwand verbunden, da im überwiegenden Teil der Fälle nur der Steuerberater in der Lage ist, diese zu erstellen. Der Aufwand der dadurch entsteht, ist nach §§ 60 Abs. 4 Satz 2 SGB II, 21 Abs. 3 Satz 4 SGB X zu entschädigen.

Hinsichtlich der Angaben zu Fördergeldern, der Gewerbeanmeldung und den Nachweisen der Kranken- und Rentenversicherung habe ich die Erforderlichkeit der Datenerhebung für die Berechnung eines ALG II-Anspruchs gesehen.

Die Behörde hat sich meiner Auffassung nicht anschließen mögen und weiterhin auf der Vorlage der Jahresabschlüsse, neben den Steuerbescheiden, bestanden. Ziel sei es, die Kunden in den Arbeitsmarkt zu integrieren und sie in die Lage zu versetzen, ihren finanziellen Bedarf und den der übrigen Mitglieder der Bedarfsgemeinschaft selbst zu decken. So gebe die EÜR Auskunft über den Gewinn des Selbständigen, und man könne so gezielte Fortbildungsmaßnahmen anbieten.

Ich habe die Behörde darauf hingewiesen, dass die Ehefrau, nicht aber der berufstätige Ehegatte Förderung zur Integration in den Arbeitsmarkt erhält. Zum anderen musste sich die Behörde vorhalten lassen, dass sie die Geschäftsunterlagen nicht aus Gründen (irgend-)einer Förderung des Geschäftsinhabers angefordert hatte, sondern von seiner Ehefrau im Hinblick auf an diese zu gewährende Leistungen zur Sicherung des Lebensunterhaltes.

Auch an der Vorlage des Anlagespiegels hat die Behörde mit der Begründung festgehalten, nur so könne man feststellen, ob Aufwendungen zum Beispiel für den auch privat genutzten Geschäfts-Pkw bei der Berechnung der Einkommensseite des SGB II-Antragstellers zu berücksichtigen seien. Diese Begründung habe ich als zu pauschal zurückgewiesen und um Mitteilung gebeten, ob es Anhaltspunkte für eine solche Annahme im konkreten Fall gegeben hat.

Die Behörde hat sich in der Folge an das SMS gewandt, mit der Bitte um Unterstützung ihrer Position. Als ihr eine Stellungnahme des Staatsministeriums vorlag, hat sie mir diese in Auszügen bekannt gegeben. Ich konnte dem entnehmen, dass das SMS die Auffassung der Behörde teilte. Da mir jedoch nicht der gesamte Wortlaut des Staatsministeriumsschreibens vorlag, bat ich um Übersendung. Dies hat die SGB II-Behörde mit dem Hinweis abgelehnt, dass es sich lediglich um eine Anfrage zur Auslegung datenschutzrechtlicher Bestimmungen gehandelt habe, die nicht im Zusammenhang mit der Verarbeitung von Sozialdaten gemäß SGB X stünden.

Dem bin ich mit dem Hinweis entgegengetreten, dass die SGB II-Behörde als öffentliche Stelle gemäß § 28 Abs. 1 Nr. 1 SächsDSG i. V. m. § 81 Abs. 2 Satz 3 SGB X verpflichtet ist, Auskunft zu den Fragen des Sächsischen Datenschutzbeauftragten zu geben sowie Einsicht in alle Unterlagen und Akten zu gewähren, die im Zusammenhang mit der Verarbeitung personenbezogener Daten stehen. In dem konkreten Fall habe ich aufgrund einer Eingabe eine datenschutzrechtliche Kontrolle durchgeführt und die Rechtswidrigkeit der betreffenden Datenerhebung dargelegt. Die von der Behörde dazu vertretene entgegengesetzte Rechtsauffassung habe sie auch mit Übereinstimmung mit der Rechtsauffassung des SMS, als Rechtsaufsichtsbehörde, begründet. Da das SMS die Aufsicht über die SGB II-Behörden führe, sei der betreffende Schriftverkehr im Zusammenhang mit der Verarbeitung personenbezogener Daten geführt worden, mit der Folge, dass die Behörde die Datenerhebung im konkreten Fall der Petentin als rechtmäßig angesehen habe bzw. dies gar wegen der Meinung der Rechtsaufsichtsbehörde als rechtmäßig habe ansehen müssen. Soweit die Aufsichtsbehörde einer Behörde Hinweise hinsichtlich der Auslegung datenschutzrechtlicher Vorschriften erteile und sich diese Hinweise unmittelbar auf die Erhebung personenbezogener Daten auswirkten, stünden diese Hinweise im Zusammenhang mit einer - in diesem Fall sehr konkreten - Erhebung personenbezogener Daten. Aus diesem Grund sei auch das Schreiben des SMS zu übersenden.

Die Behörde hat daraufhin meiner Bitte entsprochen und das Schreiben in Ablichtung übersandt. Dem konnte ich nunmehr entnehmen, dass auch das SMS die Auffassung vertreten hat, dass, wenn bereits ein Steuerbescheid vorliege, Einkommenssteuererklärung und EÜR nicht gefordert werden dürften, da der Steuerbescheid das Arbeitseinkommen ausreichend abbilde. Anders sei dies allerdings zu bewerten, wenn noch kein gültiger Bescheid vorliege. In diesem Fall könne auf diese Unterlagen nicht verzichtet werden.

Dies entsprach auch meiner rechtlichen Bewertung, allerdings hatte ich diese so deutlich noch nicht gegenüber der Behörde zum Ausdruck gebracht, da bis zu diesem Zeitpunkt die Frage erörtert worden war, ob die Steuererklärungen und die EÜR neben dem Steuerbescheid verlangt werden dürfen.

Hinsichtlich der Vorlage des Anlagespiegels hat mich das SMS von seiner Auffassung überzeugen können. Danach müsste die Behörde prüfen können, ob das Anlagevermögen tatsächlich zum Schonvermögen (die Vermögensgegenstände sind zur Fortsetzung der Erwerbstätigkeit unentbehrlich und damit nach § 4 Abs. 1 ALG II-V nicht zu berücksichtigen) gehört. Dafür ist jedoch eine Übersicht über die Vermögensgegenstände des Gewerbetreibenden erforderlich.

In Bezug auf die Erhebung einer aktuellen betriebswirtschaftlichen Auswertung hat das SMS eingeräumt, dass hier zunächst mit der Selbstauskunft des Selbständigen gearbeitet werden könne.

Ich habe dem SMS den Vorschlag unterbreitet, dass sowohl hinsichtlich der Steuererklärung des Vorjahres (soweit der Steuerbescheid nicht vorliege) als auch in Bezug auf die aktuelle betriebswirtschaftliche Auswertung vom Hilfebedürftigen zunächst nur eine Selbstauskunft, belegt durch die Prognose eines Steuerberaters, gefordert werden sollte, und habe das Staatsministerium um aufsichtsrechtliche Maßnahmen gegenüber der Behörde zur Durchsetzung dieser Auffassung gebeten. Dies wurde mit der Begründung abgelehnt, dass der Leistungsträger im Einzelfall und unter Beachtung des Grundsatzes der Verhältnismäßigkeit nur selbst entscheiden könne.

Das habe ich als unbefriedigend zurückgewiesen, und ich habe der SGB II-Behörde folgende datenschutzgerechte, aber auch zur Aufgabenerfüllung des Amtes gerecht werdende Verfahrensweise vorgeschlagen:

Die SGB II-Behörde verlangt vom selbständig tätigen Hilfebedürftigen bei Antragstellung zunächst die Vorlage

- bereits erlassener Steuerbescheide,
- einer Selbstauskunft hinsichtlich der aktuellen Einkommens- und Vermögensverhältnisse,
- wenn erforderlich, Angaben zu Fördergeldern, Gewerbeanmeldungen und Nachweise zu Kranken- bzw. Rentenversicherung,
- Kontoauszüge von Geschäftskonten (teilweise geschwärzt),
- Auflistung der Vermögensgegenstände (Anlagespiegel).

Bestehen danach Zweifel an der Richtigkeit der Angaben, kann nach Prüfung im Einzelfall weiter die Vorlage der Prognose des Steuerberaters, ähnlich einer betriebswirtschaftlichen Auswertung, verlangt werden.

Da danach die Einkommensverhältnisse nur prognostisch feststehen, kann der Leistungsbescheid unter Vorbehalt erlassen werden. Liegen die Steuerbescheide vor, ist der vorläufige Bescheid zu überprüfen. Nach alledem ist das Verlangen nach Vorlage der Steuererklärungen einschließlich der Anlagen nicht mehr erforderlich und somit nicht zulässig.

Im Ergebnis haben dann sowohl der Landkreis als auch das SMS meinem Kompromissvorschlag folgen können.

10.2.9 Sinnlose Datenerhebung betreffend den Hauptmietvertrag bei in Wohngemeinschaften wohnenden Empfängern von Leistungen nach SGB II

(1) Die SGB II-Arbeitsgemeinschaft (ARGE) einer bedeutenden sächsischen Großstadt - insoweit übe ich (siehe oben 10.2.1) im Bereich der Leistungen für Unterkunft und Heizung unverändert die datenschutzrechtliche Kontrolle aus - hat von sämtlichen Leistungsempfängern, die als *Untermieter* in einer Wohngemeinschaft leben, zum Nachweis der Wohnungskosten nicht nur die Vorlage des Untermietvertrages verlangt, sondern auch die Vorlage des Hauptmietvertrages, also desjenigen Vertrages, den der Hauptmieter mit dem Hauptvermieter geschlossen hat. Diese Leistungsempfänger kamen dabei nicht selten in die Situation, dass der Hauptmieter die Herausgabe des Hauptmietvertrages verweigerte. Den Leistungsempfängern, die den Hauptmietvertrag nicht vorlegen konnten oder wollten, hat die Behörde die Kürzung ihrer Leistungen angedroht.

Die zur Stellungnahme aufgeforderte ARGE begründete die Anforderung des Hauptmietvertrages - den sie, wie sich herausstellte, tatsächlich bei allen Untermietverhältnissen verlangte - damit, dass der Leistungsempfänger gemäß § 22 Abs. 1 SGB II nur Anspruch auf die angemessenen Kosten für Unterkunft und Heizung habe. Nach dem diesbezüglichen Stadtratsbeschluss richteten sich die Angemessenheitskriterien nach drei Faktoren: Anzahl der im Haushalt lebenden Personen, Bruttokaltmiete und Heizkosten. Für die Feststellung der Angemessenheit einer Wohnung - so die ARGE weiter - sei daher auf die Anzahl der haushaltsangehörigen Personen abzustellen; dafür, so hat die Behörde gemeint, sei die Vorlage des Hauptmietvertrages erforderlich; inwieweit aus dem Hauptmietvertrag diese Anzahl typischerweise oder gar notwendig hervorgeht (Geeignetheit!), hat die Behörde nicht erklären können - es ist schlichtweg nicht der Fall. Außerdem, so die Behörde weiter, solle geprüft werden, ob die Untermietverhältnisse zulässig seien.

(2) Ich habe die ARGE zunächst darauf hingewiesen, dass das Verlangen nach Vorlage des Hauptmietvertrages beim Untermieter - der ja gar nicht Partei dieses Vertrages ist - den Versuch einer Datenerhebung bei einem Dritten darstellt. Gemäß § 67a Abs. 2 Nr. 2 SGB X ist für eine solche Erhebung eine Rechtsvorschrift erforderlich, die dies ausdrücklich erlaubt, bzw. eine Aufgabe nach dem SGB II, die dies erforderlich machen würde, oder aber dass die Erhebung beim Betroffenen unverhältnismäßig aufwendig wäre. Vor allem aber setzt die Datenerhebung, sei es beim Betroffenen oder beim Dritten, immer voraus, dass die betreffenden Sozialdaten

für die Aufgabenerfüllung der erhebenden Stelle erforderlich sind (§ 67a Abs. 1 Satz 1 SGB X).

(2.1) Bereits an dieser Voraussetzung scheitert jedoch die Zulässigkeit der Anforderung des Hauptmietvertrages. Denn die Überlegung, aufgrund deren die Behörde den Hauptmietvertrag kennen zu müssen gemeint hat, hält, wie schon angemerkt, einer näheren Prüfung nicht stand:

Die Stadt wollte bei der Angemessenheitsprüfung Wohngemeinschaften genauso behandeln wie Bedarfsgemeinschaften, also die nach § 7 Abs. 3 SGB II in einem Haushalt zusammenlebenden, miteinander durch enge Lebensbeziehung verbundenen Personen. Laut Stadtratsbeschluss gelten für die Angemessenheit folgende Obergrenzen: Für einen Ein-Personen-Haushalt sind Wohnkosten inklusive Heizung in Höhe von 300 € angemessen, für einen Drei-Personen-Haushalt (Bedarfsgemeinschaft), zum Beispiel, jedoch insgesamt nur 500 €, so dass auf das einzelne Mitglied der Bedarfsgemeinschaft rein rechnerisch lediglich 166,66 € entfielen, also annähernd 144 € weniger, als wenn diese Person allein lebte. Die ARGE hat daraus gefolgert, dass, um bei dem Beispiel zu bleiben, einem Leistungsempfänger, der in einer Drei-Personen-Wohngemeinschaft lebt, maximal 166 € als angemessene Wohnkosten zu zahlen seien. Deswegen wollte sie durch Prüfung des Hauptmietvertrages feststellen, wie viele Mitglieder die betreffende Wohngemeinschaft hat. Das aber geht eben aus einem Hauptmietvertrag in der Regel nicht hervor.

(2.2) Aber auch abgesehen davon war diese Überlegung aus folgendem Grund falsch: Grundsätzlich steht es dem Antragsteller nach dem SGB II frei, sich an den jeweils festgelegten Kriterien der Angemessenheit zu orientieren. So kann er sich entscheiden, ob er eine besonders große oder kleine Wohnung mietet, solange er nur die Obergrenze (in der betreffenden Stadt: 300 €) nicht überschreitet. Folgerichtig ist es ihm auch überlassen, ob er eine von ihm allein bewohnte oder aber eine Unterkunft im Rahmen einer Wohngemeinschaft wählt. Würde sich die Angemessenheit der Kosten des WG-Zimmers bzw. WG-Anteils in der von der ARGE geltend gemachten Weise durch Division aus dem Wert für eine gleich viele Köpfe umfassende Bedarfsgemeinschaft bestimmen, hätte dies zur Folge, dass ein Hilfebedürftiger, der allein in einer Wohnung lebt, maximal 300 € erhielte, derjenige, der in derselben Wohnung mit zwei anderen in einer Wohngemeinschaft lebt, jedoch maximal 166 €. Würde dies der Angemessenheitsprüfung in einer Wohngemeinschaft zugrunde gelegt, würden keine WG-Zimmer bzw. -Anteile mehr von den Hilfebedürftigen gemietet. Dies wiederum hätte in der Regel zur Folge, dass die SGB II-Behörde die

im Vergleich zum WG-Zimmer (bzw. Anteil) in der Regel höheren Kosten für eine Ein-Personen-Wohnung tragen müsste.

Dieses Ergebnis widerspricht jedoch der Regelung des § 22 SGB II, wonach die SGB II-Behörde auch die Aufwendungen für die Unterkunft tragen muss, die einen angemessenen Umfang übersteigen, solange es den Hilfebedürftigen nicht möglich ist, die Aufwendungen durch einen Wohnungswechsel zu senken. Genau dies wäre aber der Fall: Der in einer Wohngemeinschaft als Untermieter lebende Hilfebedürftige wird als Einzelstehender, der er nun einmal ist und auch weiter sein darf, gar keine preiswertere Wohngelegenheit finden können, da eine Wohngelegenheit in einer Wohngemeinschaft strukturell preisgünstiger ist als eine Einzelwohnung. (Schließlich weiß jeder, dass eine Wohngemeinschaft in aller Regel zu dem Zweck eingegangen wird, um verglichen mit einer Einzelwohnung geringere Kosten aufwenden zu müssen.)

(2.3) Abgesehen davon ist die unterschiedliche Behandlung der Wohngemeinschaft gegenüber der Bedarfsgemeinschaft bei der Bestimmung der Angemessenheit der Kosten der Unterkunft deswegen gerechtfertigt, weil die Bedarfsgemeinschaft anders als die bloße Wohngemeinschaft nicht nur durch räumliche Nähe, sondern auch durch persönliche Nähe gekennzeichnet ist.

(2.4) Aus all dem folgt, dass eine Kenntnis des Hauptmietvertrages in diesen Fällen für die Aufgabenerfüllung der SGB II-Behörde nicht erforderlich ist.

(3) Für die Aufgabenerfüllung ebenfalls nicht erforderlich ist die Vorlage des Hauptmietvertrages bei Zweifeln am wirksamen Zustandekommen der Untermietverträge. Die Prüfung zivilrechtlicher Vorschriften ist für die Berechnung der Kosten für Unterkunft und Heizung nicht erforderlich. Der SGB II-Leistungsträger hat diese Kosten unabhängig von der Rechtmäßigkeit des Mietverhältnisses zu erbringen (vgl. Landessozialgericht Niedersachsen-Bremen, Beschluss vom 22. Juni 2006, Az.: L8AS165/06 ER-juris).

(4) Angesichts des Umstandes, dass aus den von mir kontrollierten einschlägigen Akten der Behörde keine Anhaltspunkte dafür ersichtlich waren, dass die Behörde auf der Grundlage der von ihr mir gegenüber geltend gemachten - angeblichen - Minderung ihrer Pflicht zur Erstattung der Kosten der Unterkunft in diesem Sinne tätig geworden und zur Vorbereitung einer späteren tatsächlichen Beschränkung der Kostenerstattung die betreffenden Hilfeempfänger dazu aufgefordert hätte, sich eine kostengünstigere Wohngelegenheit zu suchen, hat es sich um eine Datensammlung *ohne Sinn und Verstand* gehandelt.

(5) Da mir die Behörde trotz mehrerer Versuche keine weiteren Gründe hat nennen können, deretwegen die Kenntnis des Inhaltes des Hauptmietvertrages für ihre Aufgabenerfüllung erforderlich gewesen wäre, habe ich sie aufgefordert, eine Anforderung der Hauptmietverträge, gleich ob vom Untermieter oder Hauptmieter, künftig zu unterlassen und bereits erhobene und gespeicherte Daten aus diesen Unterlagen zu sperren.

Die ARGE hat mir daraufhin mitgeteilt, sie werde künftig auf die Abforderung der Hauptmietverträge bei Untermietverhältnissen verzichten. Sie hat angekündigt, im Einzelfall die erforderlichen Einzelangaben im Gespräch erheben zu wollen und, falls dies keine Klärung bringe, aufgrund einer schriftlichen Einwilligung des Leistungsberechtigten die erforderlichen Angaben beim Vermieter oder den entsprechenden Versorgungsträgern einzuholen.

Auch diesem Vorschlag habe ich nicht zustimmen können, da die Behörde nicht hat darlegen können, in welchen „Einzelfällen“ die Datenerhebung für die Aufgabenerfüllung denn erforderlich sein solle. Zudem habe ich vorsorglich darauf hingewiesen, dass im Bereich des Sozialdatenschutzes die Zulässigkeit einer Datenerhebung nicht auf die Einwilligung des Betroffenen gestützt werden kann (§ 67a Abs. 1 Satz 1 und Satz 4 SGB X).

Die betreffende SGB II-ARGE, also die betreffende Stadtverwaltung, sträubt sich noch, ich bin aber zuversichtlich, sie vollständig zu einer datenschutzgerechten Verfahrenweise bewegen zu können.

10.2.10 Vorsorgliche Weitergabe von Mitteilungen über die Zwangsräumung gemieteten Wohnraumes durch die Sozialhilfebehörde an die SGB II-ARGE?

Das Sozialamt einer Großstadt hat sich mit der Frage an mich gewandt, ob es die ihm vom jeweiligen Gerichtsvollzieher gemachten Mitteilungen über anstehende Zwangsräumungen von Wohnraum an die SGB II-ARGE weiterleiten dürfe, damit auf diese Weise vermieden werden könne, dass die ARGE eventuell unrechtmäßig über die Zeit der Zwangsräumung hinaus Leistungen für die Kosten von Unterkunft und Heizung (siehe § 22 SGB II) gewährt, und ob es in diesem Zusammenhang zusätzlich auch Informationen über eventuell bestehende Mietschulden des ALG II-Beziehers weitergeben dürfe.

Ich habe zur Frage der Zulässigkeit einer solchen Unterrichtung der SGB II-ARGE durch die Sozialhilfebehörde betreffend Gerichtsvollzieher-Mitteilungen über die

bevorstehende Durchführung einer Zwangsräumung sowie über ein Bestehen von Mietschulden wie folgt Stellung genommen:

(1) Bei der Benachrichtigung der ARGE vom Termin einer Zwangsräumung sowie vom Bestehen von Mietschulden durch die Sozialhilfebehörde handelte es sich in datenschutzrechtlicher Hinsicht um die Übermittlung von Sozialdaten, die für ihre Rechtmäßigkeit einer entsprechenden Rechtsgrundlage bedürfte.

(2.1) Die in der vom Sozialamt vorgelegten Anfrage genannten §§ 52 SGB II, 118 SGB XII kommen als Rechtsgrundlage für derartige Übermittlungen nicht in Betracht. Denn sie setzen voraus, dass es sich auf Seiten der zu Abgleichszwecken übermittelnden (vgl. § 118 Abs. 1 Satz 2 SGB XII, § 52 Abs. 2 SGB II) Stelle bei den Betroffenen um (tatsächliche, aktuelle) *Leistungsbezieher* (Gesetzeswortlaut eindeutig; Kommentare setzen das ohne Erörterung voraus, z. B. Schellhorn BSHG 16 Rdnr. 14 zu § 117 BSHG, Eicher/Spellbrink Rdnr. 6 zu § 52 SGB II) handelt. Die von dem betreffenden Sozialamt vorgelegte Anfrage hat jedoch nicht unterstellt, dass die den Sozialhilfebehörden vom Gericht bzw. vom Gerichtsvollzieher gemeldeten zwangsgeräumten Ex-Wohnungsmieter Empfänger von Leistungen der (zu Abgleichszwecken übermittelnden) Sozialhilfebehörde sind, ja sie ist eher vom Gegenteil ausgegangen, weil sie ja Fälle des Leistungsbezuges nach dem SGB II statt nach dem SGB XII hat erfassen wollen.

(2.2) Hinzu kommt, dass bei der gebotenen wörtlichen Auslegung des Gesetzes eine nach § 44b SGB II das Gesetz ausführende „Arbeitsgemeinschaft“ nicht unter § 118 Abs. 1 Satz 1 Nr. 1, 1. Fall SGB XII („Bundesagentur für Arbeit [Auskunftsstelle]“) fällt, trotz §§ 51 Abs. 1 Satz 2, 52 Abs. 1 Nr. 5 SGB II, und dass sie damit überhaupt nicht in den Anwendungsbereich des § 118 SGB XII fällt, insbesondere auch nicht unter § 118 Abs. 4 SGB XII, weil die ARGE auch nicht eine „andere Stelle ihrer Verwaltung“ der Kommunalen Gebietskörperschaft ist, die an ihr beteiligt ist. Denn eine ARGE nach § 44b SGB II ist eine Einrichtung eigener Art, welche als eigenständiger Träger von Rechten und Pflichten zur Erfüllung ihrer Aufgaben insoweit berechtigt ist, Verwaltungsakte und Widerspruchsbescheide zu erlassen. Zum anderen führt die Geschäfte der ARGE ein Geschäftsführer, der die ARGE gerichtlich und außergerichtlich vertritt. Bei der ARGE handelt es sich danach nicht um ein Amt der jeweiligen kommunalen Gebietskörperschaft. Daran ändert auch der Umstand nichts, dass die Aufgaben der ARGE gegebenenfalls durch Personal der kommunalen Gebietskörperschaft wahrgenommen werden. Das Erfordernis des Abschlusses eines entsprechenden Dienstleistungsüberlassungsvertrages zur Ausübung ihrer Tätigkeit im (Aufgaben-)Bereich der ARGE zeigt, dass die Mitarbeiter der ARGE ja gerade

nicht in ihrer Eigenschaft als Beschäftigte der kommunalen Gebietskörperschaft tätig werden.

(2.3) Schließlich findet § 52 SGB II keine Anwendung auf die Übermittlung personenbezogener Daten durch eine Sozialhilfebehörde zu Abgleichzwecken an die das SGB II ausführenden Behörden; die Vorschrift gilt nur für die *Rück*übermittlung der die Trefferfälle betreffenden Datensätze an die das SGB II ausführende Stelle (vgl. § 52 Abs. 3 Satz 2 SGB II).

(3) Nach geltendem Recht ist daher das Sozialamt auf eine Datenübermittlung im Einzelfall aufgrund konkreter Anhaltspunkte nach den §§ 67d ff. SGB X beschränkt. Als Rechtsgrundlage kommt dabei allenfalls § 69 Abs. 1 Nr. 1, 3. Fall SGB X in Betracht, wonach die Übermittlung von Sozialdaten insoweit erlaubt ist, als sie erforderlich ist, damit der empfangende Leistungsträger (hier: die SGB II-ARGE) eine ihm im SGB (hier: SGB II) zugewiesene Aufgabe erfüllen kann. Auch wenn man davon auszugehen hat, dass zu den Aufgaben des Sozialleistungsträgers auch die Aufgabe zählt, zu überprüfen, ob die Voraussetzungen für die Leistungsgewährung - hier: Kosten für eine tatsächlich genutzte Unterkunft und Heizung nach § 22 SGB II als Teil des ALG II und des Sozialgeldes nach § 28 SGB II - (noch) vorliegen oder ob diesbezügliche Zahlungen aufgrund einer inzwischen durchgeführten Räumung nicht mehr anfallen bzw. zumindest zukünftig entfallen, ist die Datenübermittlung in dem vorgesehenen Ausmaß, nämlich offensichtlich die Weitergabe sämtlicher beim jeweiligen Sozialamt eingehender Mitteilungen über anstehende Räumungen, nicht erforderlich und damit unzulässig. Denn es ist davon auszugehen, dass es sich bei den Meldungen des Gerichtsvollziehers an das Sozialamt nicht lediglich um Fälle handelt, in denen der von der Zwangsräumung Betroffene ALG II-Bezieher ist. (Es wäre auch nicht nachvollziehbar, woher dem jeweiligen Gerichtsvollzieher dieses Datum bekannt sein sollte.) Nur insoweit kann eine Datenübermittlung seitens des Sozialamts an die ARGE zwecks Aufgabenerfüllung zulässig sein. Das Sozialamt bleibt daher auf eine Datenübermittlung im Einzelfall aufgrund konkreter Anhaltspunkte nach den §§ 67d ff. SGB X beschränkt, welche demnach ein entsprechendes Übermittlungsersuchen der ARGE voraussetzte. Dafür brauchte die SGB II-Behörde wiederum eine Übermittlungs- und Erhebungsbefugnis, die sich nur aus der Erforderlichkeit im Einzelfall, also einem Anfangsverdacht ergeben könnte.

(4) Zu prüfen ist auch, inwieweit die Sozialhilfebehörde die für die Unterbringung Obdachloser zuständige Behörde ist: Die Benachrichtigung von einer bevorstehenden Zwangsräumung ist ja von derjenigen von einer (auf mutmaßlicher Zahlungsunfähigkeit beruhenden, § 34 Abs. 2 Satz 3 SGB XII) Räumungsklage, § 34 Abs. 2 SGB XII,

zu unterscheiden. (Interessant ist übrigens die Frage der Erhebungs- und Speicherungsbefugnis der Sozialhilfebehörde im Hinblick auf § 34 SGB XII, zumindest in verfassungsrechtlicher Hinsicht, generell, denn diese Regelung unterstellt ja außerhalb des Absatzes 2 Satz 3 wohl - im Hinblick auf § 18 Abs. 1 SGB XII? - die Erforderlichkeit für die Aufgabenerfüllung gerade seitens der Sozialhilfebehörde.)

(5) Für die Übermittlung des Datums „Mietschulden“ gilt das Vorstehende entsprechend.

Einwände gegen meine Rechtsauffassung, die ich unter den Datenschutzbeauftragten zur Diskussion gestellt habe, hat es nicht gegeben.

10.2.11 Weitergabe einer Vaterschaftsanerkennungsurkunde durch das Jugendamt an einen die Vaterschaftsanerkennung bestreitenden, die Erhebung einer Vaterschaftsanfechtungsklage beabsichtigenden Dritten

Ein Jugendamt hat sich an mich gewandt, nachdem es von einem Rechtsanwalt gebeten worden war, zur Durchführung einer Vaterschaftsanfechtungsklage die Kopie einer Vaterschaftsanerkennungsurkunde herauszugeben.

Hierzu muss man Folgendes wissen:

Ist ein Kind ehelich geboren oder ist die Vaterschaft eines nichtehelichen Kindes mit Zustimmung der Mutter durch entsprechende Beurkundung der Vaterschaftsanerkennung vor einer Urkundsperson beim Jugendamt wirksam anerkannt, so wird die Vaterschaft dieses Mannes für und gegen jedermann vermutet, sie gilt somit insbesondere auch gegenüber einem Dritten, der die Vaterschaft für sich in Anspruch nehmen möchte. Die Vaterschaft kann dann grundsätzlich nur durch eine Vaterschaftsanfechtungsklage vor dem Familiengericht angefochten werden, dabei gilt eine Anfechtungsfrist von zwei Jahren.

Berechtigt, eine solche Klage zu erheben, ist - eben wegen der genannten Sperrwirkung einer solchen Vaterschaftsanerkennung - selbstverständlich derjenige, der sich für den „wirklichen“ Erzeuger des Kindes hält. Dabei muss er jedoch seine Klage nicht nur gegen das Kind richten, sondern zusätzlich auch gegen denjenigen, der die Vermutung der Vaterschaft für sich in Anspruch nehmen kann. Dies bedeutet: Er muss in seinem Klageantrag zumindest Namen und Anschrift des seiner Meinung nach „falschen“ Vaters gegenüber dem Gericht angeben, andernfalls ist die Klage bereits als unzulässig abzuweisen. Diese Personalien waren in unserem Fall dem

Kläger aber eben gerade nicht bekannt. Um diese herauszubekommen, hat sein Rechtsanwalt das Jugendamt, welches nach seiner Kenntnis seinerzeit die Vaterschaftsanerkennung hinsichtlich des Kindes beurkundet hatte, um Übersendung einer Ablichtung der Vaterschaftsurkunde gebeten, hilfsweise zumindest um Namen und Anschrift der Person, die ausweislich der Urkunde die Vaterschaft anerkannt hatte.

Auch wenn das Interesse des Klägers nachvollziehbar war, habe ich dem Jugendamt dennoch mitteilen müssen, dass es für die Herausgabe der Personalien, bei denen es sich um Sozialdaten im Sinne des § 67 Abs. 1 SGB X handelt, an der erforderlichen Datenübermittlungsbefugnis für das Jugendamt fehlt (die Übermittlung einer Kopie der gesamten Vaterschaftsanerkennungsurkunde schied aus Gründen der Verhältnismäßigkeit von vornherein aus). Insbesondere handelt es sich in einem solchen Fall nicht um eine Datenübermittlung *zur Erfüllung gesetzlicher Aufgaben* des Jugendamtes (§ 69 Abs. 1 Nr. 1 SGB X). Denn das Jugendamt ist lediglich berechtigt, die Daten an die in § 1597 Abs. 2 BGB genannten Personen zu übermitteln, das heißt an den Vater, die Mutter, das Kind sowie an den zuständigen Standesbeamten. Und auch die Vorschrift des § 69 Abs. 1 Nr. 1, 1. Fall. SGB X, wonach Sozialdaten zu dem Zweck übermittelt werden dürfen, zu dem sie erhoben worden sind, schied meiner Auffassung nach als Befugnisnorm aus, die danach geforderte so genannte *Zweckidentität* war vorliegend nicht erkennbar. Denn die Datenerhebung des Jugendamts erfolgt in solchen Fällen nur zu dem Zweck der dem Jugendamt als Aufgabe und Befugnis übertragenden Beurkundung der in § 59 Abs. 1 SGB VIII abschließend aufgezählten Erklärungen (hier einschlägig § 59 Abs. 1 Nr. 1 SGB VIII). Die vorliegend gewünschte Übermittlung der genannten Daten hätte demgegenüber dem Zweck der Ermöglichung einer (zulässigen) zivilgerichtlichen Klage zur Klärung der Abstammung des betroffenen Kindes und damit der Überprüfung der Richtigkeit der Vaterschaftsanerkennung, gedient, welche vom Jugendamt bei der öffentlichen Beurkundung aber gerade *nicht* zu prüfen ist.

Ich habe dem Jugendamt jedoch insoweit weiterhelfen können, als ich es zur Frage der Weitergabe von Daten aus Personenstandsurkunden durch ein Standesamt im Falle einer (wie hier vorliegenden) Glaubhaftmachung eines rechtlichen Interesses auf meine Ausführungen in 6/5.4 hingewiesen habe.

10.2.12 Zählung in einer Beratungsstelle der Jugendhilfe

Ein Landratsamt beabsichtigte eine Zählung der Klienten in drei Beratungsstellen für Kinder, Jugendliche und Familien im Landkreis. Diese Aufgaben nach dem SGB VIII erfüllenden Beratungsstellen befinden sich in freier Trägerschaft, erhalten aber per

Bescheid des Jugendamtes Zuwendungen des Landkreises, einschließlich der Weiterleitung von Fördermitteln des Landes. Es war vorgesehen, dass Bedienstete des Landkreises im Wartebereich der Beratungsstelle die Besucher zählen sollten. Zur Frage, ob eine solche Zählung im Hinblick auf die Besucher datenschutzrechtlich zulässig wäre, habe ich wie folgt Stellung genommen:

(1) Zuständig wäre das Jugendamt des Landkreises (§ 1 SächsLaJuHiG, § 85 Abs. 1 SGB VIII); die Zählung dürfte nur durch Bedienstete des *Jugendamtes* des Landkreises erfolgen, nicht etwa durch Bedienstete des Landratsamtes, die anderen funktionalen Stellen angehören. Das Jugendamt wäre in seiner Eigenschaft als Leistungsträger im Sinne der §§ 12, 27 SGB I tätig und daher gemäß §§ 35 Abs. 1 Satz 1, Abs. 2, 37 SGB I an die Datenverarbeitungsvorschriften des SGB gebunden.

Bei der beabsichtigten Erhebung der Besucherzahlen und der Besuchsdauer in der Beratungsstelle eines Trägers der freien Jugendhilfe handelte es sich um die Erhebung von Sozialdaten im Sinne des § 67 Abs. 1 Satz 1 SGB X, also insbesondere um Angaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person. Zwar würden durch die Zählung, so wie sie beabsichtigt war, zunächst nicht Daten bestimmter Personen erhoben, jedoch würde die Bestimmbarkeit einzelner Personen herbeigeführt werden können. So könnte bei Heranziehung der in der Beratungsstelle geführten Beratungsakten ermittelt werden, zu welcher Zeit, wie lange und zu welchem Zweck sich bestimmte Personen in der Beratungsstelle aufgehalten haben. Die Angaben zu Grund und Dauer eines Aufenthaltes einer Person an einem bestimmten Ort sind personenbezogene Daten. Allerdings stammten diese Feststellungen genau genommen dann doch ausschließlich aus den Akten, durch die Besucher-Zählung und Besuchsdauer-Feststellung kämen keine zusätzlichen Angaben hinzu.

Jedoch ergäbe sich in anderer Hinsicht eine Erhebung personenbezogener Daten: Es wäre nicht ausgeschlossen, dass die zählenden Jugendamtsbediensteten einzelne Besucher der Beratungsstelle aus ihrer anderweitigen Tätigkeit kennen und feststellen, dass gerade sie zu dieser Zeit diese Beratungsstelle aufgesucht haben. Kurz: Man könnte einen Personenbezug der Feststellungen nicht vollständig ausschließen, obwohl er nicht beabsichtigt wäre.

(2) Als wegen dieses Personenbezuges nötige Rechtsgrundlage nicht in Betracht käme der an die Beratungsstelle gerichtete *Zuwendungsbescheid* des Landkreises. Da die Erhebung personenbezogener Daten durch Sozialleistungsträger nur aufgrund von Vorschriften des SGB erfolgen darf (vgl. §§ 35 Abs. 2, 37 SGB I), reicht der bloße

Zuwendungsverwaltungsakt nicht aus. Dies gilt gleichermaßen für Nebenbestimmungen dieses Verwaltungsaktes, der nur das Verhältnis zwischen dem Träger der öffentlichen Jugendhilfe (Landkreis) und dem ‚Freien Träger' regelt.

(3) Als Rechtsgrundlage für die Erhebung der Daten durch den Landkreis käme § 62 Abs. 1 i. V. m. Abs. 3 Nr. 2, Buchst. a SGB VIII in Betracht. Danach dürfen Sozialdaten erhoben werden, soweit ihre Kenntnis zur Erfüllung der jeweiligen Aufgabe erforderlich ist, und setzt zusätzlich eine Erhebung, die *ohne Mitwirkung des Betroffenen* stattfindet, voraus, dass die jeweilige Aufgabe ihrer Art nach eine Erhebung „bei anderen" erfordert und die Kenntnis der Daten erforderlich ist für die Feststellung der Voraussetzungen oder für die Erbringung einer Leistung nach dem SGB VIII.

Als Rechtsgrundlage kommt daneben auch § 67a Abs. 1 i. V. m. Abs. 2 Satz 2 Nr. 2, Buchst. b, Doppelbuchst. aa SGB X in Betracht, auf den § 61 Abs. 1 SGB VIII verweist.

(3.1) Als *Aufgabe* des Jugendamtes des Landkreises nach dem SGB VIII kommt dabei zum einen die Planung des Angebotes von Beratungsstellen im Landkreis in Betracht, zum anderen auch die Prüfung der Verwendung von Zuwendungen. (Zur Erhebung personenbezogener Daten zum Zweck der Prüfung der Wirtschaftlichkeit und Qualität der durch den Träger der freien Jugendhilfe erbrachten Leistungen vgl. 11/10.2.5.)

(3.1.1) Die Aufgabe der Planung, insbesondere der Ermittlung des Bedarfes an Einrichtungen und Diensten im Sinne des SGB VIII, ergibt sich aus § 80 Abs. 1 Nr. 2 SGB VIII und § 20 Abs. 1 SächsLaJuHiG.

Die Zählung von Klienten der Beratungsstelle und die Ermittlung der Dauer der jeweiligen Beratungsgespräche sind für die Erfüllung dieser Aufgaben erforderlich. Sie werden für eine bedarfsgerechte Bereitstellung der Einrichtungen und Dienste nach dem SGB VIII (§ 79 Abs. 2 Satz 1) benötigt. Nur mit einem Überblick über den Beratungsbedarf können die örtlichen Träger der Jugendhilfe dieser Aufgabe nachkommen.

(3.1.2) Das Recht zur Prüfung der Verwendung von Zuwendungen kann man meines Erachtens als Aufgabe der örtlichen Träger der öffentlichen Jugendhilfe § 17 Abs. 3 Satz 3 SGB I und § 74 Abs. 1 SGB VIII entnehmen. Danach sollen die Träger der öffentlichen Jugendhilfe die freiwillige Tätigkeit auf dem Gebiet der Jugendhilfe fördern, wenn der jeweilige Träger, unter anderem, gemäß § 74 Abs. 1 Nr. 2

SGB VIII die Gewähr für eine zweckentsprechende und wirtschaftliche Verwendung von Mitteln bietet. Wendet die öffentliche Jugendhilfe dem Träger der freien Jugendhilfe solche Fördermittel zu, dann umfasst das nicht nur nach § 74 Abs. 1 SGB VIII die Prüfung der Voraussetzungen der Zuwendung, sondern nach § 17 Abs. 3 Satz 3 SGB I auch die Prüfung der Verwendung.

Dazu gehört meiner Auffassung nach auch der Auslastungsgrad einer Einrichtung eines freien Trägers hinsichtlich geförderter Leistungen.

(3.1.3) Mithin handelte der Landkreis bei der geplanten Datenerhebung als örtlicher Träger der öffentlichen Jugendhilfe in Erfüllung der beiden genannten Aufgaben.

(3.2) Die Daten dürften auch in der geplanten Art *ohne Mitwirkung der Betroffenen*, durch dessen bloße Beobachtung, erhoben werden.

(3.2.1) Die Erhebung erforderte im Sinne des § 62 Abs. 3 Nr. 2, 2. Fall SGB VIII eine Erhebung gerade *ohne Mitwirkung des Betroffenen*: Bloße Beobachtung, statt der nachträglichen Befragungen nach Anfangs- und Endzeit des Besuches, wäre erforderlich, weil der Besucher sich die (Anfangs-)Zeit nicht ohne Weiteres mit der nötigen Genauigkeit merkt, so dass die nötigen Daten mit der für die Erreichung des Erhebungszwecks erforderlichen Genauigkeit nicht bei ihm erhoben werden könnten.

Zugleich könnte das Jugendamt die Erhebung der Daten zum Auslastungsgrad der Beratungsstelle nicht dadurch mit der erforderlichen Zuverlässigkeit ersetzen, dass es sich mit - statistischen - Angaben der Beratungsstelle begnügte: Weil es zugleich darum geht, inwieweit Zuwendungen an den freien Träger der Beratungsstelle sinnvolle Mittelverwendung sind, dürfte sich der Träger der öffentlichen Jugendhilfe nicht vollständig auf die Angaben des freien Trägers verlassen, sondern müsste erforderliche Daten selbst erheben. (Der Landkreis verstand die Zählung sogar als Prüfung der bestimmungsgemäßen Verwendung der Zuwendung an den Träger der Beratungsstelle.)

Das zusätzliche Erfordernis des § 62 Abs. 3 Nr. 2, 2. Fall i. V. m. Buchst. a SGB VIII, dass die Kenntnis der Daten für die *Erfüllung einer Leistung nach dem SGB VIII erforderlich ist*, wäre ebenfalls erfüllt. Gemäß §§ 2 Abs. 2 Nr. 1 und 2, 11 Abs. 3 Nr. 6 und 16 Abs. 2 Satz 2 SGB VIII ist der Träger der Jugendhilfe verpflichtet, Jugendberatung, Erziehungsberatung und Beratung in allgemeinen Fragen der Erziehung als Leistung anzubieten. Da der Landkreis dies durch Übertragung auf einen freien Träger gewährleisten möchte, sind die gewünschten Daten für die nötige

Kenntnis des Bedarfes (Auslastung) für die weitere Planung des Beratungsangebotes erforderlich.

(3.2.2) Daneben wäre aus denselben Gründen meines Erachtens auch die Voraussetzung des § 67a Abs. 2 Satz 2 Nr. 2, Buchst. b, Doppelbuchst. aa SGB X erfüllt. Wiederum in dem Sinne, dass nicht eine Erhebung *bei anderen*, sondern ohne Mitwirkung des Betroffenen (worauf es ja unter Datenschutzgesichtspunkten ankommt!) erforderlich wäre. Überwiegende schutzwürdige Belange des Betroffenen sind nicht erkennbar, zumal die Daten für eine rasche Aggregierung, ohne Absicht auf Herstellung eines manifesten Personenbezuges, bestimmt sind.

(4) Seitens des freien Trägers läge keine *Übermittlung* personenbezogener Daten vor, sondern er ermöglichte nur dem Jugendamt des Landkreises eine Erhebung personenbezogener Daten in seinen Räumen. Eine Anwendung der sozialdatenschutzrechtlichen Übermittlungsvorschriften über § 61 Abs. 4 SGB VIII auf das Handeln des freien Trägers käme mithin nicht in Frage. Abgesehen davon wären die Voraussetzungen, die § 75 Abs. 1 Nr. 2 SGB X für die Übermittlung von Sozialdaten zu Planungszwecken vorsieht, erfüllt: Die Einholung einer Einwilligung nach § 75 Abs. 1 Satz 2 SGB X wäre dem Betroffenen unzumutbar, da sie zu einem Mehr an Verarbeitung auf seine Person bezogene Daten führte.

Zusammenfassend war festzustellen, dass ich aus datenschutzrechtlicher Sicht keine Bedenken gegen eine in der erläuterten Weise durchzuführende Zählung der Klienten in den Beratungsstellen hatte, soweit es sich bei den Personen, die die Zählung durchführen würden, um Bedienstete des Jugendamtes handelt und die Zählung nur zu den hier geprüften Zwecken durchgeführt würde. An diese Voraussetzungen hat sich das Landratsamt dann gehalten.

10.2.13 Anspruch eines Leistungsverpflichteten auf Auskunft über sein ihm gegenüber unterhaltsberechtigtes Kind betreffende Daten

Nicht selten kommt es vor, dass sich eine Behörde auf Gründe des Datenschutzes beruft, um eine Auskunft verweigern zu können. Zu der Kontrolle eines rechtmäßigen Umgangs mit personenbezogenen Daten gehört daher auch die Prüfung solcher Sachverhalte.

Ein unterhaltspflichtiger Vater war von einem überörtlichen Sozialleistungsträger zur Zahlung eines Unterhaltsbeitrages herangezogen worden. Seine Tochter sollte Leistungen von einem Trägerverein im Rahmen des ambulant betreuten Wohnens erhalten. Der Trägerverein hatte nach Aussage des überörtlichen Sozialleistungsträgers

die Leistungen erbracht und abgerechnet. Auf der Grundlage des übergangenen Unterhaltsanspruches forderte der überörtliche Sozialleistungsträger gemäß § 94 Abs. 1 SGB XII vom Vater nunmehr Beiträge zum Unterhalt. Der zur Zahlung herangezogene Vater hatte jedoch Zweifel, ob die Leistungen von dem Verein tatsächlich erbracht worden waren, und forderte den Sozialleistungsträger auf, ihm die Leistungsnachweise des Vereins zur Verfügung zu stellen. Dies wurde ihm unter Berufung auf Datenschutzgründe verweigert. Der Betreuungsverein - an den sich der Vater auch gewandt hatte - verwies hinsichtlich der Auskunftserteilung auf den überörtlichen Sozialleistungsträger, so dass der Vater letztlich keine Auskunft erhielt.

Ich habe dem überörtlichen Sozialleistungsträger mitgeteilt, dass gemäß § 25 Abs. 1 SGB X dem Beteiligten Einsicht in die das Verwaltungsverfahren betreffenden Akten zu gestatten ist, soweit deren Kenntnis zur Geltendmachung oder Verteidigung seiner rechtlichen Interessen erforderlich ist. Mit der Aufforderung an den Unterhaltspflichtigen, einen Unterhaltsbeitrag zu leisten, sei dieser als Beteiligter des Verfahrens Adressat eines Verwaltungsaktes geworden und könne sich damit grundsätzlich auf § 25 Abs. 1 SGB X berufen. Er habe auch ein rechtliches Interesse an der Akteneinsicht, da er als Unterhaltsverpflichteter nicht zur Zahlung von Leistungen herangezogen werden dürfe, die nicht erbracht worden sind. Dies ergibt sich offenkundig aus § 94 Abs. 1 SGB XII, wonach Ansprüche nur dann übergehen, wenn der leistungsberechtigten Person „Leistungen erbracht“ worden sind, und eben nur in Höhe der geleisteten Aufwendungen.

Das Recht auf Akteneinsicht, das ja zugleich auch einen datenschutzrechtlichen Gehalt hat, bestünde gemäß § 25 Abs. 3 SGB X ausnahmsweise nur dann nicht, wenn die Vorgänge wegen der berechtigten Interessen betroffener Personen geheim gehalten werden müssten. Ein solches berechtigtes Geheimhaltungsinteresse, das dem Recht auf Akteneinsicht entgegenstünde, sei aber zumindest datenschutzrechtlich nicht begründet, weder auf Seiten der Tochter des Petenten noch gar auf Seiten des Trägervereins.

Ich habe den überörtlichen Sozialleistungsträger deshalb aufgefordert, dem Petenten die entsprechenden Auskünfte zu erteilen und zukünftig bei Ansprüchen auf Akteneinsicht gemäß § 25 Abs. 1 SGB X in gleicher Weise zu verfahren. Der überörtliche Sozialleistungsträger hat mir daraufhin mitgeteilt, dass er von der Inanspruchnahme des unterhaltspflichtigen Vaters nunmehr absehe! Dies - genauer gesagt die Rücknahme oder der Widerruf des betreffenden Leistungsbescheides - hatte zur Folge, dass der Anspruch auf Akteneinsicht gemäß § 25 Abs. 1 SGB X nunmehr weggefallen war, da der Petent nicht mehr Beteiligter eines von dem betreffenden Sozial-

leistungsträger durchgeführten Verwaltungsverfahrens war. Dem Petenten stand deshalb nunmehr lediglich noch der (datenschutzrechtliche) Auskunftsanspruch gemäß § 83 SGB X zu, der jedoch auf die Auskunft zu seinen personenbezogenen Daten beschränkt ist; ob nach Wegfall des ihn betreffenden Kostenerstattungsheranziehungsverfahrens die unmittelbar nur seine Tochter betreffenden Daten aus einem anderen rechtlichen Grunde, d. h. wegen einer anderen durch eine Rechtsbeziehung begründeten rechtlichen Betroffenheit, mittelbar auch ihn betrafen (latenter Mehrfachbezug, vgl. 11/5.8.2), hat nicht geprüft zu werden brauchen; dem Petenten ist es nur um die konkrete Heranziehung zu Geldzahlungen gegangen.

Die Beachtung meiner Hinweise in zukünftigen Fällen hat der überörtliche Sozialleistungsträger mir zugesichert.

10.2.14 Datenübermittlung eines Jugendamtes an Polizei oder Staatsanwaltschaft zur Person eines Hinweisgebers

Die behördliche Datenschutzbeauftragte eines sächsischen Landkreises sah sich gezwungen, mich um Unterstützung in einer Auseinandersetzung mit ihrem Rechtsamt und der Staatsanwaltschaft zu bitten, in der es um folgenden Sachverhalt ging:

Eine Sozialarbeiterin des Jugendamtes war telefonisch informiert worden, dass eine Einwohnerin des Landkreises ihre Kinder vernachlässige. Die Sozialarbeiterin leitete daraufhin eine Prüfung zum Wohle der Kinder in dieser Familie ein. Sie hatte keinerlei Anhaltspunkte dafür, dass der Informant wider besseres Wissen oder auch nur leichtfertig falsche Behauptungen aufgestellt hatte. Die Mutter der Kinder erstattete in der Folge Anzeige wegen *Verleumdung* gegen Unbekannt. Das Ermittlungsverfahren wurde von der Staatanwaltschaft Chemnitz geführt, die die Sozialarbeiterin als Zeugin anhören wollte. Die dafür erforderliche Aussagegenehmigung erteilte das Landratsamt nicht und verwies auf den Sozialdatenschutz, allerdings unter Nennung einer falschen Rechtsvorschrift. Die Staatsanwaltschaft intervenierte dagegen, und das Rechtsamt erteilte daraufhin die Aussagegenehmigung für die Sozialarbeiterin doch. Die Datenschutzbeauftragte ist über diesen Fall erst später informiert worden und meinte, die Aussagegenehmigung hätte nicht erteilt werden dürfen. Im Einzelnen ging es letztlich um die Klärung folgender Fragen, bei der ich helfen konnte:

(1) *Handelt es sich bei Daten, die Informanten dem Jugendamt bezüglich eines konkreten Kindes bekannt geben, um Sozialdaten*?

Bei den Angaben zur Person eines Informanten, der einem Jugendamt Mitteilungen über eine angebliche oder tatsächliche Vernachlässigung von Kindern in einer Familie macht, handelt es sich um Daten, für die das sog. „Sozialgeheimnis“, d. h. die besonderen Datenschutzregelungen des Sozialgesetzbuches gelten, nämlich um „Sozialdaten“.

Der Begriff des Sozialdatums wird in den §§ 35 Abs. 1 SGB I, 67 Abs. 1 SGB X bestimmt, auf die auch das Jugendhilferecht in § 61 Abs. 1 SGB VIII verweist. Danach ist ein Sozialdatum jede Einzelangabe über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person, die von einem Sozialleistungsträger im Hinblick auf seine Aufgaben nach dem SGB erhoben, verarbeitet oder genutzt werden. Von den Datenschutzvorschriften des SGB erfasst werden danach nur solche Informationen (Daten), die der Sozialleistungsträger mit dem nötigen „fachlichen Bezug“ (Hauck/Haines, § 67 SGB X Rdnr. 23), verarbeitet (sc. in einem weiterem Sinne) hat. Die Verarbeitung der Daten darf also „nicht nur im Zusammenhang“ mit seiner Aufgabenwahrnehmung stattfinden, sondern sie muss der Erfüllung von Aufgaben dienen, die sich unmittelbar aus dem SGB ergeben (Kasseler Kommentar, § 67 SGB X Rdnr. 24; vgl. 12/10.2.10, S. 238 oben).

Zu den gesetzlichen Aufgaben des Trägers der öffentlichen Jugendhilfe zählt nach § 1 Abs. 3 Nr. 3 SGB VIII der Schutz vor Gefahren für das Wohl der Kinder und Jugendlichen. Bei Verdacht von Kindesmisshandlung oder -vernachlässigung muss die Behörde prüfen, ob sie namentlich die in §§ 42, 43 SGB VIII geregelten repressiven Maßnahmen zu ergreifen hat.

Die Informationen, die das Jugendamt zur Person des Informanten erhalten hat, sind Teil der Sachverhaltsfeststellungen, die das Jugendamt zum Zweck der Erfüllung dieser Aufgabe durchzuführen gehabt hat. Angaben zur Person einer Informationsquelle (eines Informanten) sind meist nötig zur Beurteilung der Information bzw. zur etwaigen Fortführung der Ermittlung des Sachverhaltes. Unter Umständen ist das Jugendamt auf weitere Mitteilungen des Informanten angewiesen.

Zumindest sind diese Angaben zur Person des Informanten zu diesem Zweck erhoben, gespeichert und gegebenenfalls auch genutzt worden. Der in einem solchen Zusammenhang gespeicherte Name des Informanten fällt somit unter den Sozialdatenschutz (vgl. BVerwG Urt. vom 4. September 2003, 5 C 48/02, BVerwGE 119, 11 ff. = DÖV 2004, 532, unter 1.2 der Gründe), aber natürlich insbesondere auch die von dem Informanten gemachten Angaben zum Sachverhalt. Denn auch diese sind im

Hinblick auf die Aufgaben des Trägers der öffentlichen Jugendhilfe erhoben und (weiter-)verarbeitet worden.

(2) *Kann gegenüber der Polizei und der Staatanwaltschaft die Aussage zu Sachverhalten im Sozialdatenbereich generell abgelehnt werden, wenn keine richterliche Anordnung vorliegt*?

Ein generelles „Aussageverweigerungsrecht“ für Bedienstete von Sozialleistungsträgern betreffend Sozialdaten gegenüber Polizei und Staatsanwaltschaft als Strafverfolgungsbehörden besteht nicht.

Stattdessen hat das Gesetz in § 35 Abs. 3 SGB I die Auskunfts- und Zeugnispflichten, die nach anderen Vorschriften, insbesondere Strafprozessordnung und Zivilprozessordnung, bestehen, insoweit beschränkt, als eine Übermittlung von Sozialdaten (nach Sozialgesetzbuch) nicht zulässig wäre.

Zulässig ist eine Übermittlung von Sozialdaten, wenn sie auf eine der in § 61 Abs. 1 Satz 1 und 2 SGB VIII i. V. m. §§ 67d ff. SGB X genannten gesetzlichen Übermittlungsbefugnisse gestützt werden kann und keine der sich aus § 76 SGB X oder §§ 64 Abs. 2, 65 SGB VIII ergebenden Schranken eingreift.

Ob eine gesetzliche Übermittlungsbefugnis besteht, ist im Einzelfall festzustellen. Zum Verhältnis des Sozialdatenschutzes zu den Vorschriften der Strafprozessordnung gilt im Übrigen: Die Verschwiegenheitspflicht nach § 54 StPO für Angehörige des öffentlichen Dienstes schützt lediglich öffentliche Geheimhaltungsinteressen. Nur auf diese kann sich die Aussagegenehmigung des Dienstvorgesetzten beziehen. Nicht von der Aussagegenehmigung umfasst werden können amtlich bekannt gewordene Privatgeheimnisse, etwa das Sozialgeheimnis. Dieses verbietet die Auskunft durch Behörden nach § 67d Abs. 1 SGB X nur dann nicht, wenn eine gesetzliche Offenbarungsbefugnis nach §§ 68 bis 77 SGB X besteht, wie bereits oben dargelegt. Liegen diese Vorraussetzungen nicht vor, besteht ein sich aus § 35 Abs. 3 SGB I ergebendes, namentlich auch im Strafverfahren geltendes Zeugnisverweigerungsrecht und Beschlagnahmeverbot (Meyer-Goßner, StPO-Kommentar, Rdnr. 6 zu § 161) zugunsten der Sozialbehörde. (Etwas anderes gilt freilich, wenn das Jugendamt als Jugendgerichtshilfe tätig wird, § 61 Abs. 3 SGB VIII i. V. m. § 38 JGG.)

(3) *Kommt als Übermittlungsbefugnis für Angaben zur Person eines Hinweisgebers § 68 Abs. 1 SGB X in Frage*?

Diese Vorschrift erlaubt lediglich die Übermittlung der dort aufgezählten, den Betroffenen unmittelbar identifizierenden Daten, einschließlich Geburtsdatum und -ort, sowie Anschrift, Aufenthalt und Arbeitgeber. Hinzu kommt das Datum, dass die Behörde mit dem Betreffenden in Erfüllung ihrer Aufgaben zu tun hat - weil sie ja sonst dessen Daten gar nicht haben dürfte und damit in aller Regel auch nicht hätte; typischerweise handelt es sich um Leistungsbezug oder zumindest Stellung eines Antrages auf Leistung.

Damit passt die Vorschrift meiner Auffassung nach ihrem typischen Anwendungsbereich und damit ihrem typischen Zweck nach nicht für eine Person, über die die anfragende Stelle lediglich weiß, dass sie die Eigenschaft hat, eine bestimmte nicht auf Leistungsbezug gerichtete Handlung H ausgeführt zu haben, an der die Behörde beteiligt war oder die der Behörde zumindest bekannt ist. Denn die Behörde übermittelte dann, wenn sie die Personalien zu dieser Person P weitergäbe, die Angabe, dass die Person P die betreffende Eigenschaft, die Handlung H ausgeführt zu haben, hat. Damit ginge die Übermittlung über den in § 68 Abs. 1 Satz 1 SGB X genannten Datensatz hinaus - was unzulässig wäre.

Diese strikte Auslegung des § 68 Abs. 1 Satz 1 SGB X ist zumindest im Falle des Hinweisgebers geboten. Der Grund ist folgender: Im Regelfall weiß der Auskunftsersuchende, der Betroffener eines für ihn unangenehmen Behördenhandelns gewesen ist, dass die Behörde vermutlich auf Hinweis eines Dritten tätig geworden ist (anschauliches Fallbeispiel der Sachverhalt der oben genannten Entscheidung des Bundesverwaltungsgerichts). Wenn der Hinweis nicht offenkundig richtig gewesen ist, kann es dem Hinweisbetroffenen gelingen, ein strafrechtliches Ermittlungsverfahren gegen den Hinweisgeber in Gang zu setzen. Wenn die Strafverfolgungsbehörde dann die Personalien des Hinweisgebers von der Sozialbehörde übermittelt bekommen dürfte, könnte der Anzeigenerstatter (Strafantragsteller) durch Einsicht in die Ermittlungsakte oder zumindest (vgl. § 406e Abs. 2 Satz 1 StPO) spätestens in der Hauptverhandlung oder auch in einer Einstellungsverfügung die Person des Hinweisgebers in Erfahrung bringen. Damit wäre der redliche, d. h. nicht böswillige oder leichtfertige Hinweisgeber entgegen § 83 SGB X (in der ständigen höchstrichterlichen Auslegung aller gleichartigen Vorschriften über den datenschutzrechtlichen Auskunftsanspruch wie auch über den verwaltungsverfahrensrechtlichen Akteneinsichtsanspruch; vgl. Hauck/Noftz, Rdnr. 18 zu § 83 SGB X, in den Folgerungen nicht ganz überzeugend) nicht geschützt.

Es ist auch nicht erkennbar, dass § 68 SGB X, wenn man ihn *weiter* auslegte, geeignet wäre, gerade solche Fälle zu erfassen und einer von § 83 SGB X abwei-

chenden Behandlung (Offenlegung des Hinweisgebers) zuzuführen, für die das angebracht wäre. § 83 SGB X erlaubt schon für sich eine hinreichend alle Abwägungsgesichtspunkte berücksichtigende Grenzziehung zwischen schutzwürdigen und nicht schutzwürdigen Hinweisgebern.

Ergebnis: § 68 Abs. 1 Satz 1 SGB X ist in den Fällen, in denen die anfragende Strafverfolgungsbehörde lediglich weiß bzw. vermuten darf, dass eine Person der Behörde einen Hinweis auf einen den Anzeigeerstatter bzw. Strafantragsteller betreffenden Sachverhalt gegeben hat, so auszulegen, dass die Behörde nicht befugt ist, Angaben über diese Person zu übermitteln. Diese Auslegung erfasst auch den Fall des unredlichen Hinweisgebers. Aber das ist unschädlich, weil in diesen Fällen der datenschutzrechtliche Auskunftsanspruch des Hinweisbetroffenen selbst besteht, der seine Erkenntnisse dann für die Strafverfolgung zur Verfügung stellen kann.

Auch wenn man dieser engen Auslegung des § 68 Abs. 1 Satz 1 SGB X nicht folgt, kommt man zu einem ähnlichen Ergebnis, nämlich dazu, dass die Übermittlungsbefugnis des § 68 Abs. 1 Satz 1 SGB X im Falle eines Verlangens nach Auskunft über einen Hinweisgeber inhaltlich genauso weit reicht wie die nach § 83 SGB X bestehende Auskunftsverpflichtung gegenüber dem Hinweisbetroffenen:

§ 68 Abs. 1 Satz 1 SGB X enthält nämlich am Ende einen *Vorbehalt zur Wahrung schutzwürdiger Interessen des Betroffenen* (also hier des Hinweisgebers), der so auszulegen ist, dass in den Fällen eines redlichen Hinweises die Übermittlung zu unterbleiben hat - aus denselben Gründen wie nach § 83 Abs. 4 Nr. 3 SGB X, also *wegen der überwiegenden berechtigten Interessen des* - eben redlichen - *Hinweisgebers*.

Dieser Schutz des redlichen Hinweisgebers im Anwendungsbereich des § 68 Abs. 1 Satz 1 SGB X weist auch nicht etwa dann eine Lücke auf, wenn er in der Rechtsprechung im Einzelfall nur auf § 83 Abs. 4 Nr. 1 SGB X gestützt werden sollte, also auf das öffentliche Interesse an der Aufgabenerfüllung der Behörde, die den Hinweis erhalten hat. Denn dann hätte die ersuchte Behörde zwar nach § 68 Abs. 1 Satz 1 SGB X eine Übermittlungsbefugnis, sie wäre aber nicht zur Übermittlung verpflichtet, weil § 4 Abs. 3 Nr. 3 SGB X sie insoweit von der Pflicht zur Amtshilfe freistellte.

Das Ermessen wäre von der Behörde in der Weise zu gebrauchen, die durch die Pflicht zur Vermeidung einer Gefährdung der Erfüllung ihrer eigenen Aufgaben geboten wäre, also durch Unterlassen der Auskunft, insbesondere auch gegenüber Strafverfolgungsbehörden.

Die maßgebliche Wertung kann nicht anders ausfallen: Im Interesse der Gefahrenabwehr (SGB-Beispiel: Kindesvernachlässigung oder -misshandlung; Beispiel für Auskunftsanspruch außerhalb des SGB: Lebensmittelüberwachung, Umweltschädigung) oder der Vermeidung einer Schädigung der Staatskasse (SGB: Sozialleistungsbetrug; Auskunftsanspruch außerhalb des SGB: Steuerhinterziehung) hat im Falle des redlichen Hinweisgebers das Interesse an einer (zugunsten des Ehrenschutzes des Hinweisbetroffenen stattfindenden) Strafverfolgung zurückzutreten.

(4) *Welche Übermittlungs-Befugnis besteht, wenn eine richterliche Anordnung nach § 73 Abs. 3 SGB X vorliegt*?

(4.1) Diese für § 68 Abs. 1 Satz 1 SGB X aufgewiesene Beschränkung muss auch für § 73 Abs. 2 SGB X gelten, also für Strafverfahren wegen Straftaten, die nicht Verbrechen sind (wie also z. B. §§ 186 f. StGB, üble Nachrede und Verleumdung, aber auch der demgegenüber schwerere Fall des § 188 StGB) und auch nicht aus anderen Gründen eine Straftat von erheblicher Bedeutung. Es darf mithin dann nicht die Person genannt werden (weil der Sachverhalt ja im Kern, freilich ohne Personenbezug, schon bekannt ist).

(4.2) Anderes gilt nur im Falle des § 73 Abs. 1 SGB X. Eine Verleumdung wird jedoch nur in höchst seltenen Fällen eine Straftat von erheblicher Bedeutung sein. Aber in jedem Fall der Verleumdung, d. h. der vorsätzlichen Falschangabe, hat ohnehin der Hinweisbetroffene zumindest das Recht auf uneingeschränkte Auskunft der Behörde darüber, was diese von den Angaben des Hinweisgebers in ihren Unterlagen festgehalten hat, einschließlich Angaben, die den Hinweisgeber unmittelbar identifizieren (Personalien).

(4.3) Für die Klärung der Frage, ob eine Verleumdung als *Straftat von erheblicher Bedeutung* im Sinne von § 73 Abs. 1 SGB X anzusehen ist, ist der Sozialleistungsträger dabei nur beschränkt verantwortlich: § 73 Abs. 3 SGB X regelt, dass die Übermittlung von Sozialdaten nur auf Anordnung des Ermittlungsrichters erfolgen darf. Der Richter hat dabei zu überprüfen, ob ein Anfangsverdacht vorliegt, ob der Umfang des Übermittlungsersuchens der jeweiligen Qualifikation der Straftat entspricht und ob die Übermittlung von Sozialdaten für die Aufklärung der Straftat erforderlich ist und den Grundsätzen der Verhältnismäßigkeit entspricht (Hauck/ Noftz, § 73 SGB X, Rdnr. 36). Damit trägt der Ermittlungsrichter auch die Verantwortung für die Auslegung des § 73 Abs. 1 und 2 SGB X. Die Prüfung des Sozialleistungsträgers hingegen beschränkt sich darauf, ob das Ersuchen von einem Strafverfolgungsorgan (Staatsanwaltschaft oder deren Hilfsbeamte) gestellt worden ist und

ob eine formell rechtmäßige Anordnung vorliegt. Die Fragen der materiellen Rechtmäßigkeit entziehen sich der Beurteilungskompetenz des Sozialleistungsträgers (Hauck/Noftz, § 73 SGB X Rdnr. 40). Bestehen in diesen Fragen Zweifel bei dem Leistungsträger, kann dieser Beschwerde gemäß § 304 StPO einlegen, man wird ihn schwerlich als dazu verpflichtet ansehen können.

Das bedeutet letztlich, dass, wenn der Richter das Vorliegen einer Straftat von erheblicher Bedeutung nach § 73 Abs. 1 SGB X bejaht, diejenigen Sozialdaten übermittelt werden dürfen und müssen, deren Übermittlung richterlich angeordnet ist.

10.2.15 Begrüßungsgeld zu Kontrollzwecken und verdachtslose Totalerfassung durch das Jugendamt - oder: Auch Bemühungen zur Verhinderung von Kindeswohlgefährdung müssen den Datenschutz wahren

(1) Aufgrund spektakulärer Fälle von Tötungen oder tödlicher Vernachlässigung von Kleinkindern sowie massiver Kindeswohlgefährdung durch Misshandlung oder Verwahrlosung, entwickeln sich auch in Sachsen allenthalben Aktivitäten, das rechtzeitige Erkennen von das Kindeswohl gefährdenden Entwicklungen namentlich durch Organisierung entsprechender Beobachtungs- und Informationsweitergabetätigkeiten verschiedener Stellen zu ermöglichen. Vielfach will man örtlich begrenzt entsprechendes Vorgehen erproben, ohne auf den Gesetzgeber, insbesondere auch den Bundesgesetzgeber, zu warten, der ja mit § 8a SGB VIII erst vor nicht allzu langer Zeit eigentlich schon weitgehende Befugnisse für die Jugendämter neu geschaffen hat.

(2) Ein Landratsamt hat ein „Frühwarnsystem“ schaffen wollen, das es, nachdem ich aufgrund eines Zeitungsberichtes nachgefragt hatte, mir mit folgenden bemerkenswert klaren Worten beschrieben hat:

„Nach der Geburt eines Kindes soll die zuständige Meldebehörde bzw. das Standesamt das Jugendamt über die Geburt des Kindes informieren. Das Jugendamt erfasst diese Daten und legt sich ein Verzeichnis mit den Geburten an. Im Anschluss sendet das zuständige Jugendamt ein Schreiben an die betreffenden Eltern, worin mitgeteilt wird, dass auf Wunsch ein Begrüßungsgeld für das jeweilige Kind gezahlt wird. Der beiliegende Antrag auf Auszahlung des Begrüßungsgeldes beinhaltet dann eine Klausel, dass der betreffende Empfänger mit seiner Unterschrift einwilligt, dass seine Daten gespeichert und verarbeitet werden können. Im Anschluss soll das Begrüßungsgeld vor Ort von einem Dritten (evtl. Freier Träger, Sparkasse) ausgezahlt werden und im zweiten Schritt nach der Einwilligung ein Hausbesuch für die Übergabe des zweiten Elternbriefes nach sechs Monaten erfolgen. Eltern, welche von dem

Begrüßungsgeld keinen Gebrauch machen, werden durch den Abgleich der Liste des Jugendamtes mit den zurückgelaufenen Auszahlungsquittungen persönlich durch Mitarbeiter des Frühwarnsystems aufgesucht."

(3) Das Landratsamt hatte sich auch schon Gedanken über die mögliche rechtliche Grundlage solcher Aktivitäten gemacht, und eine Vermutung, dass das geplante System die eine oder andere diesbezügliche Schwachstelle haben könnte, hat das Landratsamt vorsorglich mir gegenüber auch gleich zu erkennen gegeben. Dabei kam es auf die vom Landratsamt erwähnte Frage, inwieweit die Meldebehörden oder die Standesämter zu den entsprechenden Datenübermittlungen an das Jugendamt berechtigt wären, jedoch gar nicht an. Denn was geplant war, hätte schon gegen das geltende Sozial(datenschutz)recht verstoßen, schon die beabsichtigten Tätigkeiten des *Jugendamtes* (sc. des Landkreises oder auch einer Kreisfreien Stadt) wären also unzulässig gewesen:

(4.1) Die im Rahmen des geplanten „Frühwarnsystems" beabsichtigte ‚Besorgung' von Daten neugeborener Kinder und insbesondere deren Eltern bei den Meldebehörden beziehungsweise Standesämtern wäre eine Datenerhebung des Jugendamts. Eine Rechtsgrundlage, die das Jugendamt berechtigte, entsprechende Daten zu erheben, besteht jedoch nicht. Nach § 62 Abs. 1 SGB VIII ist eine Datenerhebung seitens des Jugendamts nur insoweit zulässig, als dies zur Erfüllung einer Aufgabe des Jugendamts nach dem Sozialgesetzbuch erforderlich ist. Hierzu zählt indes - auch unter Beachtung des in § 16 SGB VIII normierten Unterstützungsauftrags des Trägers der öffentlichen Jugendhilfe - nicht die persönliche Aushändigung von - wie dem erwähnten Zeitungsbericht zu entnehmen war - einzelnen auf die jeweilige Entwicklungsphase zugeschnittenen Briefen an die Eltern neugeborener Kinder. Eine dahingehende Datenerhebungsbefugnis des Jugendamts besteht nach § 62 Abs. 3 Nr. 2, Buchst. d SGB VIII vielmehr erst, wenn dies zur Erfüllung des Schutzauftrags des Jugendamts bei (dem Verdacht) einer Kindeswohlgefährdung nach § 8a SGB VIII erforderlich ist. Dies wäre jedoch bei der hier geplanten generellen und insbesondere verdachtsunabhängigen Datenerhebung gerade nicht der Fall. Dies hatte das Landratsamt auch schon selbst vermutet.

(4.2) Gleiches gilt im Ergebnis für das geplante Verfahren betreffend die Einführung eines Begrüßungsgeldes. Hier ist nicht ersichtlich, inwieweit dies eine Leistung darstellen könnte, die in die Aufgabenzuständigkeit des Jugendamts fällt. Darüber hinaus wäre eine Datenerhebung und -weiterverarbeitung seitens des Jugendamts jedenfalls nur insoweit zulässig, als dies für die Bearbeitung von Anträgen auf Auszahlung des Geldbetrags erforderlich wäre. Dies gilt auch für die Speicherung

wie die Nutzung der im Rahmen der Bearbeitung des Antrags erhobenen Daten. Inwieweit zur Bearbeitung des Antrages dabei ein Hausbesuch erforderlich sein soll, erschließt sich nicht. Denn gerade auch die Durchführung von Hausbesuchen ist im Hinblick auf Art. 13 GG ausschließlich im Rahmen der Aufgabenerfüllung zur Sachverhaltsermittlung zulässig, wenn deren Notwendigkeit im Einzelfall plausibel gemacht wird. Ein generelles Besichtigungsrecht im Rahmen der Leistungsgewährung besteht (zumindest nach geltendem Recht) nicht.

(4.3) Der Nachweis der Erforderlichkeit eines Hausbesuchs im Einzelfall kann auch nicht durch die pauschale Einholung von Einwilligungen umgangen werden. Zudem wäre es fraglich, ob bei einer derartigen Verknüpfung von Leistungsantrag und Hausbesuch noch vom Vorliegen der erforderlichen Freiwilligkeit bei der Abgabe der Einwilligungserklärung ausgegangen werden könnte. Die Durchführung von Hausbesuchen und die damit verbundene Erhebung personenbezogener Daten ist aber im Anwendungsbereich des Sozialgesetzbuchs auch schon deswegen nicht aufgrund bloßer Einwilligung zulässig, weil § 62 SGB VIII wie auch § 67a SGB X dies für die Datenerhebung gar nicht als Erlaubnistatbestand vorsehen und dadurch gemäß § 35 Abs. 2 SGB I ausschließen. Der Inhalt dieser Vorschriften ist Ausdruck bzw. Auswirkung eines auch außerhalb des Anwendungsbereichs des Sozialgesetzbuchs geltenden Prinzips: Kraft des verfassungsrechtlichen *Grundsatzes des Vorbehaltes des Gesetzes* (vgl. Art. 20 Abs. 3, 2. Halbs. GG i. V. m. der Grundrechtsbindung, Art. 1 Abs. 3 GG, und dem Demokratieprinzip, Art. 20 Abs. 1 GG) dürfen Träger öffentlicher Gewalt nicht in größerem Maße ihnen im Gesetz nicht ausdrücklich zugewiesene Aufgaben mit Hilfe einer lediglich durch Einwilligung der Betroffenen gerechtfertigten Verarbeitung personenbezogener Daten an sich ziehen und erfüllen und dazu durch Verarbeitung personenbezogener Daten in Grundrechte eingreifen.

(4.4) Dies gilt insbesondere für die ebenfalls geplanten Hausbesuche bei denjenigen Eltern, die kein Begrüßungsgeld beantragen. Soweit keine Leistung beansprucht bzw. beantragt wird, scheidet selbstverständlich eine Datenerhebung wie auch -weiterverarbeitung mangels Erforderlichkeit für die Erfüllung einer durch Gesetz ausdrücklich zugewiesenen Aufgabe von vornherein aus. Kurz: Es bedarf keiner Datenerhebung seitens des Jugendamts oder eines Nachweises seitens der Eltern, wenn man nichts vom Staat möchte. Insbesondere begründet der Umstand, keine staatlichen Hilfen in Anspruch zu nehmen, noch nicht den Verdacht einer Kindeswohlgefährdung. Eine dennoch erfolgende Verarbeitung personenbezogener Daten der Eltern durch das Jugendamt, insbesondere auch in Form des vorgesehenen Datenabgleichs, wäre ein eklatant rechtswidriger Eingriff in das Recht der betroffenen Eltern auf informationelle Selbstbestimmung.

(5) Es bleibt allein dem Gesetzgeber - der bislang den Schutzauftrag der Kinder- und Jugendhilfe auf die Fälle der Kindeswohlgefährdung beschränkt hat - überlassen, im Bedarfsfall die rechtlichen Grundlagen zu schaffen, um eine *einzelverdachtslose Totalerfassung*, wie sie hier beabsichtigt war, zu erreichen, wobei die entsprechenden Regelungen den verfassungsrechtlichen Anforderungen, namentlich Art. 6 Abs. 1 bis 3 GG wie auch Art. 2 i. V. m. Art. 1 GG, genügen müssten.

(6) Es verbleibt die datenschutzrechtlich unbedenkliche Möglichkeit, den betreffenden Eltern bereits bei einem vor dem Geburtstermin erfolgenden Krankenhausbesuch bzw. nach der Entbindung durch das Krankenhaus oder bei Anzeige der Geburt des Kindes (§ 16 PStG) durch das Standesamt einen entsprechenden (ersten) Elternbrief auszuhändigen mit dem darin enthaltenen schriftlichen Hinweis, dass Eltern, soweit sie dies wünschen, direkt mit dem Jugendamt in Verbindung treten und dort mitteilen können, falls sie die Zusendung weiterer Elternbriefe wünschen. Diese Verfahrensweise könnte auch auf sonstige Stellen angewandt werden, welche in der Regel von werdenden Eltern aufgesucht werden (z. B. Einrichtungen, die Schwangerschaftsgymnastikkurse anbieten, oder Hebammen). Auf die Möglichkeit der schriftlichen Beantragung eines Begrüßungsgeldes kann dabei ebenfalls hingewiesen werden.

(7) Der Ansatz, von Staats wegen dafür zu sorgen, dass die Eltern bei der Erfüllung der ihnen zukommenden Aufgabe, ihre Kinder liebevoll und fürsorglich großzuziehen (Art. 6 Abs. 2 Satz 1 GG fällt gegenüber anderen Grundrechtsgewährleistungen dadurch auf, dass dieses (Pflicht-)Recht als „natürlich“ bezeichnet wird, die „Überpositivität“ dieses Grundrechts wird also besonders betont, das Grundgesetz beruft sich hier offenbar explizit auf eine anthropologische Naturkonstante), gestärkt werden und Unterstützung angeboten bekommen (statt dass der Staat ihnen diese Aufgabe in größerem Maße abnimmt oder von Dritten abnehmen lässt), ist sicherlich die verfassungsgemäße, namentlich grundrechtswahrende und dem Menschenbild der Demokratie entsprechende Herangehensweise. Aber auch diese Bestrebungen müssen sich, sofern sie mit Grundrechtseingriffen wie namentlich mit Eingriffen in das Grundrecht auf informationelle Selbstbestimmung einhergehen, auf Problem-Gruppen beschränken - die datenschutzrechtliche Lage ist insoweit letztlich nicht anders als im Sicherheits-Bereich oder im Bereich der Steuererhebung oder der sozialen Leistungsmissbrauchskontrolle: Die einzelverdachtslose Totalerfassung kann nur unter Grenzbedingungen zulässig sein.

(8) Dass die öffentliche Gewalt auch aus anderen, ebenso trivialen wie durchschlagenden Gründen gerade auch im Bereich des Kindeswohles gut daran tut, insoweit ihre Datenverarbeitungs-Aktivitäten auf die vergleichsweise wenigen, extremen Fälle

zu konzentrieren, zeigt die Erkenntnis, dass in den in der Öffentlichkeit bekannt gewordenen spektakulären Fällen von voraussehbar gewesener Tötung bzw. länger andauernder Misshandlung oder Verwahrlosung von Kindern es nicht auf fehlende Datenerhebungsbefugnisse zurückzuführen gewesen ist, wenn sie nicht behördlicherseits verhindert worden sind - die für ein Eingreifen nötigen Informationen haben den zuständigen Stellen durchaus vorgelegen. Vielmehr hat es sich in diesen Fällen um eine fehlerhafte (oder wegen Überlastung mangelhafte) Bearbeitung oder Verfahrensweise seitens der zuständigen Behörden gehandelt.

(9) *Zusammengefasst* lässt sich als Ergebnis auch für andere in diesem Problemfeld angestellte Überlegungen vor allem festhalten, dass die Totalerfassung sämtlicher Eltern (neugeborener Kinder) wie auch insbesondere deren Überprüfung bei der Ausübung der elterlichen Sorge durch das Jugendamt bzw. für diese durch freie Träger der Jugendhilfe ohne konkrete Verdachtsmomente für eine Kindeswohlgefährdung nach geltendem Recht nicht vorgesehen ist, mit der Folge, dass auch hierauf abzielende diesbezügliche Datenerhebungen sowie anschließende Datennutzungen rechtswidrig wären. (Art. 6 Abs. 2 Satz 1 GG dürfte einer dahingehenden Regelung wohl entgegenstehen; anderes gälte wohl, wenn die [Dienst-]Leistung der Eltern, ihre Kinder [nicht nur durch Aufwendungen zu versorgen, sondern auch] zu *pflegen und zu erziehen* [so die Formulierung des Grundgesetzes] finanziell honoriert würde: Dann dürfte sich der Staat - wie in anderen Zusammenhängen auch - ein Bild davon machen, ob das von ihm gegebenen Geld auch die gewollte und nötige Wirkung hat: Daten gegen Geld, Geld gegen Daten, ein ganz normaler „Tausch"-Vorgang im Zusammengang staatlicher Leistungsgewährung.)

Und ferner: Einwilligung ist kein Ausweg. Denn Träger öffentlicher Gewalt - und zu diesen zählen auch die Jugendämter - dürfen nicht dort, wo ihnen keine Aufgaben und Befugnisse zur Verarbeitung personenbezogener Daten vom Gesetz zugewiesen worden sind, Aufgaben an sich ziehen oder Ziele verfolgen und sich die Grundlagen für die Verarbeitung der dafür erforderlichen personenbezogenen Daten durch Einholung von Einwilligungen beschaffen.

Auch hier wird deutlich - es ändert nichts an aufgefallenen Missständen, wenn statt fehlender notwendiger Kapazitäten der Jugendämter rechtliche Kompetenzen ausgeweitet werden.

Es zeichnet sich ab, dass dieses Thema den Datenschutz in der nächsten Zukunft sehr stark beschäftigen wird.

10.2.16 Überlassung einer Wohngeldakte an die Staatsanwaltschaft für ein Ermittlungsverfahren wegen Betrugsverdachts

Schwierigkeiten bereiten immer wieder die Übermittlungsvorschriften des SGB X, insbesondere auch, was ihren jeweiligen Anwendungsbereich betrifft.

So sah sich die Wohngeldstelle eines Landratsamtes daran gehindert, der Staatsanwaltschaft eine Wohngeldakte zu übersenden, nachdem dort ein Vermieter Anzeige erstattet hatte, da seine Mieterin zwar Wohngeld erhielt, dieses jedoch nicht zur Mietzahlung verwendete. Die Wohngeldstelle sah sich an einer Übermittlung der Akte aufgrund der Vorschrift des § 73 SGB X gehindert, wonach gemäß Absatz 3 der Vorschrift die Übermittlung eine vorherige richterliche Anordnung voraussetzt, die aber hier nicht vorlag.

Eine richterliche Anordnung als Voraussetzung für eine Weitergabe der Wohngeldakte war in diesem Fall aber gar nicht erforderlich. Denn die gesetzliche Übermittlungsbefugnis der Wohngeldstelle ergab sich hier aus § 69 Abs. 1 Nr. 2 SGB X: Die Datenübermittlung ist danach zulässig, soweit sie für die Durchführung eines mit der Erfüllung einer *gesetzlichen Aufgabe der übermittelnden Stelle* nach dem Sozialgesetzbuch zusammenhängenden gerichtlichen Verfahrens, einschließlich eines Strafverfahrens, erforderlich ist, wobei unter letzteres auch schon ein staatsanwaltschaftliches Ermittlungsverfahren fällt (siehe hierzu 12/10.2.10).

Hinsichtlich des nach § 69 Abs. 1 Nr. 2 SGB X geforderten Zusammenhanges des gerichtlichen Verfahrens mit einer gesetzlichen Aufgabe nach dem Sozialgesetzbuch reicht dabei jede Aufgabe aus, die, wie es in § 30 Abs. 4 SGB IV formuliert ist, *gesetzlich vorgeschrieben oder zugelassen ist, die sich also aus dem Sozialgesetzbuch ergibt* (v. Wulffen/ Bieresborn, Rdnr. 13 zu § 69 SGB X). Zu den gesetzlichen Aufgaben eines Sozialhilfeträgers zählt namentlich, zu überprüfen, ob die Voraussetzungen für die Leistungsgewährung vorliegen oder ob Zahlungen zu Unrecht erfolgt sind und deshalb zurückgefordert werden müssen (v. Wulffen/ Bieresborn a. a. O.). Die Bekämpfung des Missbrauchs von Sozialleistungen durch Gerichte und Staatsanwaltschaften weist daher diesen Zusammenhang mit den sozialrechtlich begründeten Aufgaben des Sozialleistungsträgers auf.

Ein solcher Fall lag hier vor. Nach den für die Wohngeldstelle maßgebenden (§ 67d Abs. 2 Satz 2 SGB X) Angaben der Staatsanwaltschaft bestand ein für die Durchführung eines Ermittlungsverfahrens hinreichender Anfangsverdacht, dass die betreffende Wohngeldempfängerin Wohngeld, jedenfalls zum Teil, nicht an den Vermieter „weitergereicht“, sondern für sich behalten, insbesondere auch nicht an die Wohn-

geldstelle zurückgezahlt, und sich dadurch strafbar gemacht hatte. Den §§ 1 Abs. 1, 28 Abs. 1 Satz 2 und 30 Abs. 2 Satz 1 und 2 WoGG kann man jedoch entnehmen, dass der Anspruch auf Wohngeld davon abhängig ist, dass der Empfänger es für die Begleichung seiner Miet- bzw. Darlehensschuld verwendet. Die zweckentsprechende Zahlung des Wohngeldempfängers an den Dritten ist demnach von der Behörde zu beobachten bzw. sicherzustellender Leistungszweck. Insoweit daher bei einer Zweckentfremdung von Wohngeld Betrug (oder Veruntreuung) zu Lasten der Wohngeldstelle als Straftatbestand in Frage kommt, liegt der in § 69 Abs. 1 Nr. 2 SGB X verlangte Zusammenhang vor.

Was die Art und Weise der Übermittlung betrifft, kommt es auch bei der Vorschrift des § 69 Abs. 1 SGB X auf die Erforderlichkeit an. Dafür reichte hier derjenige Teil der Wohngeldakte aus, der sich auf die maßgebende angebliche Tatzeit bezog. Sinnvoll davon abtrennbare Teile der Akte (s. § 67d Abs. 3 SGB X) durften nicht übermittelt werden. Einen Grund dafür, die Staatsanwaltschaft dagegen auf bloße Auskunftserteilung zu beschränken und Akteneinsicht erst dem Gericht zuzubilligen, wie dies wohl ebenfalls vertreten wird (so anklingend bei v. Wulffen/Bieresborn a. a. O. Rdnr. 26), sehe ich nicht; § 67d Abs. 3 SGB X spricht für das Gegenteil.

Soweit es sich dagegen *nicht* um eine Straftat *zu Lasten der Wohngeldbehörde* als einer der in § 35 SGB I genannten Stellen gehandelt hätte, sondern um die Verfolgung von Straftaten, die zum Nachteil Dritter verübt werden, wäre in der Tat dann § 73 SGB X die maßgebliche Vorschrift gewesen, der gemäß Absatz 3 jedoch eine Befugnis zur Datenübermittlung nur aufgrund der (vorherigen) Entscheidung des zuständigen Ermittlungsrichters zulässt.

Abschließend noch ein Hinweis: Oft werde ich von Behörden gefragt, ob sie denn zur Datenübermittlung *verpflichtet* sind. Antwort: Ob die Behörde nicht nur *berechtigt*, sondern auch *verpflichtet* ist, die verlangten Angaben zu übermitteln, habe ich nicht zu beurteilen, denn datenschutzrechtlich stellt sich nur die Frage, ob die Übermittlung zulässig ist. Ich erlaube mir aber in diesen Fällen den Hinweis, dass in dem durch die datenschutzrechtlichen Übermittlungserlaubnisse gesetzten Rahmen (und nur in diesem!) Amtshilfepflichten bestehen können (vgl. im Einzelnen § 4 SGB X).

10.2.17 Datenabgleichsbefugnisse des Rechnungsprüfungsamtes im Bereich des Sozialdatenschutzes?

Das Rechnungsprüfungsamt eines Landratsamtes hat mich gefragt, ob datenschutzrechtliche Einwände dagegen bestünden, dass es die Daten der SGB II-Behörde des Landkreises (sog. Optionskommune, vgl. 10.2.1) mit den Daten der Abfallbehörde

abgleicht, um auf diese Weise eventuell „fingierte Akten“, wie das Amt formuliert hat, von Hilfeempfängern aufspüren wie auch die Angaben der Hilfeempfänger auf Richtigkeit prüfen zu können.

Das Ergebnis war: Die SGB II-Behörde ist zwar befugt, dem Rechnungsprüfungsamt Sozialdaten zu übermitteln, jedoch nicht zu dem genannten Zweck eines Datenabgleichs mit Daten der Abfallbehörde. Ein solcher Datenabgleich wäre nämlich unzulässig. Das ergibt sich im Einzelnen aus Folgendem:

Damit tatsächlich eine effektive Finanzkontrolle ermöglicht wird, umfasst das Prüfungsrecht des Rechnungsprüfungsamts auch die Befugnis, sich Unterlagen mit personenbezogenen Daten vorlegen zu lassen. Dadurch soll zum einen dem Umstand Rechnung getragen werden, dass das Prüfungsrecht eines Rechnungsprüfungsamts grundsätzlich nicht bereits durch die Prüfungsbefugnisse oder allgemeinen Aufsichtsbefugnisse anderer Rechtsträger eingeschränkt oder ausgeschlossen ist. Die Prüfung durch das Rechnungsprüfungsamt ist vielmehr als eigenständiges Kontrollinstrument neben den diesbezüglichen Aufgaben und Befugnissen der Aufsichtsbehörde konzipiert, wobei das Rechnungsprüfungsamt im Rahmen seiner Prüftätigkeit unabhängig und weisungsfrei tätig wird (§ 103 Abs. 2 Satz 2 SächsGemO, § 4 KomPrüfO) und hierfür auch gemäß § 103 Abs. 1 Satz 1 SächsGemO als eigenständige Organisationshoheit, getrennt von anderen Ämtern der Gemeinde, eingerichtet ist. Diese Unabhängigkeit überlässt dem Rechnungsprüfungsamt die Beurteilung, welche Unterlagen bzw. Daten es für seine Kontrolltätigkeit konkret benötigt, sowie die Befugnis, insoweit auch Zeitpunkt, Gegenstand und Inhalt der Prüfung (Voll- oder Stichprobenprüfung) frei zu wählen. Insoweit stehen auch weder das Steuergeheimnis noch das Sozialgeheimnis seinen Prüf- und Erhebungsrechten grundsätzlich entgegen (siehe bereits 12/10.2.8).

Bei der hier vorgesehenen Datenweitergabe von der SGB II-Behörde an das Rechnungsprüfungsamt hätte es sich in datenschutzrechtlicher Hinsicht nicht lediglich um eine Datennutzung, sondern - da eine Datenweitergabe an eine andere *Stelle im funktionalen Sinn* vorgenommen worden wäre - um eine Daten*übermittlung* gehandelt. Die dafür wegen §§ 67b Abs. 1 Satz 1, 67d Abs. 1 SGB X i. V. m. § 35 Abs. 1 Satz 4, letzter Fall SGB I erforderliche gesetzliche Befugnis zu Übermittlung müsste § 69 Abs. 5 i. V. m. § 67c Abs. 3 SGB X entnommen werden. Danach ist die Übermittlung von Sozialdaten zulässig für die Erfüllung der gesetzlichen Aufgaben der Rechnungshöfe und der anderen Stellen, auf die § 67c Abs. 3 Satz 1 SGB X Anwendung findet, hier die Durchführung von Rechnungsprüfungen durch ein örtliches Rechnungsprüfungsamt.

Die im Gesetz dem Rechnungsprüfungsamt übertragene Aufgabe bzw. Befugnis hinsichtlich der Prüfung der Haushalts- und Wirtschaftsführung der zu überprüfenden Behörde ist - auch unter Beachtung der für das Rechnungsprüfungsamt geltenden Unabhängigkeit - *nicht unbegrenzt*, die *Rechtmäßigkeitskontrolle* ist von ihr allerdings umfasst (Schmid in Quecke/Schmid, SächsGemO, § 103 Rdnr. 62). Dies bedeutet, die Rechnungsprüfung erstreckt sich auch auf die Frage, ob die Entscheidungen der zu prüfenden Stelle rechtsfehlerfrei zustande gekommen sind, also ob die Behörde die für sie maßgeblichen Rechtsvorschriften - aber auch nur diese! - ordnungsgemäß angewandt hat.

Daraus folgt jedoch, dass eine (Über-)Prüfung nur in dem Umfang und mit denjenigen Daten zulässig ist, die auch der zu überprüfenden Behörde im Rahmen ihrer Aufgabenerfüllung zur Verfügung stehen und von ihr zu beachten sind. Das heißt: Dem Rechnungsprüfungsamt können nicht mehr Datenverarbeitungsbefugnisse zur Prüfung der Rechtmäßigkeit von Entscheidungen der zu überprüfenden Behörde zustehen als dieser selbst. Insbesondere folgt daraus, dass das Rechnungsprüfungsamt für seine Prüfzwecke nicht mehr Daten erheben und auf sonstige Weise verarbeiten darf, als dies auch der zu überprüfenden Stelle nach den für sie maßgebenden Vorschriften von Rechts wegen möglich (d. h. erlaubt) ist.

Mit anderen Worten: Die aus den Prüfungsbefugnissen sich ergebenden Datenverarbeitungsbefugnisse des Rechnungsprüfungsamtes können nicht weiter gehen als die Datenverarbeitungsbefugnisse der zu überprüfenden Stelle, hier also der SGB II-Behörde. Darüber hinausgehende Datenverarbeitungen wären unzulässig, da Ergebnisse hieraus der zu prüfenden Stelle - mangels eines von ihr begangenen Rechtsverstoßes - nicht vorgehalten werden dürften und damit zur Aufgabenerfüllung des Rechnungsprüfungsamts auch nicht geeignet wären.

Aufgrund dessen wäre die Übermittlung an das Rechnungsprüfungsamt zum Zweck eines Abgleichs der Daten mit denjenigen der Abfallbehörde unzulässig, da ein solcher Abgleich der SGB II-Behörde selbst nicht erlaubt wäre: § 52 SGB II sieht keinen Datenabgleich mit der Abfallbehörde vor.

Kurz gesagt gilt: Eine Datenübermittlung an das Rechnungsprüfungsamt zur Durchführung eines Datenabgleichs, der um Übermittlung ersuchten Fachbehörde ist nicht erlaubt.

10.2.18 Zum Auskunftsanspruch gemäß § 18 SächsDSG

Dem SMS habe ich etliche Fragen zur Anwendung des § 18 SächsDSG beantwortet (die Tätigkeitsbereiche des Staatsministeriums außerhalb der vorrangigen Spezialvorschrift des § 83 SGB X betreffend, der allerdings eine weitgehende Ähnlichkeit mit der entsprechenden Regelung im Sächsischen Datenschutzgesetz hat). Einiges davon dürfte von allgemeinerem Interesse sein:

(1) Gemäß § 18 Abs. 1 SächsDSG ist dem Betroffenen von der Daten verarbeitenden Stelle auf Antrag kostenfrei und ohne unzumutbare Verzögerung Auskunft zu erteilen über folgende Sachverhalte (*als Gegenstand des Anspruches*):

1. die zu seiner Person gespeicherten Daten,
2. den Zweck und die Rechtsgrundlage der Verarbeitung,
3. die Herkunft der Daten und die Empfänger von Übermittlungen sowie die übermittelten Daten, soweit dies gespeichert oder sonst bekannt ist und
4. die Auftragnehmer im Sinne des § 7, sofern diese Daten des Betroffenen verarbeiten.

(2) Dieser Auskunftsanspruch unterliegt jedoch Beschränkungen.

(3) Grundsätzlich ist dem Betroffenen über die in § 18 Abs. 1 Nr. 1 bis 4 SächsDSG genannten Sachverhalte *Auskunft* zu erteilen.

Diesen *Anspruchsinhalt* konkretisiert Absatz 3 dahingehend, dass bei der Verarbeitung (Speicherung) der Daten in *Akten* anstelle der Auskunftserteilung auf Verlangen *Einsicht* in diese zu gewähren ist.

(4) Nach § 18 Abs. 4 SächsDSG bestimmt die Daten verarbeitende Stelle das Verfahren, insbesondere die Form der Auskunftserteilung bzw. Einsichtnahme nach pflichtgemäßem Ermessen, wobei berechtigte Interessen Dritter nicht beeinträchtigt werden dürfen.

Absatz 4 regelt also nicht das „Ob“ der Auskunftserteilung, sondern das „Wie“. In diesem Sinne ist auch die in Absatz 4 enthaltene Einschränkung zu verstehen. Es geht insoweit nur darum, die berechtigten Interessen Dritter bei der Ausgestaltung der Form der Auskunftserteilung zu wahren. Damit soll der Daten verarbeitenden Stelle etwa die Möglichkeit eingeräumt werden, Auskunft über elektronisch erfasste personenbezogene Daten zu geben, ohne dass der Betroffene selbst den Rechner

nutzen muss. § 18 Abs. 4 SächsDSG und die darin enthaltene Beschränkung des Auskunftsanspruchs regelt nur die *Form* der Auskunft.

(5) Eine Einschränkung des *Inhalts* (Umfangs) der Auskunftserteilung - unter Einschluss der Akteneinsicht! - nimmt dagegen erst *Absatz 5* SächsDSG vor. Dabei geht es um die Frage, *ob*, genauer: in welchem Umfang, Auskunft zu erteilen ist. Erst in diesem Absatz fordert das Gesetz eine Abwägung zwischen den hier in Nr. 1 bis 3 genannten, mit den Interessen des Betroffenen widerstreitenden Interessen. Anders als beim „Wie“ der Auskunftserteilung nach Absatz 4 hat die Daten verarbeitende Stelle beim „Ob“ der Auskunftserteilung nach Absatz 5 kein Ermessen. Dies ergibt sich bereits aus dem Wort „unterbleibt“, aber auch daraus, dass der Gesetzgeber - anders als in Absatz 4 - die Erwähnung des pflichtgemäßen Ermessens unterlassen hat. Um es hervorzuheben: Der Daten verarbeitenden Stelle ist bei der Prüfung der Frage, inwieweit eine Auskunftserteilung bzw. Einsichtsgewährung aus Gründen des § 18 Abs. 5 Nr. 1 bis 3 SächsDSG unterbleiben soll, kein Ermessen eingeräumt. Insoweit die Behörde zu dem Ergebnis kommt, dass die Interessen des Betroffenen an der Auskunftserteilung die in Absatz 5 genannten Interessen überwiegen, ist Auskunft zu erteilen bzw. Einsicht zu gewähren. Für den umgekehrten Fall gilt das Gegenteil.

Dabei gilt freilich, dass Auskunftserteilung bzw. Akteneinsicht *insoweit* zu verwehren sind, als einer der in Absatz 5 Nr. 1 bis 3 genannten Gründe entgegensteht und schwerer wiegt als das Auskunftsinteresse des Betroffenen. Für die Betroffenen-Daten, auf die dies nicht zutrifft, besteht kein Grund, Auskunft bzw. Akteneinsicht zu verweigern.

Diese Auskunfts- bzw. Akteneinsichtsverweigerung kann durch Schwärzen der betreffenden Daten in einer vorzulegenden bzw. auszuhändigenden Ablichtung erfolgen. Ist dies nicht möglich, kommt auch ein Entfernen oder anderes Unzugänglichmachen des betreffenden Akteninhalts in Betracht. Dies darf allerdings nur in der Weise erfolgen, dass der Auskunftsersuchende erkennt, dass ihm Einsicht in bestimmte Aktenteile nicht gewährt wird. Nur wenn er weiß, dass er teilweise keine Einsicht gewährt bekommt, kann er seine Rechte aus § 18 Abs. 6 SächsDSG wirklich ausüben.

(6) Fraglich ist, wie ein Auskunftsersuchen zu behandeln ist, wenn zu befürchten steht, dass beabsichtigte Maßnahmen bzw. deren Erfolge beeinträchtigt werden. Unabhängig davon, dass eine solche Fallgestaltung außerhalb des § 29 VwVfG - auf die dann § 18 SächsDSG natürlich gleichwohl anwendbar wäre - kaum vorstellbar ist,

weil einer derartigen Maßnahme in der Regel ein Verwaltungsverfahren vorausgehen muss, gilt Folgendes:

In Betracht käme allein ein Auskunftsverbot (Auskunftsanspruchseinschränkung) nach § 18 Abs. 5 Nr. 1 SächsDSG aus dem Grunde, dass die Auskunft die öffentliche Sicherheit gefährden oder für das Wohl des Freistaates Sachsen, eines anderen Landes oder des Bundes Nachteile bereiten würde. Eine Gefährdung der öffentlichen Sicherheit ist nach den allgemeinen Regeln des Polizeirechts gegeben, wenn die objektive Rechtsordnung, subjektives Recht oder Rechtsgüter des Einzelnen oder Einrichtungen und Veranstaltungen des Staates gefährdet sind (vgl. Auernhammer, § 19 BDSG Rdnr. 29). Eine solche Gefährdung käme etwa bei geplanten Strafverfolgungsmaßnahmen in Betracht oder auch dann, wenn mit der Auskunft ein anderer gesetzlich verfolgter Zweck - etwa eine behördenärztliche oder andere behördliche Maßnahme - gefährdet würde.

Das Wohl des Bundes oder eines Landes umfasst nur die wesentlichen Interessen der Gebietskörperschaften. Dazu zählen insbesondere die äußere und innere Sicherheit. Das Wohl des Landes oder des Bundes ist somit ein Oberbegriff, der bereits die öffentliche Sicherheit umfasst, wie im Wortlaut des § 19 Abs. 4 BDSG zum Ausdruck kommt. Die Feststellung der Gefährdung und die nach § 18 Abs. 5 SächsDSG nötige Abwägung erfolgt jeweils durch Anwendung der unbestimmten Rechtsbegriffe, die gerichtlich voll nachprüfbar ist.

(7) Wird dem Betroffenen die Akteneinsicht verweigert, ist dies entsprechend zu bescheiden. Der Bescheid ist grundsätzlich zu begründen. Dieses Begründungserfordernis ist ausnahmsweise eingeschränkt, wenn die Voraussetzungen des § 18 Abs. 6 Satz 1 SächsDSG vorliegen. Es handelt sich dabei jedoch nur um eine Einschränkung des Begründungsumfanges, nicht aber um eine vollständige Freistellung von der Begründungspflicht.

(8) Fraglich kann im Einzelnen auch sein, welche Schriftstücke unter den Begriff der „Akte“ fallen: Nicht der Akteneinsicht unterliegen persönliche Notizen des Bearbeiters und Vorentwürfe. Sie dienen in der Regel nicht dem Nachweis dienstlicher Vorgänge oder als Entscheidungsgrundlage. Entscheidungsvorschläge, Entwürfe zu Entscheidungen sowie Arbeiten zur unmittelbaren Vorbereitung einer Entscheidung unterliegen nur dann der Akteneinsicht, wenn sie zur Akte verfügt sind oder zu verfügen wären.

Eine analoge Anwendung des § 29 Abs. 1 Satz 2 VwVfG, der bis zum Abschluss des Verwaltungsverfahrens Entwürfe zu Entscheidungen sowie die Arbeiten zu ihrer

unmittelbaren Vorbereitung vom Recht auf Akteneinsicht durch den Beteiligten ausnimmt, auf das Auskunftsrecht nach § 18 SächsDSG kommt nicht in Betracht. Denn eine solche Analogie ist im öffentlichen Recht zumindest dann nicht statthaft, wenn sie zu Lasten von Grundrechten wirkte (vgl. Dreier/Schulze-Fielitz, Art. 20 GG, Rdnr. 95 ff.). Dies ergibt sich aus Art. 20 Abs. 3 GG, der den Vorbehalt des Gesetzes normiert.

10.2.19 Landesrechtliche Umsetzung des Brustkrebsfrüherkennungsprogramms (Mammographie-Screening)

Sehr intensiv beschäftigen müssen habe ich mich (von 2003 bis 2006) mit der Einführung des sog. Mammographie-Screenings, einer (freiwilligen) Krebsfrüherkennungs-Reihenuntersuchung, die allen Frauen vom 50. bis zum 70. Lebensjahr angeboten werden soll, mit dem Ziel der Früherkennung von Brustkrebs durch entsprechende Röntgenuntersuchungen und im Bedarfsfall anschließende zusätzliche andersartige Untersuchungen. (Träger öffentlicher Gewalt führen die Einladungen durch, die eigentliche Untersuchung leisten niedergelassene Ärzte.) Hierzu hat Ende 2003 der *Gemeinsame Bundesausschuss der Kassenärzte und Krankenkassen* (§ 91 SGB V) die auf der Grundlage der §§ 92, 94 SGB V beschlossenen *Krebsfrüherkennungsrichtlinien* entsprechend geändert (15. Dezember 2003, BAnz 2004 S. 2). Damals habe ich zunächst gegenüber dem BfDI Stellung genommen und rechtliche Einwände geltend gemacht.

Bei der anschließenden landesrechtlichen Umsetzung des Vorhabens bin ich vom SMS dankenswerterweise sehr frühzeitig beteiligt worden, habe jedoch immer wieder auf erhebliche datenschutzrechtliche Probleme hinweisen müssen. Dabei hat es sich vor allem um folgende Kritikpunkte gehandelt:

(1) Bereits die Tatsache, dass auf der Grundlage von Richtlinien nach dem SGB V - hier nach den vom *Gemeinsamen Bundesausschuss* (der Ärzte und Krankenkassen) beschlossenen Krebsfrüherkennungs-Richtlinien - (und entsprechend den im Einzelnen in diesen Richtlinien gegebenen Vorgaben!) eine medizinische Reihenuntersuchung für die gesamte weibliche Bevölkerung der betroffenen Altersgruppe (so jetzt § 2 Abs. 1 Satz 1 SächsFrühErDurchfG), d. h. *auch für die nicht gesetzlich krankenversicherten Frauen*, eingeführt werden sollte, hat von Anfang an einen grundlegenden rechtlichen Konstruktionsfehler dargestellt, der, weil es bei dem ganzen Programm ja vor allem um Verarbeitung personenbezogener Daten geht, entsprechende datenschutzrechtliche Folgen hat: Die die Verarbeitung personenbezogener Daten betreffenden Regelungen in solchen Richtlinien taugen schon von ihrem vor-

gegebenen Anwendungsbereich her nicht als (die erforderliche) Rechtsgrundlage für die Verarbeitung von Daten des betreffenden Personenkreises. Überdies gilt bekanntlich seit dem sog. Volkszählungsurteil des Bundesverfassungsgerichts (BVerfGE 65, 1 ff.), dass Träger öffentlicher Gewalt personenbezogene Daten nur insoweit erheben und auf jegliche andere Weise verarbeiten dürfen, als ihnen dies durch ein vom Parlament beschlossenes Gesetz oder aber durch eine Rechtsverordnung oder Satzung, die auf einem ausdrücklich hierzu ermächtigenden Parlamentsgesetz beruht, gestattet ist. Die Krebsfrüherkennungs-Richtlinien, wie alle Richtlinien nach §§ 92, 94 SGB V, haben im Verhältnis zum Versicherten aber gerade *keine solche Rechtsnormqualität* - entgegen der BSG-Entscheidung vom 20. März 1996 (Az. 6 RKa 62/94) die in ihrer Begründung Eingriffe in Grundrechte der Versicherten gar nicht berücksichtigt: Zumindest im Ergebnis wie hier Krauskopf-Knittel, Rdnr. 41 zu § 92 SGB V, unter Hinweis unter anderem auf Ossenbühl, NZS 1997, 497 (dies ist übrigens nunmehr wohl auch erklärte Auffassung des BMG, denn es hat in einem Schreiben vom 20. Februar 2006 (Az.: 212-44747-22) an den Vorsitzenden des Gemeinsamen Bundesausschusses ausgeführt, dass die nötigen Rechtsgrundlagen für Eingriffe in das Recht auf informationelle Selbstbestimmung nicht Richtlinien des Gemeinsamen Bundesausschusses entnommen werden können, sondern nur einer *gesetzlichen Ermächtigung*); grundlegende Kritik auch bei Kingreen, Verfassungsrechtliche Grenzen der Rechtssetzungsbefugnis des Gemeinsamen Bundesausschusses im Gesundheitsrecht, NJW 2006, 877 m. w. N.

Im Hinblick darauf bedarf es daher für die gesetzlich Krankenversicherten einer - sozialrechtlichen und damit *bundesrechtlichen - gesetzlichen* Grundlage für die Verarbeitung ihrer Daten zum Zweck der Einladung und zu sonstigen diesbezüglichen Informationsverarbeitungsvorgängen zwecks Teilnahme an den geplanten Brustkrebs-Reihenuntersuchungen. Unabhängig davon bedarf es im Hinblick auf nicht gesetzlich Krankenversicherte einer Datenverarbeitungserlaubnis, die aufgrund der Verteilung der Gesetzgebungszuständigkeit durch das Grundgesetz (kein Fall des Art. 74 Abs. 1 Nr. 19 GG) nur eine *landesrechtliche* sein kann.

(2) Im Hinblick auf den Demokratie- und den Rechtsstaats-Grundsatz (Art. 20 GG) begegnet es erheblichen Bedenken (siehe hierzu ebenfalls Kingreen a. a. O.), wenn in den in den Landtag eingebrachten Gesetzentwürfen, welche also zu den erforderlichen landesgesetzlichen Regelungen werden sollten, die Einzelheiten der Verarbeitungsvorgänge durch Verweisung auf die Krebsfrüherkennungs-Richtlinien (jetzt § 1 Abs. 2 SächsFrühErDurchfG) geregelt werden sollten - und damit durch eine dynamische Verweisung auf den fremden Willen eines anderen Normgebers, der wiederum für sich betrachtet nur äußerst mittelbar demokratisch legitimiert ist. Die ver-

fassungsrechtlichen Auffassungen dazu sind nicht einheitlich (vgl. Dreier in: Dreier, GG, Rdnr. 111 f. m. w. N.). Aber unabhängig davon dürfte die unter dem Gesichtspunkt von Normenklarheit und Demokratie zulässige Grenze für die dynamische Verweisung auf von Nicht-Parlamenten verabschiedete Regelungen allerdings hier insoweit überschritten sein, als die Richtlinie unter B Nr. 4 Buchst. d Abs. 8 ihrerseits wiederum wegen näherer Einzelheiten der Datenübermittlung [!] auf Anhang 9 der Anlage 9.2 des „Bundesmantelvertrages Ärzte“ sowie des entsprechenden Vertrages mit den Ersatzkassen mit Stand vom 12. Dezember 2003 verweist.

(3) Ein weiterer datenschutzrechtlicher Einwand galt und gilt gegenüber der Festlegung, dass die Aufgaben der „Zentralen Stelle“ im Sinne von Abschnitt B Nr. 4 der Krebsfrüherkennungsrichtlinien durch die *Kassenärztliche Vereinigung Sachsen* wahrgenommen werden soll (vgl. § 2 Abs. 2 SächsFrühErDurchfG). Die Übertragung von Aufgaben auf eine durch Bundesgesetz errichtete und mit Aufgaben und Zuständigkeiten ausgestattete Einrichtung, insbesondere auch, wenn es sich um eine Körperschaft des öffentlichen Rechts mit Zwangsmitgliedschaft handelt, durch den Landesgesetzgeber ist nur zulässig, soweit der Bundesgesetzgeber das durch eine entsprechende Öffnungsklausel wie in § 75 Abs. 1 Satz 2 SGB V zugelassen hat. Im Übrigen ist die den Gegenstand dieser Öffnungsklausel bildende notärztliche Versorgung im Rahmen des Rettungsdienstes noch eine dem Sicherstellungsauftrag der KVen nahe Aufgabe, während die hier zu beurteilende GKV-unabhängige Gesundheitsvorsorge auch nicht im Ansatz zu den bundesrechtlich festgelegten Aufgaben der KVen gehört. Offensichtlich geht auch der Bundesgesetzgeber davon aus, dass generell der Landesgesetzgeber einer durch Bundesrecht geschaffenen Stelle nur dann durch Landesrecht zusätzliche Aufgaben übertragen darf, wenn das durch Bundesgesetz ausdrücklich erlaubt ist.

(4) Hiermit in Zusammenhang habe ich auch Bedenken angemeldet, inwieweit diese Gesundheitsverwaltungsaufgabe, die der Freistaat Sachsen in Bezug auf die Brustkrebsreihenuntersuchungen zu übernehmen hat - hier: die Verarbeitung personenbezogener Daten zur Gewinnung von Personen zur Teilnahme am Früherkennungsprogramm - gegebenenfalls seitens des Freistaates im Wege der *Datenverarbeitung im Auftrag* (vgl. §§ 7 SächsDSG, 80 SGB X) überhaupt auf Dritte übertragen werden kann. Die Frage, ob eine Übermittlung (hier, durch die Meldebehörden) aus Datensparsamkeitsgründen unmittelbar an den Auftragsverarbeiter des Übermittlungsempfängers erfolgen darf, ist davon zu unterscheiden. Sie stellt sich aber nur dann, wenn die beauftragende Stelle auch tatsächlich unverändert ihre Verwaltungsfunktion wahrnimmt. Dabei ist zu beachten, dass ‚staatlicherseits’ ausschließlich das - weit verstandene - Einladungswesen durchgeführt wird, die eigentlichen Früher-

kennungsmaßnahmen jedoch nicht durch Träger öffentlicher Gewalt durchgeführt werden. Das heißt: Die Gesundheitsverwaltungs-Aufgabe, welche der Freistaat Sachsen durch ein entsprechendes Gesetz bezogen auf alle für das jeweilige Früherkennungsprogramm infrage kommenden auf seinem Gebiet gemeldeten Personen nach dem Gesetz übernimmt, besteht ausschließlich in der Verarbeitung personenbezogener Daten zur Gewinnung der betreffenden Frauen zur Teilnahme an Früherkennungsmaßnahmen und zur Übermittlung von Ort und Zeit der jeweils zur Verfügung stehenden Untersuchungshandlungen. Aus diesem Grunde ist die Möglichkeit, im Wege der Auftragsdatenverarbeitung Teile der durch ein solches Gesetz dem staatlichen Gesundheitswesen des Freistaates Sachsen übertragenen Aufgaben im Wege der Datenverarbeitung im Auftrag auf Dritte zu übertragen, von vornherein äußerst beschränkt.

(5) Im Hinblick auf die vom Gesetzgeber ausgesprochene Ermächtigung, dass das SMS durch Rechtsverordnung Gesundheitsvorsorgemaßnahmen anderer Art, d. h. genauer die damit verbundene Verarbeitung personenbezogener Daten, anordnen dürfe (jetzt § 4 SächsFrühErDurchfG), ist zu beachten, dass der Staat insgesamt von Verfassungs wegen (Art. 2 Abs. 1 GG) nur sehr begrenzt gesundheitliche Beeinträchtigungen seiner Bürger oder sonstiger Privater zum Gegenstand der Kontrolle zu Vorsorgezwecken machen darf. Die Grenzen ergeben sich dabei nicht nur aus der verfassungsrechtlich gebotenen Schwere der gesundheitlichen Beeinträchtigung, insbesondere in ihrer Wirkung auf Dritte, sondern auch im Hinblick auf Art und Periodizität der Maßnahmen, mit entsprechenden Folgen gerade auch für die zur Durchführung der Maßnahmen erforderliche Verarbeitung personenbezogener Daten. Es muss gewährleistet bleiben, dass die Betroffenen nicht ständig von der öffentlichen Gewalt - auf der Grundlage von Meldedaten - auf Gesundheitsvorsorgemaßnahmen angesprochen werden, und auch, dass zwischen zwei Ansprachen in derselben Sache, wie z. B. Brustkrebs, zeitliche Mindestabstände liegen.

In diesem Zusammenhang ist auch bemerkenswert, dass man es nicht überall wie Sachsen für notwendig gehalten hat, dass die Meldebehörden *vierteljährlich* (ursprünglich sollte es sogar monatlich geschehen) die Daten aller Frauen im Alter zwischen 50 und 70 Jahren an die „Zentrale Stelle“ übermitteln müssen, während der Abstand der Einladungen zur Teilnahme an der Untersuchung zwei Jahre beträgt (Richtlinie Abschn. B Nr. 4 Abs. 3, Buchst. a, Abs. 1).

(6) Nachdem ich schon zu einigen Vor-Entwürfen Stellung genommen hatte, habe ich auch während des eigentlichen Gesetzgebungsverfahrens (Gesetzentwurf der Staatsregierung LT-DS: 4/4557) den zuständigen Fachausschüssen im Rahmen ihrer inter-

nen Befassung zum Gesetzentwurf mündlich wie schriftlich ausgiebig beratend zur Verfügung gestanden und mich, auch schriftlich, zu den Entwürfen von Fraktionen geäußert. Das „Gesetz über die Durchführung eines Mammographie-Screenings und anderer Früherkennungsmaßnahmen im Freistaat Sachsen“ - kurz: *Sächsisches Früherkennungsdurchführungsgesetz* (SächsFrühErDurchfG) - ist dann schließlich am 10. Mai 2006 (GVBl. S. 150) mit einigen deutlichen Verbesserungen verabschiedet worden.

(7) Die Haupt-Ursache dieser rechtlichen Probleme hat der Bund zu verantworten: Er setzt sich, wie auch in anderem Zusammenhang, wenn ein gewisser gesellschaftlicher Druck besteht (hier: Die Untersuchungen sind durch das Programm *ohne Weiteres kostenlos* geworden - natürlich sind sie vorher schon auf Eigeninitiative möglich gewesen und haben die Ärzte sie auch, wenn Anlass bestand, „verschrieben“), über die grundgesetzliche Zuständigkeitsverteilung einfach hinweg, teils mit (bloßen) Entschließungen des EU-Parlaments im Rücken, und überlässt den Ländern die Lösung vertrackter Umsetzungsprobleme.

Die anderen Bundesländer haben es im Großen und Ganzen nicht viel besser gemacht als Sachsen. Ein Kollege in einem großen Bundesland hat dieselben grundlegenden rechtlichen Einwände vorgebracht wie ich und ist nicht durchgedrungen; sein Fazit: „Meine größte Niederlage“.

(8) Das Thema beschäftigt die Datenschützer weiter: Nunmehr machen von den mit der Steuerung des Ganzen beschäftigte Fachleute darauf aufmerksam, dass die mit der Reihenuntersuchung verbundene Strahlenbelastung das ganze Unternehmen medizinisch nur gerechtfertigt sein lässt, wenn zusätzlich eine strikte Erfolgs- und Qualitätskontrolle *des gesamten Systems*, und zwar unter Abgleich mit dem epidemiologischen Krebsregister, stattfindet - mit der Folge, dass dazu die Verarbeitung personenbezogener Daten gegenüber dem in der Früherkennungsrichtlinie bisher Vorgesehenen nicht unbeträchtlich erweitert werden müsste. Nachdem man den Betreibern des Systems in puncto *Vorbehalt des Gesetzes* schon so weit entgegengekommen ist, verwundert es nicht sehr, dass dort durchaus die Erwartung vorhanden ist, man könne diese Erweiterung sogar ohne Veränderung der Richtlinie vornehmen. (Im Hintergrund steht wohl eine lebhafte wissenschaftliche Diskussion über den praktischen Sinn solcher Reihenuntersuchungen, von der man im Wissenschaftsteil mancher Zeitungen immer wieder einmal lesen kann.)

10.3 Lebensmittelüberwachung und Veterinärwesen

In diesem Jahr nicht belegt.

10.4 Rehabilitierungsgesetze

In diesem Jahr nicht belegt.

11 Landwirtschaft, Ernährung und Forsten

11.1 Ein überflüssiges Verlangen nach Einwilligung in eine Verarbeitung personenbezogener Daten

Im Zusammenhang mit auf Antrag erfolgenden Leistungsgewährungen verlangen Behörden nicht selten von den Antragstellern die Erklärung der Einwilligung in die Verarbeitung bestimmter sie betreffender Daten und erklären die Erteilung dieser Einwilligung zur Voraussetzung der Leistungsgewährung, obwohl das Gesetz selbst schon die Behörde zu der betreffenden Verarbeitungshandlung befugt.

In einem derartigen Fall hatte es den Inhaber eines landwirtschaftlichen Betriebes sehr befremdet, dass er im „Antrag auf Direktzahlungen und Agrarförderung 2005“ gemäß dem Vordruck „Sammelantrag - Freistaat Sachsen“ unter „Erklärungen zum Datenschutz“ sein Einverständnis damit erklären sollte, dass seine personenbezogenen bzw. betriebsbezogenen Daten *zur Feststellung der Versicherungspflicht, der Anspruchsberechtigung und zum Zwecke der Beitragserhebung an die Träger der landwirtschaftlichen Sozialversicherung übermittelt werden dürften und dass im Gegenzug die landwirtschaftliche Sozialversicherung der Landwirtschaftsbehörde derartige Daten übermitteln dürfe*. Das Befremden war so groß gewesen, dass der Betriebsinhaber den betreffenden Passus durchgestrichen hatte - aber er hatte dann erleben müssen, dass die Behörde seinen Antrag rundweg abgelehnt hat.

Die Datenschutzbeauftragte des von mir auf die Eingabe des Betriebsinhabers hin eingeschalteten SMUL hat umgehend gegenüber der nachgeordneten Behörde klargestellt, dass die Übermittlung an die Träger der landwirtschaftlichen Sozialversicherung durch § 197 Abs. 4 Satz 4 SGB VII erlaubt sei, es deswegen einer Einwilligung des Betroffenen nicht bedürfe und der Satz im Antragsvordruck nur Hinweischarakter haben könne, so dass dessen Streichung deswegen keine Antragsablehnung begründen könne. Was die zusätzliche Einwilligung in eine Datenerhebung der Landwirtschaftsbehörde bei den Trägern der landwirtschaftlichen Sozialversicherung und ergänzend die Einwilligung in die entsprechende Übermittlung seitens der Sozialversicherungsträger an die Landwirtschaftsbehörde betrifft, also den zweiten Teil des zitierten Textes, hat das Staatsministerium klargestellt, dass die Ämter für Landwirtschaft, als Bewilligungsstellen, zwar insoweit zur Prüfung der Zuwendungsvoraussetzungen (nach einer einschlägigen Richtlinie des SMUL für die Gewährung von Ausgleichszulagen in benachteiligten Gebieten) und zur Berechnung des Umfangs und der Höhe der Zuwendung nach einer Richtlinie zur Förderung des Vorruhestandes in der Landwirtschaft Daten benötigten, dass diese jedoch beim Betroffenen selbst eingeholt werden könnten, ohne dass dies zu einem unzumutbaren

Aufwand für die Bewilligungsbehörde führte, weswegen auch die Streichung dieses Passus keinen Ablehnungsgrund darstelle.

Dem betreffenden landwirtschaftlichen Betrieb war damit schnell geholfen. Das Problem besteht aber in kaum absehbarem Ausmaß: Solche Einwilligungsklauseln werden aus Unsicherheit in Vordrucke aufgenommen; es handelt sich um Fälle dessen, was Juristen „Angstklauseln“ nennen - eine zwecks Arbeitsersparnis unter Privaten probate „Technik“ zur Vermeidung juristischen Klärungs-Aufwandes. Nur: Behörden ist solch ein Vorgehen nicht erlaubt, sie sind an Gesetz und Recht gebunden und dürfen daher ihr Aufgaben erfüllendes Daten verarbeitendes Handeln nicht, auch nicht vorsorglich, auf Einwilligung der Betroffenen stützen; vgl. dazu auch 10.2.15 unter (4.3).

11.2 Überwachung, Förderung und Beratung durch einen in Nebentätigkeit als Wettbewerber der Betroffenen tätigen Bediensteten

Eine Zeitungsmeldung hatte bestätigt, was in Fachkreisen schon gemunkelt worden war: In einem durch strenge, insbesondere sehr ins Einzelne gehende Meldepflichten gekennzeichneten, sehr begrenzten Bereich landwirtschaftlicher Sonderkulturen (vgl. auch 3/11.2 und 4/11.1) hatte der Fachberater, der zugleich alle Meldungen wie auch alle Förderanträge aller Betriebe bearbeitete, sich an einem Betrieb nicht unbeträchtlicher Größe als einer von drei Gesellschaftern beteiligt, und folgerichtig hatte er auch einen Antrag auf Mitgliedschaft in dem betreffenden Anbau-Verband gestellt.

Ungeachtet der von ihnen nicht bestrittenen fachlichen Tüchtigkeit des Fachberaters waren verschiedene Landwirte, auch Inhaber größerer, namhafter Betriebe, sowie der Verbandsvorsitzende empört: Mit dem Wissen aus den Meldungen, aber auch den Förderanträgen, würde der künftige Mitbewerber über Wissen über seine Konkurrenten verfügen, das sich, so sind mir die Verhältnisse auf diesem speziellen, engen Markt überzeugend geschildert worden, in gutes Geld ummünzen lassen würde. Der zuständige Referent im SMUL hatte, so hieß es mir gegenüber, kein Problem zu sehen erklärt, weswegen Betroffene sich, in Erinnerung an den im dritten und vierten Tätigkeitsbericht geschilderten Fall, an mich gewandt haben. Von mir auf das Problem angesprochen, hat der betreffende Amtsleiter zunächst als Lösung vorgeschlagen, dem betreffenden Bediensteten die Bearbeitung der Meldungen und der Förderanträge zu entziehen, ihm aber die Beratung zu belassen. Ein Petent zu diesem Vorschlag: „Dann werden bestimmte Fragen eben nicht mehr, zwecks Beratung, gestellt

werden, bei Beratung in bestimmter Hinsicht geht es eben doch um Betriebsgeheimnisse“. Allgemein ausgedrückt: Wer sich beraten lassen will, muss im starken Maße auch personenbezogene Daten dazu offenbaren.

Daraus folgte zwingend, dass der Freistaat Sachsen seine Beratungsaufgabe zur Förderung der betreffenden Sonderkulturen in Sachsen nicht mehr in dem bisherigen Maße, sondern nur noch erheblich vermindert würde erfüllen können, falls er den betreffenden Bediensteten unverändert für die einschlägige Beratung zuständig sein ließe.

Es galt, hier eine personell-organisatorische Maßnahme zu treffen, die erforderlich war, um eine rechtmäßige Datenverarbeitung zu gewährleisten (vgl. § 9 Abs. 1 Satz 1 SächsDSG). Es war erforderlich, dass der böse Schein vermieden würde, dass die sächsische Verwaltung jemanden mit der Verarbeitung personenbezogener Daten - hier Betriebsdaten - betraut, der notwendigerweise ein privates Interesse an der Nutzung dieser Daten in einem mehr oder weniger großen Umfang, hat.

Die Datenschutzbeauftragte des Staatsministeriums hat die Problematik sofort erkannt. Das Staatsministerium hat umgehend - der nächste größere Meldetermin stand für die Betriebe nahe bevor - mit einer Umsetzung des betreffenden Beschäftigten reagiert und damit, dieser Ausdruck sei hier einmal erlaubt, die Kuh vom Eis geholt.

Ob nicht auch die andere, für den Freistaat personalverwaltungstechnisch einfachere Lösung nebentätigkeitsrechtlich möglich gewesen wäre, ist von mir nicht zu beurteilen. Aber aller Wahrscheinlichkeit nach war die getroffene Entscheidung die sicherere angesichts des nun einmal in Erscheinung getretenen Bestrebens des betreffenden Bediensteten, sich privat gerade in dem von ihm verwalteten Anbau-Bereich zu betätigen.

12 Umwelt und Landesentwicklung

12.1 Ein Abwasserzweckverband und sein Beratungsunternehmen - mangelnde Reaktion auf Datenmissbrauch durch den Auftragsdatenverarbeiter

Einen Abwasserzweckverband habe ich wegen der Verletzung seiner Pflichten als Auftraggeber beanstanden müssen. Gemäß § 7 SächsDSG kann eine öffentliche Stelle (Auftraggeber) eine andere (Auftragnehmer) mit der Verarbeitung personenbezogener Daten beauftragen. Dabei hat der Auftraggeber den Auftragnehmer unter besonderer Berücksichtigung der Eignung der vom Auftragnehmer getroffenen personellen, technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. Der Auftrag für die Datenverarbeitung muss schriftlich erteilt werden und den Gegenstand und Umfang der Datenverarbeitung sowie die notwendigen zusätzlichen personellen, technischen und organisatorischen Maßnahmen festlegen. Der Auftraggeber muss sich von der Einhaltung dieser Festlegungen beim Auftragnehmer überzeugen, er hat erforderliche Weisungen zu erteilen, denen gemäß die Datenverarbeitung durch den Auftragnehmer zu erfolgen hat. § 7 Abs. 2 Satz 5 SächsDSG bestimmt ausdrücklich, dass die Datenverarbeitung durch den Auftragnehmer nur im Rahmen des Auftrages und der Weisungen des Auftraggebers zulässig ist.

Der Beanstandung lag folgender Sachverhalt zugrunde:

Der Abwasserzweckverband beauftragte eine Firma für Umwelttechnik (nachfolgend „Umwelt-GmbH“ genannt) mit der Erarbeitung eines Indirekteinleiterkatasters. In dieses sollten die Betriebe aufgenommen werden, die Abwasser indirekt, also nach einer Vorbehandlung in einer eigenen Anlage, einleiten; darunter fallen insbesondere Großküchen, namentlich auch Gastwirtschaften. Auf der Grundlage des Katasters sollten später Abwassereinleitungsverträge abgeschlossen werden. Für die Erstellung des Katasters war eine Datenerhebung bei den Betrieben erforderlich, für die die Umwelt-GmbH vom Abwasserzweckverband eine „Vollmacht“ erhielt. Diese enthält folgende Passage: „Die Mitarbeiter der [Umwelt-]GmbH werden dahingehend belehrt, dass das erfragte und bearbeitete Datenmaterial den Bestimmungen des Datenschutzes unterliegt und eine unbefugte Nutzung oder Bekanntgabe desselben nicht gestattet ist.“ In der Folge überprüfte die Umwelt-GmbH die Abwasseranlagen der Betriebe und führte Abwasseruntersuchungen durch. Auf der Grundlage der Untersuchungsergebnisse entwarf die Umwelt-GmbH jeweils einen (öffentlich-rechtlichen) Abwassereinleitungsvertrag, der den Betrieb gegenüber dem Abwasserzweckverband unter anderem verpflichtete, turnusmäßige Untersuchungen seines

Abwassers durch einen Fachmann zu veranlassen. Diesen vorbereiteten Entwurf des Abwassereinleitungsvertrages hat der Abwasserzweckverband sodann den einzelnen Betrieben als Vertragsvorschlag unterbreitet.

Ein solcher Vertragsentwurf wurde auch einem Pflegeheim - als GmbH betrieben und nachfolgend als „Pflege-GmbH“ bezeichnet - unterbreitet. In diesem waren vierteljährliche Abwasserkontrollen vorgesehen, die die Pflege-GmbH in Auftrag geben und deren Ergebnis dem Abwasserzweckverband mitgeteilt werden sollte. Diesen Vertrag hat die Pflege-GmbH jedoch nicht abgeschlossen. In direktem zeitlichem Zusammenhang mit der Übersendung des Vertrages durch den Abwasserzweckverband bekam die Pflege-GmbH, adressiert an den Geschäftsführer unter Namensnennung, ein Schreiben der Umwelt-GmbH, in dem diese mitteilte, dass sie in Erfahrung gebracht habe, dass der Pflege-GmbH der Text für einen Einleitungsvertrag übersandt worden sei. Sie bot an, die durchzuführenden regelmäßigen Abwasserkontrollen zu übernehmen. Obwohl die Pflege-GmbH auf dieses Schreiben nicht reagiert hat, wurde wenig später ein konkretes Angebot unterbreitet (vierteljährliche Probeentnahme und Untersuchung für 105 €).

Daraufhin hat sich der Geschäftsführer der Pflege-GmbH mit der Bitte an mich gewandt, zu prüfen, ob die Verwendung der Daten aus dem Verwaltungsverfahren zu wirtschaftlichen Zwecken der Umwelt-GmbH datenschutzrechtlich zulässig sei.

Ich habe den Abwasserzweckverband an Ort und Stelle kontrolliert und sein „Auftragsverhältnis“ mit der Umwelt-GmbH durchleuchtet. Dabei habe ich festgestellt, dass die Vereinbarung mit der Umwelt-GmbH kaum Regelungen zum Umgang mit personenbezogenen Daten enthielt und der Abwasserzweckverband diesbezüglich auch keine Weisungen erteilt hat. Allein aus der oben zitierten „Vollmacht“ war ersichtlich, dass wohl mündlich der Umfang der Datenverarbeitung und das Verbot einer gewerblichen Nutzung mehr oder weniger genau geklärt war. Danach durfte die Umwelt-GmbH die erhobenen Daten nicht für eigene gewerbliche Zwecke nutzen. Bis zu diesem Punkt hatte ich keinen Grund, eine Beanstandung auszusprechen. Zwar waren die schriftlichen Vereinbarungen über die Datenerhebung sehr knapp, aber doch zumindest ansatzweise vorhanden. Auch war die Zusammenarbeit mit der Umwelt-GmbH bereits beendet, und der Abwasserzweckverband hatte, auf meine Intervention hin, die Umwelt-GmbH aufgefordert, die dort im Auftrag verarbeiteten Daten zu löschen. Dies lehnte die Umwelt-GmbH mit der Begründung ab, dass diese Daten wegen eventueller Gewährleistungsansprüche gespeichert werden müssten. Ich habe den Abwasserzweckverband deshalb aufgefordert, mit der Umwelt-GmbH eine vertragsergänzende Vereinbarung abzuschließen, die den Gegenstand und Umfang

der Datenspeicherung nach Abschluss der Datenverarbeitung im Auftrag zum Gegenstand haben sollte. Danach sollte der Auftragnehmer dem Auftraggeber Auskunft über alle bei ihm gespeicherten Daten geben, die er im Rahmen des Auftragsverhältnisses übermittelt bekommen oder sonst erhoben bzw. verarbeitet hat, einschließlich Auskunft darüber, welche Daten er unbefugt im eigenen Interesse genutzt hat. Ferner sollte die Umwelt-GmbH detailliert darlegen, welche konkreten personenbezogenen Daten sie für welche konkreten Gewährleistungsansprüche wie lange benötige. Die nicht mehr wegen der Gewährleistung benötigten Daten sollten gelöscht, bzw. an den Abwasserzweckverband herausgegeben werden; hinsichtlich der anderen Daten sollten Löschungs- bzw. Herausgabefristen vereinbart werden. Ferner sollte die Umwelt-GmbH erklären, dass sie die im Auftrag verarbeiteten Daten zukünftig nicht für private Interessen verwenden und den Auftraggeber über jegliche Verarbeitung dieser personenbezogenen Daten unterrichten werde.

Obwohl die Umwelt-GmbH gegenüber dem Abwasserzweckverband bereits ihre Bereitschaft angekündigt hatte, eine Erklärung dahingehend abzugeben, dass sie die ihr im Rahmen des Auftragsverhältnisses zugänglich gemachten personenbezogenen Daten nicht im eigenen Interesse weiterverwenden werde, lehnte der Abwasserzweckverband jegliche weiteren Handlungen zur Sicherung der datenschutzgerechten Verarbeitung gegenüber der Umwelt-GmbH ab. Er begründete dies damit, dass durch die Umwelt-GmbH überhaupt keine personenbezogenen Daten, sondern lediglich Daten von „Firmen“ verarbeitet worden seien, die jedoch nicht unter das Sächsische Datenschutzgesetz fielen. Dieser Einwand wurde auch in der Anhörung anlässlich meiner Beanstandung vertieft, mit der Folge, dass es die Umwelt-GmbH entgegen vorherigen Ankündigungen ablehnte, irgendeine Erklärung hinsichtlich der weiteren Nutzung der Daten abzugeben. Die Weigerung des Abwasserzweckverbandes, als Auftraggeber für den datenschutzgerechten Umgang der personenbezogenen Daten Sorge zu tragen, habe ich beanstandet. Zur Problematik des Personenbezugs in dem konkreten Beschwerdefall habe ich wie folgt Stellung genommen: „Es handelt sich bei dem beanstandeten Sachverhalt auch um eine Verarbeitung personenbezogener Daten, also gemäß § 3 SächsDSG von Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener). Grundsätzlich sind darin Angaben über juristische Personen oder Personenmehrheiten unmittelbar nicht erfasst. Etwas anderes gilt jedoch, wenn zu den Angaben über ein Unternehmen auch die Namen und Funktionen der Vorstandsmitglieder, Prokuristen, Betriebsräte oder etwa des Geschäftsführers gespeichert werden. Dabei handelt es sich um Daten eines Unternehmensangehörigen, die insbesondere seine Zugehörigkeit zum Unternehmen und seine Funktion betreffen. Dies sind schon unmittelbar personenbezogene Daten zum Unternehmen des Angehörigen (vgl.

Simitis, BDSG, § 3 Rdnr. 41 ff.) - hier in der Person des Geschäftsführers. Die personenbezogenen Daten des Geschäftsführers der Pflege-GmbH waren somit ebenso unmittelbar Gegenstand der Datenverarbeitung im Auftrag wie die Daten, die sich unmittelbar ausschließlich auf die juristische Person als solche bezogen."

Die datenschutzrechtliche Kontrolle hat, nachdem Abwasserzweckverband und Umwelt-GmbH auch noch anwaltliche Stellungnahmen gegen mich aufgeboten hatten, dann folgenden Verlauf genommen: Der Verbandsvorsitzende des Abwasserzweckverbandes hat mir mitgeteilt, dass er die Beanstandung zur Kenntnis nehme, sich der Auffassung des Abwasserzweckverbandes anschließe, der Vertrag mit der Umwelt-GmbH beendet sei und bei zukünftigen Aufträgen ähnlicher Art meine Hinweise Beachtung finden würden. Eine Beanstandung, die mit solch lapidarer Begründung zu den Akten gelegt wird oder (von mir) werden muss, offenbart wieder einmal (siehe dazu bereits 11/10.2.8) die Schwäche des Sächsischen Datenschutzgesetzes wie der Datenschutzgesetze insgesamt: Der Datenschutzbeauftragte darf zwar eine Beanstandung aussprechen, kann die darin aufgestellten Forderungen nach einem datenschutzgerechten Umgang mit personenbezogenen Daten, also die in § 29 Abs. 1 Satz 1 SächsDSG genannte „Behebung der Verstöße", jedoch nicht durchsetzen. So bleibt mir zum einen der noch nicht ganz abgeschlossene Versuch, die Aufsichtsbehörden, und zwar zunächst den Landkreis und, „darüber", das Regierungspräsidium zu einer entsprechenden Einwirkung auf den Zweckverband zu bewegen. Landkreis wie Regierungspräsidium haben in ihren Antworten die nötige Sensibilität dafür, dass der Betroffene ein Recht darauf hat, dass für Träger öffentlicher Gewalt tätige Auftragsdatenverarbeiter kein Schindluder mit den ihnen anvertrauten personenbezogenen Daten treiben, vermissen lassen. Wegen seiner bisherigen Bemühungen, auf der Grundlage unbehelflicher rechtlicher Erwägungen zu dem Ergebnis zu kommen, dass rechtsaufsichtliche Maßnahmen nicht veranlasst seien, habe ich auch hinsichtlich des Regierungspräsidiums eigentlich keine Hoffnungen mehr. Aber es gibt ja noch das SMI. Ergänzend bleibt mir zum anderen als Versuch, entsprechende Einwirkungen auf den Zweckverband auszulösen, nur die Veröffentlichung des Falles im Tätigkeitsbericht, wie hiermit geschehen.

12.2 Vorsicht bei Einheits-Vordrucken für verschiedenartige Anträge

Erstaunt war ein Petent - ein Anwohner einer sächsischen Kleinstadt - angesichts der Aufforderung der Stadtwerke, einen formgebundenen „Antrag auf Abwasserentsorgung" auszufüllen. In diesem Vordruck sollte er unter anderem angeben, wie viele Personen das Wohngebäude bewohnen und über wie viele Waschbecken und Bade-

wannen etc. das Haus verfüge. Erstaunt war der Petent deshalb, weil er keinerlei Veränderungen an der Abwassereinleitung vorgenommen hatte und sich nicht erklären konnte, wozu die Stadt nunmehr solch detaillierte Angaben benötigte.

Erstere Frage klärte sich relativ schnell: Der Eigentümer hatte Mitte der 90er Jahre lediglich einen formlosen Antrag auf Anschluss an den Abwasserkanal gestellt, aus dem nicht hervorging, ob auch Niederschlagswasser eingeleitet wird. Ihm war sodann die Einleitung von Niederschlags- und Schmutzwasser genehmigt worden. Wegen der Veränderungen des Kanalsystems im Jahre 2005 - so teilten die Stadtwerke nun mit - sei eine solche Genehmigung nicht mehr zulässig, so dass eben eine an die neuen Bedingungen angepasste Einleitgenehmigung erforderlich geworden sei. Aus diesem Grund sei das in vielen Fällen verwandte Antragsformular versandt worden. Diese Verfahrensweise war datenschutzrechtlich einwandfrei. Bedauerlich war nur, dass die Stadt erst mir erklärt hat, warum sie sich an den Petenten gewandt hatte, und dies nicht schon in verständlicher Weise dem Petenten bei der Versendung der Antragsformulare selbst erläutert hatte. (Ich muss leider sehr häufig feststellen, dass Behörden ihr Handeln nicht erklären. Dies führt in der Regel zu Streit und Missverständnissen, die doch durch ein paar wenige erklärende Worte vermieden werden könnten.)

Datenschutzrechtlich nicht zulässig war jedoch die pauschale Versendung des Antragsvordruckes. Es handelte sich dabei um ein Formular für mehrere verschiedenartige Anträge. Es galt sowohl für den „Neuanschluss“ wie auch für die „Änderung der Abwasserentsorgung“ und auch für einen „Direktanschluss“. Je nach Antragsart hätten unterschiedliche Angaben gemacht werden müssen. Erkennbar war aber nicht, welche Angaben für welchen Antrag erforderlich waren. Dies hatte zur Folge, dass der Petent - und sicherlich jeder andere Benutzer des Vordruckes auch - annehmen musste, er müsse alle in dem Formular vorgesehenen Angaben machen, etwa auch zur Anzahl der Duschen und Waschbecken.

Dass diese Angaben für den Anschluss eines Einfamilienhauses nicht notwendig waren, sondern allenfalls bei Anschluss eines Hotels oder Gewerbebetriebes, mussten auch die Stadtwerke einräumen. Gemäß § 126 Abs. 2 SächsWG dürfen Körperschaften des öffentlichen Rechts und andere Träger der Abwasserbeseitigungspflicht zur Erfüllung ihrer Aufgaben von Betroffenen die *notwendigen* personen- bzw. betriebsbezogenen Daten erheben. Fordern die Stadtwerke jedoch das Ausfüllen des gesamten Fragebogens oder lassen sie den Betroffenen über den Umfang der Pflicht zum Ausfüllen des Fragebogens im Unklaren, handeln sie rechtswidrig.

Ich habe vorgeschlagen, dem allgemeinen Antragsbogen Ausfüllhinweise beizufügen, die den Antragstellern genauere Auskunft darüber geben, welche Daten in welchem Fall anzugeben sind. In Vorbereitung dazu habe ich empfohlen, zu klären, welche konkreten Angaben für welchen der verschiedenen Anträge („Neuanschluss“, „Änderung der Abwasserentsorgung“ oder „Direktanschluss“) und für welchen Anschlussnehmer (Gewerbe, Wohngebäude, Sonstige) für die Durchführung der Abwasserentsorgung benötigt werden.

Die Stadtwerke haben diesen Vorschlag dahingehend umgesetzt, dass künftig alle Antragsformulare mit einem Anschreiben versandt werden, in dem konkrete Ausfüllhinweise enthalten sein werden. Nach Verbrauch der alten Vordrucke werden die neuen Formulare konkretere Ausfüllhinweise erhalten. Dem Petenten wurde infolgedessen konkret dargelegt, welche Angaben von ihm benötigt wurden. An der Neufassung künftiger Antragsvordrucke werde ich beteiligt.

13 Wissenschaft und Kunst

13.1 Nutzung von Studentendaten für einen „Alumni-Newsletter“?

Der Fachbereich „Wirtschaft“ einer Hochschule wollte für die landeseigene Wirtschaftsförderungsgesellschaft Wirtschaftsförderung Sachsen GmbH (WfS) die Konzeption für einen Newsletter-Versand entwickeln, mittels dessen die Vielzahl von Absolventen, die nach dem Examen nicht nur Sachsens Hochschulen, sondern auch den Wirtschaftsraum Sachsen verlassen, später über aktuelle Geschehnisse in Sachsen unterrichtet werden sollten, wovon man sich insbesondere auch Entscheidungen der Betreffenden zugunsten von Auftragsvergaben nach Sachsen, aber auch zugunsten von Urlaubsaufenthalten im Freistaat erhoffte.

Wegen der Frage, ob die Wirtschaftsförderungsgesellschaft erlaubterweise für solche regelmäßigen Zusendungen an die E-Mail-Anschriften von Absolventen sächsischer Hochschulen die dafür nötigen Daten von den Hochschulen bekommen dürfe, insbesondere Namen und E-Mail-Anschrift, nach Möglichkeit auch die Fachrichtung des abgeschlossenen Studiums, hat sich die Hochschule an mich gewandt. Genauer gesagt war geplant, die von den Studenten gegenüber der Hochschulverwaltung freiwillig und verbunden mit einer Einwilligung in die Verwendung der Anschrift durch die Hochschulverwaltung angegebenen E-Mail-Anschriften einmalig für eine Kontaktaufnahme zu den Absolventen zu nutzen und im Falle der Bekundung von Interesse die Betreffenden in den Verteiler aufzunehmen, anderenfalls seine Daten zu löschen.

Dazu habe ich in datenschutzrechtlicher Hinsicht wie folgt Stellung genommen:

(1) Die Hochschulverwaltung hat die E-Mail-Anschriften rechtmäßig erhoben und gespeichert:

Gemäß § 1 Nr. 6 SächsStudDatVO i. V. m. § 106 Abs. 1 Satz 3 i. V. m. Satz 1 SächsHG darf die Behörde die *gegenwärtigen Anschriften* des Studienbewerbers und im Falle der Immatrikulation gemäß § 2 der VO auch des Studenten erheben und speichern.

Für den Zeitpunkt nach der Exmatrikulation sieht die SächsStudDatVO in § 12 Nr. 3 nur die Speicherung der *letzten Wohnanschrift* vor. Die Verarbeitung des Datums „E-Mail-Anschrift“ hält sich auch im letzteren Fall noch in den Grenzen des durch die Ausdrücke „Anschriften“ bzw. „Wohnanschrift“ bezeichneten Begriffes. Es ist dem Gesetz bzw. der Verordnung zu entnehmen, dass die Hochschulverwaltung

Daten erheben und speichern darf, welche die schriftliche Telekommunikation mit dem Betreffenden ermöglichen. Kommt, wie es der Fall ist, das Einverständnis des Betroffenen, als implizite Einwilligung durch schriftliche Angabe der E-Mail-Anschrift, hinzu, ist das Grundrecht auf informationelle Selbstbestimmung nicht verletzt und hält sich zugleich die Behörde im Rahmen der ihr nach geltendem Recht zugewiesenen Aufgaben.

(2) Das von den Studenten mit der freiwilligen Hingabe des Datums „E-Mail-Anschrift“ erklärte Einverständnis (Einwilligung) erstreckt sich jedoch nicht darauf, dass die Hochschule die Anschrift für elektronische Post an Dritte weitergibt.

Eine Übermittlung der Daten an die WfS wäre auch nicht durch die für derartige Übermittlungen maßgebliche Vorschrift des § 106 Abs. 2 SächsHG erlaubt.

Als Rechtsvorschrift, die gemäß § 106 Abs. 2 Satz 1 Nr. 1 SächsHG eine solche Erlaubnis enthalten könnte, kommt nicht die einschlägige Übermittlungserlaubnis des allgemeinen Datenschutzrechtes, also § 14 SächsDSG, in Betracht. Das folgt eindeutig daraus, dass § 106 Abs. 2 Satz 1 SächsHG vor allem in Nr. 3 bis 6 eine Regelung enthält, die die Übermittlung gerade nur für einen Teil derjenigen Fälle erlaubt, in denen sie nach § 14 Abs. 1 SächsDSG zulässig ist. Anders ausgedrückt: § 106 Abs. 2 Satz 1 SächsHG knüpft die Übermittlungserlaubnis nur an einen Teil der alternativen Übermittlungstatbestände des § 14 SächsDSG. Dasselbe gilt übrigens für die Nutzungserlaubnis nach § 106 Abs. 2 Satz 2 SächsHG: Auch sie weicht erheblich von der Regelung des § 13 Abs. 2 und 3 SächsDSG ab, ist also als abschließend zu verstehen.

(3) Dieses Ergebnis ließe sich auch nicht dadurch vermeiden, dass die Hochschule selbst die Versendung des elektronischen Informationsbriefes des Freistaates übernähme. Denn in § 106 Abs. 1 Satz 1 SächsHG ist die Pflege des Kontaktes *der Hochschule* mit ihren eigenen Absolventen gemeint, nicht die *Kontaktpflege* des Freistaates. Dies ergibt sich aus dem Kontext, in dem in § 106 Abs. 1 Satz 1 SächsHG die Kontaktpflege mit ehemaligen *Hochschulmitgliedern* steht, er ist ein rein hochschulbezogener. Nur in Satz 3 der Vorschrift wird dieser auf die einzelne Hochschule bezogene Zusammenhang auf Bedürfnisse des Landes (Freistaates) erweitert. Ähnliches gilt für § 106 Abs. 2 Satz 2 SächsHG, da die dort erwähnten Aufsichtsrechte im Wesentlichen solche des Staates sind.

Daraus folgt: Alles, was nicht für die Zwecke der betreffenden einzelnen Hochschule als solcher geschieht, stellt eine Zweckänderung gemäß § 106 Abs. 2 SächsHG dar, und dessen Voraussetzungen für eine - zweckändernde - Nutzung sind nicht erfüllt.

(4) Für die Übermittlung des zusätzlichen Datums „Studiengang“ gilt das Vorstehende entsprechend. Eine Befugnis der Hochschulverwaltung, dieses Datum an die Wirtschaftsförderungsgesellschaft zu übermitteln, ist nicht zu erkennen.

Datenschutzrechtlich unbedenklich wäre es - darauf habe ich hingewiesen -, wenn die Hochschulverwaltung in einem Schreiben, das sie aus Gründen der Erfüllung von Aufgaben der Hochschulverwaltung an Absolventen richtet, etwa ein Faltblatt mit näheren Angaben über den geplanten elektronischen Informationsbrief beifügte. Eine besondere Datennutzung fände in diesem Fall nicht statt.

Selbstverständlich habe ich der Hochschule angeboten, das SMWK einzubeziehen, um dessen Rechtsauffassung in Erfahrung zu bringen, schließlich ging es ja um die Auslegung des Sächsischen Hochschulgesetzes. Die Hochschule hat sich jedoch in der Angelegenheit dann nicht mehr gemeldet. Sollte ein solches Vorhaben - nicht nur von dieser Hochschule, sondern weiter verbreitet - weiterverfolgt werden, so ist dies nur mit einer Änderung der entsprechenden Regelung im Sächsischen Hochschulgesetz möglich.

13.2 Evaluierung von Vorlesungen an einer Berufsakademie

An einer staatlichen Berufsakademie wurde, wie sich dann aufgrund einer Eingabe herausgestellt hat, ein Jahr lang eine Bewertung der Lehrveranstaltungen durch deren Teilnehmer vorgenommen. Die bewerteten Dozenten hielten diese Einholung der Meinung der Studenten grundsätzlich für ein sinnvolles Mittel zur Verbesserung der Qualität ihrer Lehre, sie waren jedoch über den Ablauf der von der Leitung der Berufsakademie veranlassten Evaluation nicht unterrichtet worden. Auch wurden die Ergebnisse den betroffenen Lehrkräften gar nicht mitgeteilt, vielmehr ihre Kenntnis den Studienrichtungsleitern vorbehalten.

(1) Ich habe die Berufsakademie darauf hingewiesen, dass bei der Evaluierung von Vorlesungen personenbezogene Daten der Dozenten erhoben werden (obwohl es sich um deren Amtstätigkeit handelt). Dies bedarf einer konkreten rechtlichen Grundlage. Zwar eröffnet § 23 Abs. 2 Satz 1 SächsBAG grundsätzlich die Möglichkeit, personenbezogene Daten des Lehrpersonals zur Beurteilung der Lehrtätigkeit zu verarbeiten. Satz 2 der Regelung sieht jedoch vor, dass durch Rechtsverordnung zu bestimmen ist, unter welchen Voraussetzungen eine Auskunftspflicht besteht oder eine Erhebung ohne Einwilligung des Betroffenen durchgeführt werden kann. Ferner ist unter anderem zu regeln, welche Merkmale erhoben werden und wie ein Erhebungsverfahren auszusehen hat. Nach Satz 3 Nr. 5 ist beispielsweise auch fest-

zulegen, wie die Unterrichtung der Betroffenen über Zweck und Inhalt von Evaluationen erfolgen soll. Da eine solche, den § 23 Abs. 2 Satz 1 SächsBAG konkretisierende, Rechtsverordnung nicht existiert, kommt § 23 Abs. 2 Satz 1 SächsBAG nicht als Rechtsgrundlage in Betracht, nicht anders als im Falle des gleichlautenden § 106 Abs. 3 Satz 2 SächsHG. Neben der Spezialregelung des § 23 Abs. 2 SächsBAG ist, entgegen einer zeitweilig von der Studienakademie mir gegenüber vertretenen Auffassung, § 12 SächsDSG nicht anwendbar, kommt also als Rechtsgrundlage nicht in Betracht (vgl. auch § 2 Abs. 3 SächsDSG - Vorrang der lex specialis); stellte man in Ermangelung der Rechtsverordnung auf § 12 SächsDSG ab, wäre das der unzulässige Versuch der Umgehung der in § 23 Abs. 2 Satz 1 SächsBAG aufgestellten Voraussetzung.

Ich habe - nicht ohne dem SMWK Gelegenheit zur Stellungnahme zu geben - die Berufsakademie deshalb aufgefordert, alle mit der Evaluation erhobenen personenbezogenen Daten des Lehrpersonals zu löschen und bis zum Vorliegen einer entsprechenden Rechtsverordnung keine Evaluation durchzuführen, in denen personenbezogene Daten des Lehrpersonals verarbeitet werden.

(2) Die Berufsakademie hat daraufhin den Vorschlag unterbreitet, (bis zum Erlass einer Rechtsverordnung nach § 23 Abs. 2 Satz 2 SächsBAG) die Befragungen zur Bewertung der Lehrveranstaltungen zukünftig aufgrund einer *Einwilligung* der Dozenten durchzuführen. Zu diesem Zweck sollte ein Merkblatt erarbeitet werden, aus dem der Zweck der Evaluation sowie alle wesentlichen Punkte des § 23 Abs. 2 Satz 3 SächsBAG (Erhebungsmerkmale und Erhebungsverfahren) ersichtlich würden. Dieses Merkblatt solle den Dozenten vorgelegt werden, um ihre Einwilligung zu der Evaluation einzuholen. Werde diese Einwilligung nicht erteilt, würden die Lehrkräfte an weiteren Befragungen nicht beteiligt, ohne dass sie Nachteile zu befürchten hätten.

(Wohlgemerkt: Diese Voraussetzungen hatten nicht vorgelegen. Vielmehr hatte die Studienakademieleitung die Studenten ohne das Wissen der Betroffenen befragt, geschweige denn mit deren Einwilligung, weswegen die Befragung rechtswidrig durchgeführt worden war.)

(3) Dazu war Folgendes anzumerken:

(3.1) Wegen des Verfassungsgrundsatzes des *Vorbehaltes des Gesetzes* dürfen Träger öffentlicher Gewalt ihre Tätigkeit nicht ohne Weiteres dort, wo sie ihnen nicht vom Gesetz als Aufgabe und Eingriffsermächtigung übertragen ist, auf die Einwilligung der in ihren Grundrechten Betroffenen stützen. Hier war jedoch *durch Gesetz* eine solche Möglichkeit gerade eröffnet:

(3.2) Da der § 23 Abs. 2 Satz 2 SächsBAG, mit seinem Erfordernis einer Rechtsverordnung, ausdrücklich nur eine Datenerhebung *ohne Einwilligung* regelt, kann insoweit für Datenerhebungen auf Einwilligungsgrundlage § 12 Abs. 4 Nr. 2 SächsDSG als Rechtsgrundlage für die Datenerhebung bei Dritten herangezogen werden.

Eine solche Einwilligung des Betroffenen setzt voraus, dass er *zuvor* in geeigneter Weise über die beabsichtigte Datenverarbeitung, ihren Zweck und die Empfänger vorgesehener Übermittlungen aufzuklären ist, § 4 Abs. 3 SächsDSG. Diese Vorschrift regelt ferner, dass die Einwilligung der Schriftform bedarf.

Zum selben Ergebnis kommt man wohl auch über § 23 Abs. 2 Satz 1 SächsBAG i. V. m. § 12 Abs. 4 Nr. 1 SächsDSG: Man wird in § 23 Abs. 2 Satz 1 SächsBAG als zwingend vorausgesetzt ansehen können, dass die Beurteilung der Lehrtätigkeit beim Beurteiler und nicht beim Beurteilten, also, jedenfalls insoweit, bei den Studierenden erhoben werden darf; jedoch wegen Satz 2 der Regelung eben *ohne Einwilligung der Lehrkraft* nur auf der Grundlage einer entsprechenden Rechtsverordnung.

(3.3) Allerdings habe ich die Behörde (Staatliche Studienakademie) als Anstalt des öffentlichen Rechts (§ 3 Abs. 2 Satz 1 SächsBAG) nachdrücklich darauf hingewiesen, dass eine Einwilligung in die Verarbeitung personenbezogener Daten nur wirksam ist, wenn der Betroffene auch tatsächlich die Möglichkeit hat, selbst frei darüber zu entscheiden. Entscheidend dafür ist, dass derjenige, der seine Einwilligung nicht erteilt, keine Nachteile befürchten muss. Darauf würde die Studienakademie die Dozenten ausdrücklich hinweisen müssen, und diese Freiheit müsste sie auch tatsächlich unzweifelhaft gewährleisten.

In diesem Zusammenhang würde insbesondere auch gewährleistet sein müssen, dass die Ergebnisse der Bewertungen nicht zu den Personalakten der bewerteten Lehrkräfte genommen und dass die Fragebögen unmittelbar nach Abschluss der Auswertung vernichtet würden.

(3.4) Der Pflicht, die bisher bereits erhobenen personenbezogenen Daten gemäß § 20 Abs. 1 SächsDSG löschen zu müssen, hat die Behörde ebenfalls auf der Grundlage einer Einwilligung enthoben werden können, nämlich auf der Grundlage einer Einwilligung der Betroffenen in die Speicherung ihrer personenbezogenen Daten, §§ 13 Abs. 2 Nr. 1 i. V. m. § 12 Abs. 4 Nr. 2 SächsDSG, allerdings nur im Rahmen des nach § 23 Abs. 2 Satz 1 SächsBAG für die Durchführung der Beurteilung der Lehrtätigkeit Erforderlichen.

Ich habe dementsprechend dem Verfahrensvorschlag der Berufsakademie zugestimmt und diese bei der Ausarbeitung des (oben unter [2] genannten) Merkblattes unterstützt.

13.3 Probandendaten aus öffentlichen Bekanntmachungen (hier: nach der Insolvenzordnung)

Das Soziologische Institut einer sächsischen Universität verschickte im Rahmen eines Forschungsvorhabens zur Überschuldung von Verbrauchern bundesweit Fragebögen an Personen, die Insolvenz (sog. Verbraucherinsolvenz nach §§ 304 ff. InsO) angemeldet hatten. Die dafür nötigen Daten hatten die Wissenschaftler dem Internet entnehmen können, wo Daten zu Insolvenzverfahren nach Maßgabe des § 9 InsO zum Zweck der öffentlichen Bekanntgabe veröffentlicht werden.

Dem Petenten aus Niedersachsen habe ich erläutert, dass sich die Zulässigkeit der Veröffentlichung durch das Insolvenzgericht aus dem genannten § 9 InsO in Verbindung mit einzelnen Bekanntmachungsgeboten wie z. B. § 30 InsO (Eröffnungsbeschluss) ergibt und dass insbesondere vorgeschrieben ist, dass auch die Anschrift anzugeben ist (§ 9 Abs. 1 Satz 2 InsO). Diese Vorschrift eröffnet die Möglichkeit, anstelle der früher üblich gewesenen Veröffentlichung in Zeitungen auch das Internet zu nutzen. Das Nähere regelt auf der Grundlage von § 9 Abs. 2 Satz 2 InsO die *Verordnung zu öffentlichen Bekanntmachungen in Insolvenzverfahren im Internet* vom 12. Februar 2002 (InsOBekV). Diese Rechtsvorschrift sieht eine Beschränkung der Suchmöglichkeiten nach Ablauf von zwei Wochen nach dem ersten Tag der Veröffentlichung vor und bestimmt Löschungsfristen. Es war ersichtlich, dass die Daten von den Forschern rechtmäßig aus dieser Quelle hatten ermittelt werden können. Die Forscher hatten auch hinreichend auf die - selbstverständliche - Freiwilligkeit einer Ausfüllung und Rücksendung des Fragebogens hingewiesen.

Die Erhebung, Speicherung und Nutzung der aus dem Internet gewonnenen Daten durch die Forscher im Rahmen von deren über mehr als ein Jahrzehnt gehenden Forschungsvorhaben war für dieses dienlich und damit von der Freiheit von Forschung und Lehre gedeckt, so dass sich nach gefestigter Auffassung die Frage nach der Erforderlichkeit dieser Datenverarbeitung nicht gestellt hat.

Zu der danach erlaubten Datenverarbeitung durch die Forscher hat dabei auch die Speicherung und Nutzung zum Zweck der Erinnerung derjenigen Probanden gehört, die aufgrund der ersten Einladung noch keinen ausgefüllten Fragebogen eingesandt hatten.

Hier allerdings hatten die Forscher im Falle des Petenten insoweit die Grenze überschritten, als sie es versäumt hatten, nach dessen mit großer Empörung schriftlich ernsthaft und endgültig erklärten Verweigerung einer freiwilligen Datenhingabe ihn aus der Probandenliste zu löschen, weil der Petent damit schon genügend deutlich gemacht hatte, dass er auch für die Zukunft auf jeden Fall eine Mitwirkung ausschließe, mit der Folge, dass eine nochmalige Aufforderung, den Fragebogen auszufüllen, nicht mehr sinnvoll sein würde.

13.4 Videoüberwachung in der Universität Leipzig

Betroffene hatten mich über angebliche Pläne der Universität, im Zuge von Umbauarbeiten auch die neuen Hörsäle mit Videoüberwachungstechnik auszustatten, informiert. Ich nahm dies zum Anlass einer umfassenden Kontrolle der Videoüberwachungssysteme der Universität Leipzig. Dabei konnte ich in der Mehrzahl der Fälle eine datenschutzgerechtere Gestaltung der bisher eingesetzten Videoüberwachung erreichen und die Voraussetzungen des Einsatzes von Videoüberwachungstechnik in Hörsälen klarstellen; hinsichtlich einiger Aspekte ist meine Tätigkeit noch nicht abgeschlossen. Die folgenden Ausführungen gelten auch für die Videoüberwachungssysteme in anderen sächsischen Hochschulen.

Nach § 106 SächsHG dürfen sächsische Universitäten „die personenbezogenen Daten verarbeiten, die insbesondere für (…) die Nutzung von Hochschuleinrichtungen (…) erforderlich sind“. *Erforderlich* ist eine Datenerhebung, wenn die Aufgabe ohne sie nicht, nicht rechtzeitig oder nicht vollständig erfüllt werden könnte, m. a. W. wenn sie zur Aufgabenerfüllung zwingend notwendig ist. Bei der Auslegung des Begriffs der Erforderlichkeit im konkreten Fall ist zu beachten, dass das Datenschutzrecht von dem Grundsatz geprägt ist, dass Datenerhebungen und andere Verarbeitungsschritte grundsätzlich verboten sind („Verbot mit Erlaubnisvorbehalt“). Im Gegensatz dazu stehen die lediglich der Aufgabenerfüllung *dienlichen* Datenerhebungen, die die Aufgabenerfüllung unterstützen und erleichtern, ohne im oben beschriebenen Sinne erforderlich zu sein. Aufgaben der Universität Leipzig sind die in den §§ 7 bis 36 SächsHG beschriebenen Aufgaben, hier insbesondere Studium und Lehre sowie die Forschung. Öffentliche Sicherheit umfasst den Schutz subjektiver Rechtsgüter und Rechte des Einzelnen, den Schutz der Einrichtungen und Veranstaltungen von Trägern von Hoheitsgewalt und die Durchsetzung von in der objektiven Rechtsordnung begründeten Verhaltenspflichten.

Nach § 33 Abs. 1 SächsDSG dürfen öffentlich zugängliche Räume nur videoüberwacht werden, soweit dies zur Aufgabenerfüllung, insbesondere zur Gewährleistung

der öffentlichen Sicherheit, erforderlich ist. Öffentlich zugänglich i. d. S. sind auch die Räume der Universität Leipzig.

Aus der Zusammenschau beider Vorschriften ergibt sich, dass die Universität Leipzig Räume (nur) videoüberwachen darf, wenn die Nutzung von Hochschuleinrichtungen insbesondere aus Gründen der öffentlichen Sicherheit ansonsten nicht, nicht rechtzeitig oder nicht vollständig gewährleistet werden könnte. Dieser strenge Maßstab ist in Literatur (vgl. z. B. Simitis u. a., BDSG/Sokol, § 13 Rdnr. 25 ff.) und Rechtsprechung (vgl. u. a. LG Berlin NZM 2001, 707, 708; BGH NJW 1995, 1957; vgl. LG Braunschweig NJW 1998, 2457, 2458) anerkannt. Erforderlich ist danach eine Videoüberwachung z. B. dann nicht, wenn der Schutz des Eigentums (gegen Diebstahl oder Vandalismus) oder des Hausrechts auch durch andere geeignete Maßnahmen wie die nächtliche Beleuchtung, den Einbau einer Schließanlage oder durch häufigere Kontrollen des Sicherheitspersonals oder des Hausmeisters erreicht werden kann (vgl. LG Berlin NZM 2001, 7070, 708).

Eine in diesem Sinne erforderliche Videoüberwachung kann gleichwohl unzulässig sein, wenn Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Maßstab sind die durch das Recht auf informationelle Selbstbestimmung geschützten Interessen derjenigen, die Objekt der Videoüberwachung sind. Der mit der Beobachtung verfolgte Zweck muss in einem angemessenen Verhältnis zu den schutzwürdigen Interessen der Betroffenen stehen. Eine Videoüberwachung ist insbesondere dann als intensiver Eingriff in die Rechte der Betroffenen zu gewichten, wenn diese im Rahmen eines normgemäßen Verhaltens zu einer Verfolgung keinen Anlass gegeben haben. Von erheblichem Gewicht ist eine Videoüberwachung ferner, wenn sie ununterbrochen einen Raum unter Kontrolle hält, dem die Betroffenen nicht ausweichen können (vgl. LG Braunschweig NJW 1998, 2457, 2458). Im konkreten Fall müsste das (Grund-)Recht auf informationelle Selbstbestimmung der Studenten, Hochschullehrer und sonstigen Bediensteten überdies vor dem Hintergrund der Gewährleistung von Maßnahmen zum Schutz der freien wissenschaftlichen Betätigung gesehen werden (vgl. BVerfGE 35, 114 ff.; 95, 209). Auch hat das Bundesverfassungsgericht mehrfach festgestellt, dass „das Grundrecht (…) über das hinaus, was es unmittelbar gewährleistet, auch dem Schutz vor einem Einschüchterungseffekt (dient), der entstehen und zu Beeinträchtigungen bei der Ausübung anderer Grundrechte führen kann, wenn für den Einzelnen nicht mehr erkennbar ist, wer was wann und bei welcher Gelegenheit über ihn weiß“ (BVerfG, Beschluss vom 12. April 2005 (2 BvR 1027/02), in NJW 2005, 1917, 1918 zur Beschlagnahme von Rechtsanwalts-Dateien).

Schließlich muss eine in diesem Sinne erforderliche und die Rechte der Betroffenen wahrende Videoüberwachung auch verhältnismäßig, also geeignet, erforderlich und angemessen, sein.

Als Beispiel mögen meine Feststellungen zu den Videokameras in den sog. PC-Pool-Räumen des Universitäts-Rechenzentrums dienen: Bei meinem Kontrollbesuch wurde mir erklärt, dass trotz „konventioneller“ Sicherungsmaßnahmen immer wieder Beschädigungen und Diebstähle der wertvollen Rechner vorgekommen seien. Insofern konnte ich die Voraussetzungen einer Videoüberwachung als erfüllt ansehen. Dabei fiel mir allerdings auf, dass die konkrete Art der Überwachung der in Linie nebeneinander stehenden Rechner trotzdem gegen den Datenschutz verstieß. Denn die Kameras waren in den Zimmerecken der PC-Pool-Räume, also schräg zu den Rechnern, angebracht. Auf diese Weise konnten die durch die Studenten aufgerufenen Webseiten mit überwacht werden. Das war zur Aufgabenerfüllung nicht erforderlich und verstieß gegen die Wissenschafts- und Informationsfreiheit. Ich habe daraufhin angeregt, die Kameras künftig so ausrichten, dass Monitorbilder der Studenten nicht mehr beobachtet und aufgezeichnet werden können, namentlich dadurch, dass die Kameras ebenfalls in Linie mit den Rechnern angebracht werden. Durch diese einfache technisch-organisatorische Maßnahme konnte der Datenschutz in den PC-Pool-Räumen verbessert werden. Die Universität ist dieser und weiteren Anregungen gefolgt.

14 Technischer und organisatorischer Datenschutz

14.1 Speicherung der Nutzungsdaten von Internetangeboten

Die Sächsische Staatskanzlei informierte mich über ihre Pläne zur Schaffung eines zentralen E-Government-Portals, das mittlerweile unter www.amt24.sachsen.de interessierten Bürgern zur Nutzung offen steht.

Ich wies frühzeitig darauf hin, dass die geplante siebentägige Speicherung von Nutzungsdaten (u. a. die IP-Adresse des Nutzers) wegen eines Verstoßes gegen § 6 Abs. 1 TDDSG unzulässig ist. Mir wurde daraufhin mitgeteilt, dass auf die geplante Speicherung der Nutzungsdaten verzichtet wird.

Bei einem Aufruf des Angebots musste ich jedoch feststellen, dass zum Datenschutz ausgeführt wird: „Nicht anonymisierte Daten werden nach einer Woche gelöscht." Weiterhin wird darauf hingewiesen, dass „für die Überwachung und Abwehr sicherheitsrelevanter Ereignisse … bei jedem Zugriff" u. a. die IP-Adresse des nutzenden Hosts gespeichert wird.

Ich wies die Staatskanzlei erneut darauf hin, dass diese Speicherung unzulässig ist.

Gemäß § 6 Abs. 1 TDDSG darf der Diensteanbieter, im vorliegenden Fall die Sächsische Staatskanzlei, personenbezogene Daten eines Nutzers ohne dessen Einwilligung nur verarbeiten, soweit dies erforderlich ist, um die Inanspruchnahme von Telediensten zu ermöglichen und abzurechnen.

Diese Rechtsauffassung wird durch ein Urteil des AG Darmstadt vom 30. Juni 2005 (300 C 397/04) bestätigt, welches durch einen Beschluss des BGH vom 26. Oktober 2006 (Az. III ZR 40/06) rechtskräftig wurde. In diesem heißt es:

„*§ 6 Abs. 1 TDDSG bestimmt, dass der Diensteanbieter personenbezogene Daten eines Nutzers ohne dessen Einwilligung nur erheben, verarbeiten oder nutzen darf, soweit dies erforderlich ist, um die Inanspruchnahme von Telediensten zu ermöglichen und abzurechnen.*

Solche Nutzungsdaten dürfen nach § 6 Abs. 4 TDDSG nur gespeichert werden, soweit sie für Zwecke der Abrechnung mit dem Nutzer erforderlich sind. Auch für § 6 Abs. 4 TDDSG gilt, dass darin lediglich die Speicherung für die Zwecke der Abrechnung, also für die Erstellung der Abrechnung als solche, nicht aber für die Durchsetzbarkeit oder Beweisbarkeit der Richtigkeit der Abrechnung zugelassen ist. Ansonsten gilt das gleiche wie zu § 97 Abs. 3 TKG. Auch in § 6 Abs. 8 TDDSG

besteht die Möglichkeit, Nutzungsdaten allgemein länger zu speichern. Dies setzt aber zu dokumentierende tatsächliche Anhaltspunkte voraus, dass Dienste von bestimmten Nutzern in der Absicht in Anspruch genommen werden, das Entgelt nicht oder nicht vollständig zu entrichten. Auch dieser Sonderfall ist vorliegend nicht gegeben.

Das Gericht weist darauf hin, dass die Sicherheit des Internets, die Verfolgung von schwerwiegenden Straftaten und gegebenenfalls auch die Verfolgung urheberrechtlicher oder zivilrechtlicher Ansprüche die Speicherung von dynamischen IP-Adressen sinnvoll oder auch erforderlich erscheinen lassen. Dies hat der Kläger selbst eingeräumt.

Dennoch sieht das Gericht im Rahmen des geltenden Rechts keine Möglichkeit der Beklagten, IP-Adressen ohne konkreten Bezug auf einen Missbrauch zu speichern (vgl. ebenso Schmitz MMR 2003, Seite 213, Heidrich DUD 2003, Seite 237; Dix DUD 2003, Seite 234; Breyer DUD 2003, Seite 491)."

An dieser Unzulässigkeit hat sich auch durch das nunmehr in Kraft getretene Telemediengesetz (BT-Drs. 16/3078) nichts geändert; eine entsprechende Regelung enthält § 15 Abs. 1 TMG.

Die Sächsische Staatskanzlei teilte mir daraufhin mit, dass sie angesichts der Rechtslage zukünftig auf die Speicherung nicht anonymisierter Nutzungsdaten verzichten wird und die Datenschutzerklärung von www.amt24.sachsen.de entsprechend fassen wird.

Aus gegebenem Anlass weise ich darauf hin, dass der Verzicht auf die Speicherung von IP-Adressen der Nutzer selbstverständlich nicht nur für das Web-Angebot der Sächsischen Staatskanzlei, sondern für alle entsprechenden Internetpräsenzen öffentlicher Stellen im Freistaat Sachsen gilt. Es ist somit z. B. auch allen anderen staatlichen Stellen, aber auch den Kommunen, Landkreisen, deren Eigenbetrieben und Kommunalwirtschaftsunternehmen untersagt, nicht anonymisierte Nutzungsdaten zu speichern, wenn diese nicht konkret zu Abrechnungszwecken benötigt werden.

Meine Rechtsauffassung wurde nach dem Ende des Berichtszeitraums durch ein Urteil des Amtsgerichts Mitte (Berlin) vom 27. März 2007 (5 C 314/06), das mit dem Urteil des Landgerichts Berlin vom 6. September 2007 (23 S 3/07) rechtskräftig wurde, bestätigt.

Ich habe in diesem Zusammenhang ein externes Unternehmen beauftragt, die technischen Randbedingungen in Bezug auf die Protokollierung für die beiden gebräuchlichsten Webserver „Apache“ (OpenSource) und „Internet Information Server“ (IIS, Fa. Microsoft) zu prüfen. Dabei stellte sich heraus, dass beide Server so konfiguriert werden können, dass IP-Adressen nicht gespeichert werden. Mir ist bekannt, dass viele Serverbetreiber zur Optimierung ihres Webangebotes eine Analyse der aufgerufenen Webseiten benötigen. Dazu sind im wesentlichen Kriterien wie Typ des Browsers, Sprache/Landesherkunft und ggf. Verweildauern von Bedeutung. Eine personenbeziehbare IP-Adresse ist dazu jedoch nicht erforderlich, allenfalls die Ableitung der Herkunft des Besuchers aus der IP-Adresse.

Aus diesem Grund habe ich prüfen lassen, inwiefern die IP-Adresse im Prozess der Protokollierung anonymisiert werden kann, so dass sowohl der Personenbezug entfällt als auch dem Wunsch der Herkunftsermittlung aus der IP-Adresse entsprochen werden kann. Für den Apache Webserver konnte bereits eine Lösung gefunden werden, über die ich nach erfolgter technischer Abnahme unter „www.datenschutz.sachsen.de“ informieren werde. Die Gespräche mit der Firma Microsoft über eine adäquate Realisierung für den IIS dauern derzeit noch an.

14.2 Biometrische Merkmale in neuen Ausweispapieren - Fortsetzung

In 12/14.2 wurde bereits ausführlich über die datenschutzrechtlichen Anforderungen und über den Entwicklungsstand beim Einsatz biometrischer Merkmale in Pässen und Ausweisen berichtet.

Seit Herbst 2005 werden die Reisepässe mit dem ersten biometrischen Merkmal, dem digitalisierten Gesichtsbild ausgestattet. Dabei wird das frontal aufgenommene Gesichtsbild nicht nur optisch auf das Dokument aufgebracht, sondern auch als Referenzdatei komprimiert im RF-Chip (Radio Frequency) des Passes gespeichert.

Dazu legt die EU-Verordnung (EG 2252/2004) Mindestnormen fest. Sie fordert die Gewährleistung der Integrität, Authentizität und Vertraulichkeit der gespeicherten biometrischen Daten (Gesichtsbild, Fingerabdruck). Zusätzliche Sicherheitsmerkmale und Sicherheitsanforderungen sollen einen höheren Schutz vor Fälschungen und Nachahmung gewährleisten sowie den unbefugten Zugriff verhindern. Deshalb sind alle gespeicherten Passdaten mit einer digitalen Signatur zu sichern. Eine ausführliche Beschreibung der vorgesehenen Sicherheitsmaßnahmen bei der Aufnahme

biometrischer Merkmale in Pässen und den zweistufigen Zugriffsschutzmaßnahmen beim Auslesen der im RF-Chip gespeicherten Daten ist unter 12/14.2 nachzulesen.

Außerdem wird angeordnet, dass jeder Mitgliedsstaat eine zuständige Stelle (hier die Bundesdruckerei GmbH) für den Druck der Pässe benennt und dass die Bürger das Recht haben, ihre auf dem Pass gespeicherten personenbezogenen Daten zu überprüfen und gegebenenfalls eine Berichtigung oder Löschung zu beantragen. Dazu stellt die Bundesdruckerei allen Passbehörden ePass-Lesegeräte zur Verfügung.

Diese Verordnung regelt auch, dass die Verwendung biometrischer Daten in Ausweisen nur zur Prüfung der Authentizität des Dokuments und der Identität des Inhabers durch direkt verfügbare abgleichbare Merkmale zu überprüfen sei, wenn die Vorlage eines Passes gesetzlich vorgeschrieben ist. Eine zentrale Speicherung der Passdaten ist verboten.

Hier soll nun über das weitere Vorgehen aus technisch-organisatorischer Sicht informiert werden.

Zukünftig wird auch der Personalausweis mit biometrischen Merkmalen ausgestattet (§ 1 Abs. 4 PersAuswG). Außerdem soll der Personalausweis (BT-Drs. 16/1880) auch eine sichere elektronische Authentisierung für elektronische Geschäftsprozesse, Online-Banking und andere Internetgeschäfte ermöglichen und optional für das Nachladen einer qualifizierten Signatur vorgesehen sein. Die Erstausgabe der neuen Ausweise ist für das Jahr 2008 vorgesehen.

Ab November 2007 sollen im RF-Chip des Reisepasses (ePass) die Fingerabdrücke als zweites biometrisches Merkmal gespeichert werden. Mit einem zertifizierten Fingerabdruck-Scanner werden die flachen Abdrücke des linken und rechten Zeigefingers erfasst. Bei Verletzungen oder unzureichender Qualität ist dann der Mittelfinger, Ringfinger oder der Daumen zu nutzen.

Die Erfassung, Speicherung, Übermittlung und Nutzung der Fingerabdruckdaten erfordert erhöhte Sicherheitsanforderungen, weil der Fingerabdruck ein besonders sensibles personenbezogenes Datum ist. So muss das ePass-Lesegerät mit einem eigenen Schlüsselpaar und einem vom RF-Chip prüfbaren Zertifikat, das die Rechte des Lesegerätes genau festlegt, ausgestattet sein. Der stärkere Zugriffsschutz wird durch Extended Access Control (EAC) gewährleistet (s. 12/14.2).

Künftig soll das Passantragsverfahren vollständig elektronisch durchgeführt werden. Dazu stattet der Passhersteller, die Bundesdruckerei, die Passbehörden mit der not-

wendigen Hard- und Software aus. Die erforderlichen Sicherheitsmaßnahmen hat das BSI in der „Technischen Richtlinie zur Produktionsdatenerfassung, -qualitätsprüfung und -übermittlung für Pässe“ (BSI TR-03104) festgelegt.

Diese Richtlinie ordnet die notwendigen Sicherheitsmaßnahmen von der Datenerfassung bis zur Datenübermittlung einschließlich Testdatenübermittlung an.

Zum besseren Verständnis soll der Verfahrensablauf zwischen Passbehörde und Passhersteller vereinfacht kurz erläutert werden:

- Die Antragsdaten der Bürger werden in der Passbehörde aufgenommen, die erforderlichen biometrischen Daten erfasst und deren Qualität geprüft. Die erfassten Antragsdaten werden zu einem digitalen Datensatz zusammengefasst, digital signiert und verschlüsselt.

- Die Passbehörde oder eine Vermittlungsstelle, die mit der Verarbeitung der Antragsdaten von der Passbehörde beauftragt werden kann, überträgt den digitalen Datensatz integer, authentisch und vertraulich zum Passhersteller.

- Der Passhersteller nimmt den Datensatz entgegen, entschlüsselt diesen, prüft die digitale Signatur und bestätigt der Passbehörde oder Vermittlungsstelle den sicheren Empfang der Daten.

- Nach einer zentralen Qualitätsprüfung wird das Personaldokument produziert und ausgeliefert.

In der technischen Richtlinie wird angeordnet, dass jede Passbehörde und der Passproduzent eigene Signaturzertifikate auf Smartcards, die sicher zu verwahren sind, einsetzt. Der Passhersteller kann auch Softwarezertifikate nutzen wegen der hoch gesicherten Einsatzumgebung.

Die erforderlichen Signatur- und Verschlüsselungskomponenten sowie die zugehörigen Smartcards und Smartcardleser müssen mindestens EAL 3+ zertifiziert sein. Digitale Signaturen, Verschlüsselung und Authentisierung sind durch X.509-Zertifikate mit ausreichender kryptographischer Stärke umzusetzen. Die erforderlichen Zertifikate sind in einer Public-Key-Infrastruktur (PKI) zu generieren, zu verwalten und zu prüfen. Die einzusetzenden Algorithmen und Schlüssellängen haben die Empfehlungen der Bundesnetzagentur zur Eignung der Signaturalgorithmen zu beachten.

Außerdem wird in der technischen Richtlinie OSCI-Transport (Online Service Computer Interface) als Übermittlungsprotokoll für die Antragsdaten und Rückantworten

festgelegt. OSCI-Transport ist ein Standard, mit dem prinzipiell beliebige Informationen automatisiert übertragen werden können. Die Informationen können signaturgesetzkonform signiert und durch Verschlüsselung vor Ausspähung geschützt werden. Daneben bietet OSCI-Transport weitere Sicherheitsmechanismen, die insbesondere die Nachvollziehbarkeit der Kommunikation betreffen. OSCI-Transport gewährleistet einen sicheren, rechtsverbindlichen und nachvollziehbaren Datenaustausch („Einschreiben mit Rückschein“).

OSCI-Transport erfüllt grundlegende Anforderungen des Datenschutzes und der Datensicherheit in hoher Qualität.

Zeitlich befristet kann die Datenübermittlung mit WSDL/SOAP (Web Services Description Language/Simple Object Access Protocol) über HTTPS (Secure Hypertext Transfer Protocol) mit einer Web-Server- und Client-Authentisierung erfolgen, wenn OSCI-Transport noch nicht installiert werden konnte.

Zu beachten ist jedoch, dass die technische Richtlinie keine Sicherheitsmaßnahmen für die Übermittlungsstrecke zwischen Passbehörde und Vermittlungsstelle festlegt, sofern eine Vermittlungsstelle zur Datenverarbeitung zwischen geschaltet wird. Die Passbehörde ist dann für ausreichende Sicherheitsmaßnahmen bei der Datenübermittlung zur Vermittlungsstelle verantwortlich. Deshalb werde ich die festgelegten Maßnahmen für diesen Übermittlungsweg in Sachsen besonders kontrollieren.

Ein Feldtest wurde auf freiwilliger Basis vom 1. März 2007 bis zum 30. Juni 2007 in mehr als 20 Passbehörden die vollständige elektronische Erfassung, Prüfung und Übermittlung sämtlicher Passantragsdaten an die Bundesdruckerei GmbH erprobt. Sächsische Passbehörden in Chemnitz, Meißen und Taucha nahmen an der Erprobung teil.

Der Pilottest sollte die fachlichen Anforderungen, die Interoperabilität, die Stabilität und vor allem auch die sichere vertrauliche, integre und authentische Übermittlung der Passantragsdaten im Echtbetrieb testen.

Die Testpässe wurden aber nicht in Umlauf gebracht und nach Ablauf der Testphase vernichtet. Die zwischengespeicherten Fingerabdruckdaten wurden ebenfalls sicher gelöscht.

Ich informierte mich vor Ort in den drei ausgewählten sächsischen Pilotpassbehörden Chemnitz, Meißen und Taucha über die Durchführung des Feldtests zur Erfassung, Übermittlung und Speicherung der Fingerabdrücke.

Die rechtlichen Grundlagen für die Durchführung des Feldtests wurden durch die Änderung des Passgesetzes (Einfügung des § 23a PaßG) geschaffen. Diese Vorschrift regelt unter anderem den Zweck, den Umfang, den Zeitraum und den Umgang mit den Fingerabdruckdaten während des Feldtests in den Pilotpassbehörden und beim Passhersteller. Diese Regelung beinhaltet auch die zulässigen technischen Anforderungen und Verfahren zur Erfassung und Qualitätssicherung der Fingerabdrücke sowie das Verfahren der Übermittlung sämtlicher Passantragsdaten von den teilnehmenden Passbehörden an den Passhersteller, die in der technischen Richtlinie vom BSI veröffentlicht wurden.

Die technische Richtlinie (BSI TR-03104) fordert eine integre, vertrauliche und authentische Übermittlung der Passantragsdaten und Rückantworten mittels OSCI-Transport oder ersatzweise Übermittlung auf Basis von XML und WSDL/SOAP über HTTPS.

Entgegen diesen Vorgaben übermittelten aber die drei Testbehörden die Antragsdaten mit dem D-SAFE®-Modul der Bundesdruckerei GmbH. Mit diesem Vorgehen werden Erkenntnisse über ein Verfahren gewonnen, die bei der rechtskonformen Datenübermittlung nicht von Belang sind. Es werden weder Funktionalität, Interoperabilität, Stabilität noch Sicherheit der vorgeschriebenen Datenübermittlung erprobt.

Ein weiteres Problem stellte teilweise das Löschen der gespeicherten Fingerabdruckdaten in den Passbehörden dar. Die gespeicherten Fingerabdrücke sind spätestens nach Aushändigung des Passes zu löschen. Nicht alle am Pilottest teilnehmenden Behörden konnten dies bisher datenschutzgerecht realisieren. Die Behörden und deren Dienstleister (Verfahrensentwickler) bemühen sich jedoch diese Anforderung so bald als möglich zu erfüllen.

Ich konnte auch feststellen, dass die Mitarbeiter der Passbehörden die Bürger, die einen Pass beantragen wollten, umfassend über den Feldtest zur Fingerabdruckerfassung aufklärten. Daher gab es bisher keine Verweigerung bei der Abnahme von Fingerabdrücken der Bürger.

Mehrfach wurde in verschiedenen Medien über die Gefahr des Klonens von gespeicherten Daten im RF-Chip von Pässen berichtet. Das BSI hat dazu im Februar 2007 Stellung genommen. In einer Kurzmeldung wird die Gefahr des Klonens von Chips ausgeschlossen. Durch geeignete Maßnahmen (digitale Signatur der gespeicherten Daten, Chip-Authentisierung beim Datenzugriff mittels Extended Access Control (EAC), starke Verschlüsselung) würde ein Klonen des ePass-Chips wirkungsvoll verhindert.

Entgegen den Forderungen der Datenschützer gibt es nun allerdings Bestrebungen, die gespeicherten biometrischen Daten in Pässen nicht nur mit den vor Ort aufgenommenen biometrischen Daten auf Übereinstimmung (1:1-Vergleich) zu prüfen, sondern auch mit Referenz- oder Fahndungsdatenbanken abzugleichen.

Der Innenausschuss des Bundesrates (BR-DS. 16/07) möchte durch Änderung des Passgesetzes z. B. einen automatisierten Abgleich von Gesichtsbild und Fingerabdruck mit geeigneten Referenzdatenbanken (z. B. automatisches Fingerabdruck Identifizierungssystem (AFIS) beim BKA) ermöglichen. Weichen die Personalien voneinander ab, kann der kontrollierende Beamte „geeignete Folgemaßnahmen“ einleiten, um die Identität zweifelsfrei feststellen zu können. So sollen z. B. falsche Angaben durch Täuschung oder Bestechlichkeit eines Mitarbeiters der passausstellenden Behörde aufgedeckt werden können.

Außerdem will der Bundesrat bei der Passkontrolle die strenge Löschungsregelung für die ausgelesenen Daten abschwächen. Sollte das Dokument unecht oder der Dokumenteninhaber nicht mit der Person, die der Pass ausweist, identisch sein, soll die sofortige Löschung unterbleiben, wenn diese Daten zur „notwendigen Beweissicherung“ für nachfolgende Verfahren (Gefahrenabwehr, Strafverfahren) benötigt würden.

Die Entschließung der Datenschutzkonferenz des Bundes und der Länder vom 8. März 2002 fordert jedoch, dass die Verwendung biometrischer Daten in Ausweisen und Pässen grundsätzlich auf die Feststellung beschränkt bleiben soll, dass die dort gespeicherten Daten mit den Merkmalen der jeweiligen Ausweisinhaber übereinstimmen. Eine Verwendung der Daten für andere öffentliche Zwecke sollte ausgeschlossen werden. Die geforderte strikte Zweckbindung würde beim Abgleich mit Referenzdatenbanken unterlaufen.

Die weitere Entwicklung bei der Nutzung biometrischer Merkmale in Pässen und Ausweisen werde ich interessiert verfolgen und darüber berichten.

14.3 RFID

Bereits in 12/14.2 hatte ich auf die Chancen und Risiken dieser Technologie hingewiesen. Seinerzeit hatte sich die 67. Konferenz der Datenschutzbeauftragten des Bundes und der Länder voll inhaltlich einer Entschließung zu „Radio Frequency Identification“ der Internationalen Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre angeschlossen, in der auf mögliche negative Folgen für

die Privatsphäre und die Berücksichtigung von Datenschutzprinzipien hingewiesen wurde.

Für den aktuellen Berichtszeitraum ist festzustellen, dass die RFID-Technologie am Markt eine steigende Verbreitung findet, was nicht zuletzt seine Ursache in den sinkenden Produktionskosten für die so genannten Funk-Etiketten hat. Stand zunächst ein Effizienzgewinn innerhalb der Logistikkette im Vordergrund, ist derzeit auch ein Trend hin zum Consumer-Artikel zu verzeichnen, der als Synonym für die Alltagsdurchdringung stehende „funkende Joghurtbecher“ erscheint aufgrund sinkender Chipkosten tatsächlich am Horizont.

Da das Potential dieser Technologie durchaus geeignet erscheint, mit einer Vielzahl von (unter Umständen unbemerkten) Datenverarbeitungsvorgängen den Alltag zu verändern, hat sich der Arbeitskreis „Technische und organisatorische Datenschutzfragen“ mit dem Thema RFID kritisch auseinandergesetzt und dazu eine Orientierungshilfe „Datenschutzgerechter Einsatz von RFID“ (siehe www.datenschutz.sachsen.de, Rubrik Arbeitshilfen) erstellt.

Zum Einsatz dieser Technologie im Zusammenhang mit der Herstellung der neuen Reisepässe verweise ich auf Kapitel 14.2.

Die auf der 72. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 26./27. Oktober 2006 verabschiedete Entschließung „Verbindliche Regelungen für den Einsatz von RFID-Technologien“ (vgl. 16.2.16) forderte erneut, rechtzeitig bei der Verfahrensentwicklung auf Transparenz, Kennzeichnungspflicht, Schutz vor heimlicher Datenverarbeitung und Profilbildung und die Möglichkeit der dauerhaften Deaktivierung zu achten.

Während diese Forderungen von den Interessenverbänden der Wirtschaft weitgehend akzeptiert werden, gehen die Auffassungen über entstehende Risiken derzeit noch auseinander.

Insgesamt ist festzustellen, dass der Bedarf an einer umfassenden gesellschaftlichen Diskussion von allen Beteiligten erkannt wurde. Dabei handelt es sich keineswegs nur um eine innerdeutsche Betrachtung, auch auf europäischer Ebene soll die Meinungsbildung durch eine im Juli 2007 gegründete RFID-Expertengruppe befördert werden, bei der die Sicht des Datenschutzes durch die Beteiligung der Artikel-29-Datenschutzgruppe einfließen wird (http://ec.europa.eu/information_society/policy/rfid/doc/rfidswp_en.pdf).

14.4 Anonyme Nutzung des Rundfunks auch in Zukunft ermöglichen

Im Berichtszeitraum gab es in den Medien immer wieder Hinweise auf die Pläne privater Fernsehanbieter, ihre Programme ausschließlich in verschlüsselter Form zu übertragen. Würden diese Pläne umgesetzt, könnten Fernsehangebote ähnlich dem so genannten Pay-TV nur mit einem entsprechenden Decoder (Set-Top-Box) und einer zugehörigen Smartcard in Anspruch genommen werden. Während das Interesse der beteiligten Unternehmen anscheinend darin besteht, den Zuschauer genauer identifizieren zu können (um dann bei Kenntnis der Interessen zielgenauere Zusatzangebote platzieren zu können), besteht das Problem aus Sicht des Datenschutzes genau darin: Die Anonymität des Zuschauers würde durch eine personengebundene Smartcard praktisch aufgehoben.

Dabei sind die rechtlichen Grundlagen klar, denn nach § 47 RStV i. V. m. § 13 Abs. 6 TMG ist die Nutzung von Rundfunk wie auch die Bezahlung in Anspruch genommener Leistungen anonym oder unter Pseudonym zu ermöglichen, wenn dies technisch möglich und zumutbar ist.

Die Datenschutzbeauftragten des Bundes und der Länder fordern deshalb in einer Entschließung auf der 73. Konferenz (vgl. 16.2.19) die Länder auf, die Einhaltung der datenschutzrechtlichen Anforderungen des Rundfunkstaatsvertrages gegenüber den Veranstaltern durchzusetzen und damit eine anonyme Nutzung von Rundfunkprogrammen auch in Zukunft sicherzustellen.

14.5 Technische Gefährdungen des Datenschutzes beim Einsatz von PDAs und neueren Übertragungswegen von Informationen

Grundsätzlich ist zu beachten, dass der Aufbewahrungsort von Speichermedien mit Daten von hohem Schutzniveau genau zu regeln und zu kontrollieren ist. Insbesondere die Inhalte mobiler Datenträger (Flashkarten, Minifestplatten, USB-Sticks) können in so genannten Kartenlesern extern (also unabhängig von der EDV mit ihren Zugriffsrichtlinien u. ä. m.) kopiert und anschließend z. B. als Multimedia-SMS per Handy versendet werden. Auch das umfangreiche Fotografieren des Bildschirminhaltes mittels neuerer Mobiltelefone bzw. PDAs stellt heute technisch kein aufwändiges Problem mehr dar. So ist in Sicherheitsbereichen oder sicherheitsrelevanten Beratungen die Benutzung von Mobiltelefonen grundsätzlich zu regeln, da die Speicherkapazitäten heutiger PDAs und Mobiltelefone eine digitale

Sprachaufzeichnung bzw. Videostreaming von längeren Konferenzen durchaus ermöglichen.

Gefährdungen stellen auch die meist auf Webseiten der jeweiligen Hersteller dargebotenen Konfigurationsmöglichkeiten für PDAs und Mobiltelefone dar. Da dies bei der Baugröße (besonders Tastengröße) heutiger mobiler Kommunikationsmittel eine willkommene Erleichterung darstellt, werden diese Daten bei den Anbietern meist dauerhaft gespeichert. Inwieweit diese Speicherung verschlüsselt erfolgt, entzieht sich meist einer genauen Kenntnis. Eine Offline-Konfiguration, also am PC des jeweiligen Anwenders, ist einer webbasierten vorzuziehen.

Auch ist darauf zu achten, dass so genannte kontaktlose Zugriffe von Drittgeräten auf die EDV vermieden werden bzw. dass solche Leistungsmerkmale deaktiviert werden. Viele Laptops und PDAs von Entscheidungsträgern haben kontaktlose Verbindungsmöglichkeiten (WLAN, Bluetooth, Infrarot bzw. andere Nahfunktechniken) bereits eingebaut, die damit der Gefahr eines unberechtigten Zugriffs ausgesetzt sein können. Solche Funktionen sollten grundsätzlich deaktiviert sein und nur für die Dauer einer beabsichtigten Benutzung aktiviert werden.

Des Weiteren sind Mobiltelefone mit Leistungsmerkmalen wie Bluetooth, Infrarot, WLAN, Internetzugang, E-Mail oder Online-Update durchaus ähnlichen Gefahren wie ein „normaler Online-Computer“ ausgesetzt. Hier mangelt es oftmals am Sicherheitsbewusstsein, da die mediale Berichterstattung weitestgehend den Computer im Fokus hat. Sollen solche Funktionen genutzt werden, sind die erforderlichen Schutzmaßnahmen auch an Mobiltelefonen zu ergreifen.

Aber auch bisher als „sicher“ geltende Übertragungsmedien (Telefon) können in Verbindung mit der Nutzung neuer Übertragungswege (Internet) zu Quellen von Sicherheitsrisiken werden. So ist beim Telefonieren über das Internet (Voice-over-IP) dieser Übertragungsweg nicht per se als sicheres Übertragungsmedium im Sinne der klassischen Telefonleitung zu betrachten. Die Nutzung dieses Transportverfahrens erfordert weitere Schutzmaßnahmen. Diese umfassen einerseits den Schutz der eigenen Infrastruktur, was bedeutet, dass Voice-over-IP-Telefonanlagen in das Gesamtsicherheitskonzept unbedingt einzubeziehen sind. Ist die Vertraulichkeit der Kommunikation zu gewährleisten, sind die Verschlüsselungseinstellungen beim Anlagenbetreiber bzw. beim Kommunikationsprovider zu erfragen oder ggf. eigene Maßnahmen zur Verschlüsselung zu ergreifen.

14.6 Verhinderung von Datenschutzgefährdungen durch Sicheres Löschen von Datenträgern

Eine weitere mögliche Quelle von Gefährdungen des Datenschutzes kann der zunehmende Einsatz der digitalen Speichertechnik in heutiger Bürotechnik sein. Besonders bei digitalen Fax-Geräten, Kopierern, Mobiltelefonen kann das Vorhandensein von Festplatten und anderen Permanentspeichern (z. B. Flash-Memory) zu einer dauerhaften Speicherung teilweise auch sehr sensibler Daten führen. Die Daten bleiben bis zur physischen Überschreibung durch aktuelle Daten auf dem Speichermedium erhalten. Insbesondere bei Leasing-Rückgaben und Aussonderung dieser Geräte ist ein unerwünschter Informationsabfluss zu verzeichnen. In dieser Hinsicht verweise ich auf Gefahren bzgl. einer Zweitverwertung von Festplatten (siehe entsprechende Mitteilungen in der Presse über das Angebot von Festplatten mit brisantem Inhalt bei Ebay). Aber auch die zunehmende mobile Nutzung moderner Kommunikationsmittel kann Datenschutzgefahren verursachen. So werden z. B. Faxmitteilungen bei Versand an das Handy/Blackberry auf Servern zwischengespeichert. Über Datensicherungen der betreffenden Server kann der Lebenszyklus dieser Daten u. U. sehr langfristig sein. Der sorgfältigen Auswahl des Providers, dessen Dienste genutzt werden sollen, kommt dabei eine große Bedeutung zu.

Dies alles ist vorab bei der Erstellung von Sicherheitskonzepten zu beachten, wenn in dem Verfahren Daten mit erhöhtem Schutzbedarf verarbeitet werden.

Da meist nur Spezialsoftware in der Lage ist, die gespeicherten Informationen von diesen Speichermedien zuverlässig zu löschen (mit entsprechenden Kosten), rege ich den Ausbau und die anschließende mechanische Zerstörung dieser Speichermedien (zumindest bei Aussonderungen) an. Auch teilweise defekte Speichermedien dürfen nicht bedenkenlos entsorgt werden, da auch Teilbereiche noch lesbare Daten enthalten können.

Auf keinen Fall dürfen diese Geräte unbehandelt einer Zweitverwendung zugeführt werden!

Zur weitergehenden Information verweise ich auf die Orientierungshilfe „Sicheres Löschen magnetischer Datenträger“ (Grundlagen, Werkzeuge und Empfehlungen aus Sicht des Datenschutzes erstellt vom Arbeitskreis „Technische und organisatorische Datenschutzfragen“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder) auf www.datenschutz.sachsen.de.

14.7 Kein IT-Sicherheitskonzept beim Einsatz einer Hochschulverwaltungssoftware

Aufgrund einer Eingabe habe ich Informationen zum Einsatz der Hochschulverwaltungssoftware und zu den konkreten personellen, technischen und organisatorischen Maßnahmen zur Gewährleistung des Datenschutzes gemäß § 9 Abs. 2 SächsDSG von der Hochschulleitung angefordert. Weitere Auskünfte wurden mir auf meine Fragen zur Vorabkontrolle, zum Verzeichnis automatisierter Verarbeitungsverfahren gemäß § 10 SächsDSG, Beteiligung des behördlichen Datenschutzbeauftragten und zum IT-Sicherheitskonzept erteilt.

Die Auswertung der Informationen ergab, dass beim Betrieb der Hochschulverwaltungssoftware umfangreiche technisch-organisatorische Einzelmaßnahmen zur Gewährleistung des Datenschutzes umgesetzt wurden, ohne diese in einem IT-Sicherheitskonzept zu erfassen, wie es für das umfangreiche Datenverarbeitungsverfahren erforderlich wäre. Das wurde auch vom behördlichen Datenschutzbeauftragten mehrfach beanstandet.

Nunmehr besteht die Absicht, ein IT-Sicherheitskonzept nach Beauftragung einer Fremdfirma in Zusammenarbeit mit den zuständigen Mitarbeitern der Hochschule zu erstellen.

Die bisher schon beim Betrieb der Hochschulverwaltungssoftware umgesetzten Einzelmaßnahmen sind in einem IT-Sicherheitskonzept zu erfassen, die datenschutzrechtlichen Anforderungen zu prüfen, die Risiken zu bewerten und zu untersuchen, ob eventuell zusätzliche Sicherheitsmahnahmen die Gewährleistung des Datenschutzes erfordern. Das IT-Sicherheitskonzept ist regelmäßig zu aktualisieren und weiter zu entwickeln. Dabei ist zu beachten, dass diese Maßnahmen nach dem Stand der Technik die Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität, Revisionsfähigkeit und Transparenz personenbezogener Daten sicherstellen (§ 9 SächsDSG).

Aufgrund der engen Verknüpfungen von Datenschutz und IT-Sicherheit können sich Datenschutz- und Datensicherheitskonzepte selbstverständlich an den handlungsbezogenen Beiträgen der „IT-Grundschutz-Kataloge“ (zuvor IT-Grundschutzhandbuch) des BSI orientieren.

Die Standardsicherheitsmaßnahmen sind jedoch für einen mittleren Schutzbedarf festlegt. Im Einzelfall und in Abhängigkeit von der Sensibilität personenbezogener Daten muss dann geprüft werden, ob die Maßnahmen zur Vertraulichkeit, Integrität, Verfügbarkeit und Revisionsfähigkeit, die bereits Forderungen des IT-Grundschutzes

sind, auch den Anforderungen des Datenschutzes entsprechen. Außerdem sind zusätzlich Maßnahmen zur Authentizität personenbezogener Daten und zur Transparenz der Datenverarbeitung nach der Erforderlichkeit und dem jeweiligen Stand der Technik zu treffen.

Die Erstellung eines umfassenden IT-Sicherheitskonzeptes - nicht nur bezogen auf die hier betrachtete Einführung der Hochschulverwaltungssoftware - muss vordringliche Aufgabe der Hochschulleitung bleiben, weil dies die Voraussetzung für eine ordnungsgemäße und datenschutzgerechte Datenverarbeitung schafft.

Als weitere Maßnahme zur Verbesserung der IT-Sicherheitsstrategie an der Hochschule ist die Gründung eines Security Management Teams geplant. Dieses Team sollte auf dem Gebiet der Sicherheit eng mit dem behördlichen Datenschutzbeauftragten der Hochschule zusammenarbeiten, vor allem dann, wenn neue Verfahren eingeführt werden sollen.

Bei meiner Stellungnahme gegenüber der Hochschulleitung wurde auch beanstandet, dass keine Regelungen oder Sicherheitsrichtlinien zur Passwortverwaltung vorhanden waren. Diese sollten unverzüglich, ohne auf die Erstellung des Sicherheitskonzeptes zu warten, entwickelt und in Kraft gesetzt werden.

Passwörter sind auch heute noch das am meisten genutzte Verfahren zur Authentifizierung von Benutzern. Mit der Eingabe des geheimen Passwortes weist sich der Benutzer gegenüber dem informationsverarbeitenden System als berechtigt aus. Meist sichert einzig und allein das geheime Passwort den geforderten Zugriffsschutz, weil die Benutzerkennung mit dem Familiennamen oder anderen bekannten Bezeichnungen übereinstimmt.

Der Versuch, sich im Netz als ein anderer Benutzer auszugeben und Passworte auszuprobieren, wird dann nicht bemerkt, wenn Fehlanmeldungen nicht protokolliert oder protokollierte Fehlversuche im Log-Protokoll nicht regelmäßig ausgewertet werden oder keine Sperrung der Benutzerkennung nach einer bestimmten Anzahl von Fehlversuchen erfolgt.

Deshalb müssen Mindestanforderungen oder Sicherheitsrichtlinien zur Passwortverwaltung (z. B. Mindestlänge, zu nutzender Zeichenvorrat, Gültigkeitsdauer, Zahl der möglichen Fehlversuche, erfolglose Login-Versuche protokollieren und auswerten) für die an der Hochschule eingesetzten Systeme festgelegt werden.

Von Bedeutung wird auch sein, wie von der jeweiligen Software die Einhaltung der Passwort-Richtlinien geprüft wird. Sollte dies bei der Hochschulverwaltungssoftware nicht der Fall sein, müsste die Hochschulleitung im Rahmen ihrer Möglichkeiten auf die Weiterentwicklung Einfluss nehmen und dies als Anforderung gegenüber den Entwicklern benennen.

Empfehlungen zum Gebrauch von Passwörtern können aus 11/14.4 oder der „Orientierungshilfe Empfehlungen zur Passwortgestaltung und zum Sicherheitsmanagement“ unter Arbeitshilfen auf meiner Web-Seite (www.datenschutz.sachsen.de) entnommen werden.

Überdies sollte im IT-Sicherheitskonzept festgelegt werden, wer die Protokolle wann wie auswertet und wann die protokollierten Daten zu löschen sind. Eine regelmäßige und stichprobenweise Auswertung der Protokolldaten ist unbedingt erforderlich, um zeitnah Unregelmäßigkeiten aufdecken und vermutete Missbrauchsversuche erkennen zu können. Daher ist die Auswertung der Protokolle nur im Fehlerfall nicht ausreichend.

Mit den beschriebenen technisch-organisatorischen Maßnahmen, der personellen Verstärkung der DV-Gruppe und der geplanten Erstellung eines IT-Sicherheitskonzeptes sowie der Gründung eines Security Management Teams sollte die Hochschulverwaltungssoftware an der sächsischen Hochschule ordnungsgemäß und datenschutzgerecht betrieben werden können. Ich werde den Sachstand zu gegebener Zeit erneut prüfen.

14.8 Verfahrensverzeichnis nach § 10 Abs. 4 SächsDSG für die Nutzung der behördlichen Telekommunikationsanlagen sowie Bemerkungen zu Datenschutzgefahren beim Einsatz moderner Digitaltechnik

In letzter Zeit erhielt ich nach § 10 Abs. 4 SächsDSG mehrere Verfahrensverzeichnisse, die im Nachgang zu meinen Vor-Ort-Kontrollen und ohne ausreichende Beachtung der auf meiner Web-Seite gemachten diesbezüglichen Äußerungen (www.datenschutz.sachsen.de, Rubrik Datenschutz und Recht) erstellt wurden.

Insbesondere wurde dabei nicht die notwendige *Vorabkontrolle des Verfahrens* beachtet; d. h. ob die *Datenverarbeitung zulässig* und die *vorgesehenen Maßnahmen* nach § 9 SächsDSG *ausreichend* sind. Der Sächsische Datenschutzbeauftragte ist nach § 10 Abs. 4 SächsDSG für die Vorabkontrolle zuständig (bei Nichtbestellung

eines Datenschutzbeauftragten der öffentlichen Stelle). Dies ist bei wesentlichen Änderungen bzw. Neugestaltungen der automatisierten Auswertung der Verarbeitung der Verbindungsdaten zu berücksichtigen.

Häufig wurde bei der Erstellung des geforderten Verfahrensverzeichnisses nur auf das automatisierte Verfahren zur Gebührenauswertung der erlaubten privaten Nutzung dienstlicher Telefonapparate abgestellt. Dabei bietet es sich aus meiner Sicht an, diese Datenverarbeitung mit der Auswertung der personenbezogenen Daten der dienstlich veranlassten Telekommunikation in einem Verfahrensverzeichnis zusammenzufassen.

Folgende datenschutzrechtliche Bemerkungen zur *Anlage der Bekanntmachung nach § 10 SächsDSG* (vgl. 16.1.1) sollen eine Hilfe bei der Erstellung des Verfahrensverzeichnisses darstellen.

Zu Punkt 2: *Bezeichnung des Verfahrens*

Wie in meiner Bekanntmachung unter Punkt II.2 aufgeführt, bietet es sich an, einen möglichst sprechenden Begriff für das *gesamte* Verarbeitungsverfahren zu wählen.

Zu Punkt 3: *Zweck und Rechtsgrundlage der Verarbeitung personenbezogener Daten*

Bei der Nennung der gesetzlichen Grundlagen nach § 4 Abs. 1 SächsDSG ist das Telekommunikationsgesetz in der jeweils aktuellen Fassung zu nennen. In diesem Zusammenhang ist zu beachten, dass die Bundesregierung das Telekommunikationsgesetz demnächst um Regelungen bzgl. Terrorabwehr ergänzen wird. Demzufolge ist die zukünftig verlängerte gesetzliche Speicherungsdauer für alle Verbindungsdaten auch in den folgenden Punkten des Verfahrensverzeichnisses zu beachten und diese nach In-Kraft-Treten der Gesetzesnovelle nach § 10 Abs. 3 SächsDSG zu aktualisieren.

Ebenfalls ist das Sächsische Datenschutzgesetz als Rechtsgrundlage zu nennen. Dienstanweisungen sind *nicht* als alleinige Grundlage für die Erstellung eines Verfahrensverzeichnisses i. S. d. § 4 Abs. 1 Nr. 1 SächsDSG anzusehen.

Zu Punkt 5: *Empfänger und Art zu übermittelnder Daten*

Hier sind nicht nur die Mitarbeiter der betreffenden Behörde mit den Daten des Einzelverbindungsnachweises (für private Verbindungsdaten) zu nennen, sondern auch die Mitarbeiter der jeweiligen Behörde, die diese Einzelverbindungsnachweise zusammenstellen sowie ihre Abrechnung kontrollieren. Sofern die Mitarbeiter zu

Korrekturzwecken (Markierung vergessener Deklarierung von Privat- als Dienstverbindungen) auch die Dienstverbindungen nochmals zur Einsichtnahme erhalten, müssen diese bei der Empfängergruppe „Mitarbeiter“ genannt werden.

Es sind des Weiteren die Verantwortlichen zu nennen, die die erlaubte Kontrolle der Dienstverbindungen auf der Grundlage von vorher festgelegten Regelungen durchführen bzw. die Personen, die eventuelle Verstöße arbeitsrechtlich sanktionieren.

Die jeweiligen Daten sind konkret für die betroffene Personengruppe aufzuführen.

Auch hier bietet es sich an, für diese Personengruppen eine möglichst für sich selbst sprechende Bezeichnung zu finden.

Zu Punkt 7: *Regelfristen für die Löschung der Daten*

Die bisher in § 97 Abs. 3 TKG geregelte Höchstspeicherdauer von sechs Monaten für private Verbindungsdaten wird sich entsprechend der neuen gesetzlichen Regelung bemessen. Verbindungsdaten dienstlich veranlasster Gespräche sind gemäß § 20 SächsDSG zu löschen, wenn sie nicht mehr für die Aufgabenerfüllung erforderlich sind.

Zu Punkt 8: *Personelle, technische, und organisatorische Maßnahmen*

Für die Darlegung getroffener personeller, technischer und organisatorischer Maßnahmen bzgl. des Datenschutzes bitte ich die Äußerungen auf meiner Web-Seite zu beachten (Bekanntmachung zum Verzeichnis automatisierter Verarbeitungsverfahren, § 10 SächsDSG - hier besonders meine Hinweise in Bezug auf *Vertraulichkeit, Integrität, Verfügbarkeit* usw., vgl. 16.1.1).

Besonders ist bei den zu nennenden behördlichen Datensicherheitsmaßnahmen darauf abzustellen, dass diese im Kontext der IT-Sicherheitsmaßnahmen der Behörde stehen müssen. Ich verweise in diesem Zusammenhang auf die Verwendung sicherer Passwortrichtlinien, der Protokollierung und Auswertung von Sicherheitseinstellungen moderner Betriebssysteme, sowie auf Sicherheitsmaßnahmen zur Zutrittssicherung sicherheitsrelevanter Räume und der sicheren Aufbewahrung mobiler Datenträger.

Aber auch Schutzmaßnahmen, z. B. vor Hochwasser - bei Unterbringung der EDV im Keller - Rohrbruch oder Stromausfall, sind zu nennen. Des Weiteren verweise ich erneut auf die konkrete und strikte Anwendung von Regeln bei der Fernwartung. Zugriffe der Fernwartung müssen stets nachvollziehbar (wer hat was, weshalb, wann

geändert) dokumentiert werden. Diese Fernzugriffe sind durch geeignete technische Maßnahmen gesichert auszuführen.

Der Einsatz moderner mobiler Kommunikationsmittel (z. B. Mobiltelefone) erfolgt bei einer zunehmend größeren Anzahl von Behörden. Aber auch bei der mitunter erlaubten privaten Nutzung dieser Geräte gilt es den Datenschutz zu beachten und das Verfahren zur Abrechnung der privaten Telefonate datenschutzgerecht zu gestalten. Besonders wichtig ist, dass das Fernmeldegeheimnis nach § 88 TKG dabei (Inhalt und nähere Umstände der Telekommunikation - wer hat wann, mit wem, von wo, wie lange, wie und wie oft kommuniziert) beachtet wird.

Hier bietet sich an, dass die Einzelverbindungsnachweise des betreffenden Mobiltelefons zunächst dem Mitarbeiter zugesandt werden. Dieser erstellt daraus eine Abrechnung seiner privaten Verbindungskosten und schwärzt danach die Angaben zu den Privatverbindungen. Danach reicht er diese Abrechnung bei der Kasse ein und übergibt die geschwärzte Liste in das weitere Verfahren zur Begleichung der restlichen, dann dienstlich veranlassten Kosten.

Eine weitere datenschutzgerechte Möglichkeit mit Wahrung des Fernmeldegeheimnisses wäre auch die Nutzung der Online-Telefonrechnung. Die Rechnung könnte direkt an die E-Mail-Adresse des Mitarbeiters gesandt bzw. online durch diesen abgerufen werden. Der Mitarbeiter druckt dann den Einzelverbindungsnachweis und die Gesamtrechnung aus, schwärzt seine Privatverbindungen auf dem Einzelverbindungsnachweis, gibt diese Belege in der Kasse ab und begleicht seine privaten Telefonate. Diese derart von den Privatverbindungen „bereinigten“ Verbindungsnachweise können durch Vorgesetzte geprüft werden.

Die Mitarbeiter sind ergänzend darauf hinzuweisen, dass die getroffenen Bestimmungen der öffentlichen Stelle für die Nutzung von E-Mail/Internet/EDV ebenfalls für die Nutzung des betrieblichen Mobiltelefons gelten können, wenn derartige Funktionen an den Mobiltelefonen genutzt werden. In diesem Fall wäre dann auch die mögliche Installation von Programmen sowie die Konfiguration von Multimediadiensten (E-Mail-Abruf, Ablage von Passwörtern, Fax-Einstellungen, SMS-Benachrichtigungen) auf derartigen Geräten zu regeln.

In manchen Behörden ist der private Fax-Versand erlaubt. In dieser Hinsicht ist aber auch eine Regelung für den privaten Fax-Empfang in einer behördlichen Regelung vorzugeben.

Entweder wird der private Fax-Empfang generell untersagt oder nach dem Bekanntwerden des privaten Charakters eines eingegangenen Telefaxes wird dieses in einem Umschlag verschlossen und dem Empfänger zur Kenntnis gegeben.

14.9 Online Durchsuchung

Die vom BMI beabsichtigte heimliche Überwachung so genannter „Informationstechnischer Systeme“ sehe ich mit großer Skepsis. Allein die Unschärfe in der Definition der zu überwachenden Gerätschaften lässt die Dimension des Vorhabens erahnen und macht deutlich, dass über dieses Vorhaben eine breite gesellschaftliche Diskussion geführt werden muss. Die Datenschutzbeauftragten des Bundes und der Länder haben ihre Position in einer Entschließung (vgl. 16.2.26) im Rahmen der 74. Konferenz bekräftigt und werden dieses Vorhaben auch in Zukunft kritisch begleiten.

Zu den technischen Aspekten der Online-Durchsuchung hat der Arbeitskreis Technik der Datenschutzbeauftragten des Bundes und der Länder ein Dokument verabschiedet, das mögliche Abläufe und technische Verfahren erläutert und aus technischer Sicht bewertet (vgl. 16.2.27).

15 Vortrags- und Schulungstätigkeit für behördliche Datenschutzbeauftragte

In meinem 12. Tätigkeitsbericht habe ich angekündigt, für die nach § 11 SächsDSG bestellten Datenschutzbeauftragten öffentlicher Stellen (von denen es mittlerweile deutlich über 400 gibt) spezielle Schulungen durchzuführen. Den Anfang machten die beiden Veranstaltungen am 19. und 20. Dezember 2006. Zu diesen erhielt ich zahlreiche Rückmeldungen, die in die weitere Gestaltung der Vorträge einfließen werden. So werde ich die Schulungen zukünftig fachspezifischer und damit auch mit einem kleineren Teilnehmerkreis durchführen. Anregungen aus dem Kreis der behördlichen Datenschutzbeauftragten hinsichtlich zu behandelnder Themen nehme ich auch weiterhin dankbar entgegen.

Nach dem Ende des Berichtszeitraums habe ich das ebenfalls angekündigte interne Forum für die Datenschutzbeauftragten öffentlicher Stellen eingerichtet. Diese können hier als geschlossene Benutzergruppe spezielle Fragen und Probleme zum Datenschutz untereinander diskutieren - und Erfahrungen austauschen. Für die Anmeldung sowie bei Problemen, die im Zusammenhang mit der Nutzung des Forums auftreten, steht den behördlichen Datenschutzbeauftragten unter der Telefonnummer (03578) 33 1717 oder auch unter der E-Mail-Adresse circa@statistik.sachsen.de ein „User-Help-Desk“ zur Verfügung.

16 Materialien

16.1 Bekanntmachungen

16.1.1 Bekanntmachung des Sächsischen Datenschutzbeauftragten zum Verzeichnis automatisierter Verarbeitungsverfahren (§ 10 SächsDSG)

vom 11. März 2004
aktualisierte Fassung vom 1. Februar 2007

I Führung eines Verfahrensverzeichnisses

Nach § 10 Abs. 1 Satz 1 des Sächsischen Datenschutzgesetzes (SächsDSG) hat jede Daten verarbeitende Stelle ein Verzeichnis über die bei ihr eingesetzten automatisierten Verarbeitungsverfahren zu führen.

Daten verarbeitende Stelle (innerhalb des in § 2 SächsDSG definierten Anwendungsbereichs) ist jede öffentliche Stelle i. S. v. § 2 Abs. 1 und 2 SächsDSG, die personenbezogene Daten für sich selbst verarbeitet oder durch andere im Auftrag verarbeiten lässt (vgl. § 3 Abs. 3 SächsDSG). „Stellen“ sind dabei Verwaltungseinheiten, die gesetzlich zugewiesene, datenschutzrechtlich zweckbestimmt abgeschottete Aufgaben erfüllen (funktionale Stelle). In einer - im organisatorischen Sinn einheitlichen - Gemeindeverwaltung sind beispielsweise Meldeamt und Personalamt jeweils Stellen im funktionalen Sinn.

Verarbeitung i. S. d. Gesetzes ist das Erheben, Speichern, Verändern, Anonymisieren, Übermitteln, Nutzen, Sperren und Löschen personenbezogener Daten (vgl. § 3 Abs. 2 SächsDSG). Eine automatisierte Verarbeitung personenbezogener Daten liegt nach § 3 Abs. 5 SächsDSG vor, wenn diese durch den Einsatz eines elektronischen Datenverarbeitungssystems (Rechner und Software) programmgesteuert durchgeführt wird. Ein automatisiertes Verfahren ist die Gesamtheit der einzelnen automatisierten Verarbeitungen mit einem bestimmten Verwendungszweck.

Die Pflicht zum Führen des Verfahrensverzeichnisses entsteht dort, wo das Verfahren eingesetzt wird. Der Spezialfall des § 8 Abs. 3 SächsDSG bei automatisierten Abrufverfahren ist zu beachten. Gerichte führen die Verzeichnisse nur in Justizverwaltungsangelegenheiten (§ 10 Abs. 2 SächsDSG); ihre Recht sprechende Tätigkeit ist ausgenommen.

Für Verfahren i. S. v. § 10 Abs. 5 SächsDSG (zur Unterstützung allgemeiner Bürotätigkeit oder durch Rechtsvorschrift erstellte Register zur Information der Öffentlichkeit) ist ein Verzeichnis nicht zu führen.

Der bisherige Teil „Geräteverzeichnis“ ist entfallen, da er aufgrund der EG-Datenschutzrichtlinie nicht mehr erforderlich war und ein solches Geräteverzeichnis ohnehin i. d. R. andernorts - meist in der IT-Abteilung - geführt wird.

II Inhaltliche Erläuterungen zum Verfahrenverzeichnis

Es wird empfohlen, für die Beschreibungen das in der Anlage zu dieser Bekanntmachung abgedruckte Muster zu verwenden. Für jedes Verfahren ist ein gesondertes Datenblatt anzulegen. Beim Ausfüllen sollte beachtet werden:

1. Bezeichnung und Anschrift der Daten verarbeitenden Stelle

Es ist die Stelle (im funktionalen Sinn) zu bezeichnen, bei der die Verarbeitung erfolgt (z. B. das Einwohnermeldeamt der Stadt). Wird das Verfahren von mehreren Stellen genutzt, ist - soweit möglich - eine zusammenfassende Bezeichnung anzugeben oder sind die Stellen einzeln zu nennen.

2. Bezeichnung des Verfahrens

Als Bezeichnung des Verfahrens ist der allgemein übliche oder ein möglichst „sprechender“ Begriff zu wählen. Darüber hinaus sollten Angaben zur eingesetzten Software (z. B. Bezeichnung, Version, Hersteller) gemacht werden.

3. Zweck und Rechtsgrundlage der Verarbeitung personenbezogener Daten

Es ist der Zweck der Datenverarbeitung zu beschreiben (z. B. Lohn- und Gehaltsabrechnung) sowie die entsprechende gesetzliche Ermächtigung gemäß § 4 Abs. 1 SächsDSG. Rechtsgrundlagen sind eindeutig zu bezeichnen oder hinreichend zu beschreiben.

4. Betroffene Personengruppen und Art der zu verarbeitenden Daten

Es sind die den betroffenen Personenkreis kennzeichnenden Merkmale aufzunehmen (z. B. „Wohngeldempfänger“, „Fahrerlaubnisinhaber“). Soweit sich der betroffene Personenkreis aus einem Verfahren im Sinne von § 10 SächsDSG ergibt (z. B. „Einwohnermeldekartei“), kann dieser Bezug verwendet werden. Weiterhin ist die Datenart (z. B. Meldedaten) ggf. unter Nennung der einzelnen Bestandteile des Datensatzes anzugeben (z. B. Personaldaten - Name, Vorname, akademischer Grad, Personalnummer, Familienstand etc.). Eine möglichst präzise Beschreibung ist erforderlich.

5. Empfänger und Art zu übermittelnder Daten

Es sind die zur Weitergabe an Dritte vorgesehenen Daten wie in Nr. 4 zu beschreiben (vgl. § 3 Abs. 4 SächsDSG). Zusätzlich ist der jeweilige Empfänger anzugeben. Ist der Empfänger eine einzelne Stelle oder Person, ist diese identifizierbar anzugeben; sind es mehrere (z. B. die Meldebehörden im Landkreis), genügt eine zusammenfassende Bezeichnung.

6. Beabsichtigte Übermittlung in Drittländer

Im Fall einer Übermittlung in Drittländer sind die Spezialvorschriften des § 17 SächsDSG zu beachten. Anzugeben sind hier der Empfänger, die Rechtsgrundlage und der Umfang der Übermittlung.

7. Regelfristen für die Löschung der Daten

Nach § 20 Abs. 1, 2 SächsDSG sind personenbezogene Daten zu löschen, wenn deren Speicherung unzulässig ist oder ihre Kenntnis zur Aufgabenerfüllung nicht mehr erforderlich ist - und die Löschung nicht aus den in § 20 Abs. 3, 4 SächsDSG aufgeführten Gründen zu unterbleiben hat. Gemäß § 10 Abs. 1 Nr. 9 SächsDSG sind hierfür Regelfristen vorzusehen. Soweit sich solche nicht aus dem Gesetz ergeben (z. B. § 43 Abs. 1a SächsPolG), sind sie gegebenenfalls durch die verarbeitende Stelle unter Beachtung der gesetzlichen Aufbewahrungsfristen festzulegen (so auch ausdrücklich z. B. § 43 Abs. 4 SächsPolG).

8. Personelle, technische, und organisatorische Maßnahmen

Sofern nach § 10 Abs. 4 SächsDSG die Pflicht zur Durchführung einer Vorabkontrolle bestand, ist zunächst anzugeben, ob dies geschehen ist.

Weiterhin sind die gemäß § 9 SächsDSG getroffenen Kontrollmaßnahmen jeweils zu beschreiben. Dazu können ggf. vorhandene Datenschutzkonzepte und Dienstvereinbarungen oder -anweisungen vorgelegt werden.

Dabei kann Vertraulichkeit z. B. neben einer Sicherung durch Schließsysteme auch durch differenzierte Zugangs- und Zugriffsberechtigungen, die durch Passwörter oder Chipkarten abgesichert werden, erreicht werden. Zur Sicherstellung der Integrität können Schreibrechte sowie die Nutzung von Schnittstellen und mobilen Medien eingeschränkt oder personenbezogene Daten verschlüsselt werden. Regelmäßige Datensicherungen sowie Ausfallsicherungen dienen der Verfügbarkeit der für die Datenverarbeitung erforderlichen Daten sowie der entsprechenden Hard- und

Software. Authentizität kann durch die Verwendung von elektronischen Signaturen, Passwörtern oder Chipkarten erreicht werden. Zur Sicherstellung der Revisionsfähigkeit sind die vorgenommenen Verarbeitungen zu protokollieren. Transparenz wird schließlich über detaillierte Dokumentationen der Verfahren erreicht, aus denen sich ergibt, welche Daten wie verarbeitet werden, wie die Rechte Betroffener gewahrt werden bzw. wie diese ihre Rechte selbst wahrnehmen können.

Soweit sich zu den Nummern 1 bis 8 Anlagen erforderlich machen, sind diese beizufügen.

III Mitteilungspflicht an den Sächsischen Datenschutzbeauftragten

Zu führen ist das Verzeichnis grundsätzlich bei der Stelle (im funktionalen Sinn), bei der die Verarbeitung stattfindet (§ 10 Abs. 1 Satz 3 SächsDSG). Jedoch ist es zweckmäßig und regelmäßig zu empfehlen, dass die Verzeichnisse bei der jeweiligen Behörde zentral zusammengeführt und sodann dem Sächsischen Datenschutzbeauftragten gebündelt übersandt werden.

Die Vorlage hat vor der erstmaligen Inbetriebnahme eines Verfahrens zu erfolgen (§ 10 Abs. 3 Satz 1 SächsDSG). Darüber hinaus ist das aktualisierte Verfahrensverzeichnis dem Sächsischen Datenschutzbeauftragten zum 1. März jeden Jahres zuzuleiten (§ 10 Abs. 3 Satz 2 SächsDSG). Dabei ist es nicht notwendig, dass alle Verfahrensverzeichnisse erneut übermittelt werden. Sofern diese sich nicht geändert haben, ist es vielmehr ausreichend, wenn auf die bereits übersandten Verzeichnisse Bezug genommen wird und nur die geänderten Verfahrensverzeichnisse zugeleitet werden.

Eine Mitteilungspflicht entfällt, sofern ein Datenschutzbeauftragter, der den Anforderungen des § 11 SächsDSG entspricht, bestellt ist (§ 10 Abs. 3 Satz 3 SächsDSG). Dann führt dieser das Verfahrensverzeichnis.

Dresden, den 1. Februar 2007
Der Sächsische Datenschutzbeauftragte
Schurig

Anlage

Verfahrensverzeichnis

(Mitteilung und Beschreibung der Verfahren nach § 10 SächsDSG für das Register beim Sächsischen Datenschutzbeauftragten nach § 31 SächsDSG)

Der Sächsische Datenschutzbeauftragte
Bernhard-von-Lindenau-Platz 1
01067 Dresden

Die Beschreibung wurde erstellt am:

Die Beschreibung wurde aktualisiert am:

Stempel, Datum, Unterschrift

Bitte ggf. Anlage(n) beifügen

1. Bezeichnung und Anschrift der Daten verarbeitenden Stelle

2. Bezeichnung des Verfahrens

3. Zweck und Rechtsgrundlage der Verarbeitung personenbezogener Daten

Zweck	Rechtsgrundlage

4. Betroffene Personengruppen und Art der zu verarbeitenden Daten

Personengruppe	Art der zu verarbeitenden Daten

5. Empfänger und Art zu übermittelnder Daten

Empfänger	Art der zu übermittelnden Daten

6. Beabsichtigte Übermittlung in Drittländer gemäß § 17 SächsDSG (Empfänger, Rechtsgrundlage und Umfang der Übermittlung)

7. Regelfristen für die Löschung der Daten

Art der Daten	Zeitraum

8. Personelle, technische und organisatorische Maßnahmen gemäß § 9 SächsDSG

Vorabkontrolle (§ 10 Abs. 4 SächsDSG) durchgeführt? □ ja □ nein

Wie ist sichergestellt, dass

1. nur Befugte personenbezogene Daten zur Kenntnis nehmen können (Vertraulichkeit),

2. personenbezogene Daten während der Verarbeitung unversehrt, vollständig und aktuell bleiben (Integrität),

3. personenbezogene Daten zeitgerecht zur Verfügung stehen und ordnungsgemäß verarbeitet werden können (Verfügbarkeit),

4. jederzeit personenbezogene Daten ihrem Ursprung zugeordnet werden können (Authentizität),

5. festgestellt werden kann, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat (Revisionsfähigkeit),

6. die Verfahrensweisen bei der Verarbeitung personenbezogener Daten vollständig, aktuell und in einer Weise dokumentiert sind, dass sie in zumutbarer Zeit nachvollzogen werden können (Transparenz)?

16.1.2 Bekanntmachung des Sächsischen Datenschutzbeauftragten zu Datenschutzbeauftragten öffentlicher Stellen (§ 11 SächsDSG)

vom 11. März 2004
aktualisierte Fassung vom 1. Februar 2007

1 Bestellung des Datenschutzbeauftragten

1.1 Ermessensentscheidung

Die Entscheidung über die Bestellung eines Datenschutzbeauftragten nach § 11 Abs. 1 Satz 1 SächsDSG ist durch die öffentliche Stelle selbst nach Ermessen zu treffen. Das Sächsische Datenschutzgesetz sieht für öffentliche Stellen (§ 2 Abs. 1 und 2 SächsDSG) keine Pflicht, sondern nur die Möglichkeit der Bestellung eines Datenschutzbeauftragten vor.

Die Bestellung kann durch die organisationsrechtliche Stelle (Behörde, z. B. eine Gemeinde) erfolgen. Sie umfasst alle funktionalen Stellen gemäß § 2 (z. B. Ordnungsamt, Sozialamt), die dieser organisatorischen Einheit angehören, sofern kein „eingeschränkter Zuständigkeitsbereich“ angegeben ist. Nicht umfasst sind hingegen organisatorisch selbständige Stellen, wie zum Beispiel Eigenbetriebe. Sofern eine Bestellung auch für diese erfolgen soll, ist dies als „erweiterter Zuständigkeitsbereich“ unter Angabe der umfassten Stellen anzugeben.

In größeren Behörden sollten jedoch als unterstützende Maßnahme zur Gewährleistung des Datenschutzes im Sinne von § 9 SächsDSG Datenschutzbeauftragte bestellt werden.

Die Verantwortung für die Einhaltung der datenschutzrechtlichen Vorschriften und die Beachtung des Rechts auf informationelle Selbstbestimmung verbleibt aber auch bei Bestellung eines Datenschutzbeauftragten beim Leiter der öffentlichen Stelle.

1.2 Schriftliche Bestellung und hausinterne Bekanntmachung

Der Datenschutzbeauftragte wird durch ein förmliches an ihn gerichtetes Schreiben bestellt (§ 11 SächsDSG), das bei eigenen Beschäftigten zu den Personalakten zu nehmen ist. Die bloße Erwähnung in einem Geschäftsverteilungsplan genügt nicht.

Die Bestellung sollte allen Mitarbeitern bekannt gegeben werden (z. B. durch Hausmitteilung oder Aushang).

1.3 Persönliche Voraussetzungen (§ 11 Abs. 2 SächsDSG)

Der Datenschutzbeauftragte muss nicht Bediensteter der Stelle sein, § 11 Abs. 1 Satz 3 SächsDSG, möglich ist grundsätzlich auch die Bestellung eines Beschäftigten einer anderen Stelle, z.B. der Aufsichtsbehörde oder einer Nachbargemeinde. Er ist als natürliche Person zu bestellen. In Fällen der Inanspruchnahme externer Dienstleister, die in Datenschutzfragen beraten und die als juristische Personen des Privatrechts auftreten, z. B. einer GmbH, ist ein Mitarbeiter persönlich zu benennen und zu bestellen.

Der Datenschutzbeauftragte muss zuverlässig und fachkundig sein. Sofern er über die fachlichen Qualifikationen (rechtliche und organisatorische Kenntnisse, Sicherheit im Umgang mit den einschlägigen Spezialvorschriften zum Persönlichkeitsschutz im eigenen Fachbereich und dem Sächsischen Datenschutzgesetz, Grundkenntnisse in automatisierter Datenverarbeitung) noch nicht verfügt, muss ihm Gelegenheit gegeben werden, diese zu erwerben. Darüber hinaus hat sich der Datenschutzbeauftragte regelmäßig fortzubilden, um Kenntnis der neuen technischen Entwicklungen und der datenschutzrechtlichen Regelungen zu haben.

Der Datenschutzbeauftragte ist nach § 6 SächsDSG auf das Datengeheimnis und ggf. nach § 1 Verpflichtungsgesetz (bei Nicht-Amtsträgern) schriftlich zu verpflichten.

1.4 Inkompatibilität

Dem Datenschutzbeauftragten kommt gegenüber der Behörde, ggf. auch gegenüber Mitarbeitern und Betroffenen eine koordinierende und beratende - aber bis zu einem gewissen Grad auch eine intern kontrollierende - Funktion zu. Ist der Datenschutzbeauftragte ein Mitarbeiter und - wie zumeist - nebenamtlich tätig, sind daher mögliche Interessenkonflikte mit seinen Hauptaufgaben im Vorfeld auszuschließen. Insbesondere bei Bediensteten aus dem Bereich der Personalverwaltung, des Organisationswesens, der Datenverarbeitung oder des Personalrats ergeben sich regelmäßig Spannungsverhältnisse zur eigentlichen Hauptaufgabe. Unzulässig ist die Bestellung von Mitarbeitern in leitenden Funktionen, die in einem besonderen dienstlichen Näheverhältnis zum Leiter der Stelle/Behördenleiter stehen und deren Bestellung regelmäßig im Übermaß Interessenkonflikte hervorrufen würde (z. B. bei Stellvertretern des Leiters, Personalamtsleitern usw.). Dasselbe gilt auch für andere Funktionen, bei denen originär personenbezogene Daten verarbeitet werden, z. B. bei Mitgliedern von Personalvertretungen.

1.5 Bestellung eines Datenschutzbeauftragten für mehrere Stellen

Nach § 11 Abs. 1 Satz 3 SächsDSG können mehrere Stellen einen gemeinsamen Datenschutzbeauftragten bestimmen. Dieser ist dann von jeder organisationsrechtlichen Stelle, für die er bestellt wurde, an den Sächsischen Datenschutzbeauftragten zu melden.

1.6 Berufung eines Vertreters des Datenschutzbeauftragten

Die Bestellung eines Stellvertreters des Datenschutzbeauftragten als Abwesenheitsvertreter ist gemäß § 11 Abs. 1 SächsDSG zulässig.

Möglich ist darüber hinaus, dass der Datenschutzbeauftragte über Mitarbeiter verfügt, die ihm zuarbeiten und unterstützende Hilfstätigkeiten erledigen. Verarbeiten diese Mitarbeiter personenbezogene Daten, so ist dabei zu beachten, dass insbesondere die Schweigepflicht nach § 11 Abs. 5 SächsDSG nur für den Datenschutzbeauftragten selbst normiert ist.

1.7 Mitteilung über die Bestellung an den Sächsischen Datenschutzbeauftragten

Nach § 11 Abs. 1 Satz 6 SächsDSG ist der Sächsische Datenschutzbeauftragte innerhalb eines Monats von der Bestellung zu unterrichten. Es wird empfohlen, dazu die in der Anlage zu dieser Bekanntmachung abgedruckten Muster zu verwenden und diese zusammen mit einer Kopie des Bestellungsschreibens an den Sächsischen Datenschutzbeauftragten zu übersenden. In allen Fällen, in denen keine Mitteilung erfolgt, geht der Sächsische Datenschutzbeauftragte davon aus, dass kein Datenschutzbeauftragter im Sinne von § 11 SächsDSG bestellt worden ist.

Mitteilungspflichtig sind gemäß § 2 Abs. 1 SächsDSG alle öffentlichen Stellen sowie gemäß § 2 Abs. 2 SächsDSG alle juristischen Personen des Privatrechts (Stiftungen, Vereine, GmbHs, AGs usw.), die durch öffentliche Stellen mehrheitlich beherrscht werden (Die juristische Person des Privatrechts muss dabei nicht mehrheitlich von einer öffentlichen Stelle beherrscht werden.) und nicht am Wettbewerb teilnehmen (§ 2 Abs. 3 SächsDSG).

2 Gesetzliche Aufgaben und Befugnisse

2.1 Gesetzliche Aufgaben

Die nach § 11 Abs. 1 Satz 1 SächsDSG bestellten Datenschutzbeauftragten

a) überwachen die Einhaltung der Datenschutzvorschriften bei der Planung, vor der Einführung von und während der Anwendung automatisierter Verfahren (§ 11 Abs. 4 Nr. 1 SächsDSG),

b) geben Hinweise an andere Mitarbeiter in Datenschutzfragen (§ 11 Abs. 4 Nr. 2 SächsDSG),

c) führen das Verzeichnis automatisierter Verarbeitungsverfahren (§ 11 Abs. 4 Nr. 3 SächsDSG),

d) prüfen nach § 11 Abs. 4 Nr. 4 SächsDSG in Vorabkontrollen die in ihren Stellen vorgesehenen

- automatisierten Abrufverfahren nach § 8 SächsDSG (vgl. § 10 Abs. 4 Nr. 1 SächsDSG),

- automatisierten Verfahren, in denen sensible Daten im Sinne von § 4 Abs. 2 SächsDSG verarbeitet werden (vgl. § 10 Abs. 4 Nr. 2 SächsDSG) oder

- automatisierten Verfahren, in denen Beschäftigtendaten im Sinne von § 37 SächsDSG verarbeitet werden (vgl. § 10 Abs. 4 Nr. 3 SächsDSG),

e) geben Einsicht in das Verfahrensverzeichnis (§ 10 Abs. 1 SächsDSG) nach § 11 Abs. 4 Nr. 5 SächsDSG,

f) werden in Einzelfällen bei Anrufung durch Betroffene oder andere Beschäftigte tätig (vgl. § 11 Abs. 5 SächsDSG).

Weitere (datenschutzorganisatorische) Aufgaben können dem Datenschutzbeauftragten von seinem Vorgesetzten im Rahmen der gesetzlichen Möglichkeiten übertragen werden.

In Zweifelsfällen kann sich der Datenschutzbeauftragte an den Sächsischen Datenschutzbeauftragten wenden.

Im Hinblick auf seine Tätigkeit dürfen dem Datenschutzbeauftragten berufliche Nachteile weder drohen noch entstehen, § 11 Abs. 2 Satz 3 SächsDSG. Dies ist Ausdruck seiner Stellung als weisungsfreier Beauftragter.

Er ist als bestellte Vertrauensperson auch nach der Beendigung seiner Tätigkeit zur Verschwiegenheit verpflichtet, § 11 Abs. 5 Satz 1 SächsDSG.

2.2 Befugnisse zur Verarbeitung personenbezogener Daten

Der behördliche Datenschutzbeauftragte darf zur Aufgabenerfüllung gemäß § 11 Abs. 3 SächsDSG ebenso wie der Sächsische Datenschutzbeauftragte Einsicht in die gespeicherten Daten und die Datenverarbeitungsprogramme nehmen. Seine Kontrolle erstreckt sich auch auf personenbezogene Daten, die einem Berufs- oder besonderen Amtsgeheimnis, insbesondere dem Steuergeheimnis nach § 30 der Abgabenordnung, unterliegen.

Dem Datenschutzbeauftragten sollten für eine effektive Aufgabenerfüllung weitere konkretisierte Handlungsbefugnisse durch interne Organisationsverfügung oder eine Stellenbeschreibung, die die im Gesetz festgelegte Weisungsfreiheit betont, verliehen werden. Insbesondere sollte dem Datenschutzbeauftragten zugestanden werden, dass

- Beschäftigte Auskunft auf seine Fragen zu geben haben,

- er das Recht hat, Stellungnahmen innerhalb der Dienststelle einzuholen,

- er über die Möglichkeit verfügt, der Behördenleitung direkt und zeitnah vorzutragen.

Dem Datenschutzbeauftragten sollte die erforderliche Arbeitszeit und Fortbildung zur Erfüllung seiner Aufgaben, auch neben seinen Hauptaufgaben, gewährt werden. Die Fachbereiche müssen den Datenschutzbeauftragten bei der Erfüllung seiner Aufgaben unterstützen (vgl. § 11 Abs. 2 Satz 4 SächsDSG).

Dresden, den 1. Februar 2007
Der Sächsische Datenschutzbeauftragte
Schurig

Anlage 1

Mitteilung über die Bestellung eines Datenschutzbeauftragten nach § 11 SächsDSG

Der Sächsische Datenschutzbeauftragte
Bernhard-von-Lindenau-Platz 1
01067 Dresden

Ort, Datum

Aktenzeichen

Bezeichnung der Stelle	Anschrift der Stelle

Name des Datenschutzbeauftragten (akademischer Grad, Vorname, Name):
……

Datum der Bestellung (laut Urkunde): ……

☐ eingeschränkter Zuständigkeitsbereich[1]
……
……
……

☐ erweiterter Zuständigkeitsbereich (z.B. kommunale Eigenbetriebe)[1]
……
……
……

☐ externer Datenschutzbeauftragter (§ 11 Abs. 1 Satz 4 SächsDSG)[2]

Anschrift: ……

☐ Beschäftigter der bestellenden öffentlichen Stelle

sonstige berufliche Aufgaben (§ 11 Abs. 2 Satz 1 SächsDSG)[2]: ……

Telefonnummer	Fax	E-Mail-Adresse

☐ Abschrift der Bestellungsurkunde ist beigefügt.

……
(Name und Funktion des Erklärenden)

……
(Ort, Datum) (Dienststempel) (Unterschrift des Erklärenden)

[1] Soweit der Zuständigkeitsbereich des Datenschutzbeauftragten nicht deckungsgleich mit der öffentlichen Stelle (im organisatorischen Sinne) ist, sind Abweichungen - gegebenenfalls in Anlage - zu beschreiben.
[2] Gem. § 11 Abs. 2 Satz 1 SächsDSG darf ein Datenschutzbeauftragter nur bestellt werden, wenn durch die Bestellung kein Interessenkonflikt mit seinen sonstigen beruflichen Aufgaben entsteht.

Mitteilung über die Bestellung eines stellvertretenden Datenschutzbeauftragten nach § 11 SächsDSG

Der Sächsische Datenschutzbeauftragte
Bernhard-von-Lindenau-Platz 1
01067 Dresden

Ort, Datum

Aktenzeichen

Bezeichnung der Stelle	Anschrift der Stelle

Name des stellvertretenden Datenschutzbeauftragten (akademischer Grad, Vorname, Name):
……

Datum der Bestellung (laut Urkunde): ……

☐ eingeschränkter Zuständigkeitsbereich[1]
……
……
……

☐ erweiterter Zuständigkeitsbereich (z.B. kommunale Eigenbetriebe)[1]
……
……
……

☐ externer stellvertretender Datenschutzbeauftragter (§ 11 Abs. 1 Satz 4 SächsDSG)[2]

Anschrift: ……

☐ Beschäftigter der bestellenden öffentlichen Stelle

sonstige berufliche Aufgaben (§ 11 Abs. 2 Satz 1 SächsDSG)[2]: ……

Telefonnummer	Fax	E-Mail-Adresse

☐ Abschrift der Bestellungsurkunde ist beigefügt.

……
(Name und Funktion des Erklärenden)

……
(Ort, Datum) (Dienststempel) (Unterschrift des Erklärenden

[1] Soweit der Zuständigkeitsbereich des Datenschutzbeauftragten nicht deckungsgleich mit der öffentlichen Stelle (im organisatorischen Sinne) ist, sind Abweichungen - gegebenenfalls in Anlage - zu beschreiben.
[2] Gem. § 11 Abs. 2 Satz 1 SächsDSG darf ein Datenschutzbeauftragter nur bestellt werden, wenn durch die Bestellung kein Interessenkonflikt mit seinen sonstigen beruflichen Aufgaben entsteht.

16.1.3 Bekanntmachung des Sächsischen Datenschutzbeauftragten zur Vorabkontrolle (§ 10 Abs. 4 SächsDSG)

vom 12. September 2005
aktualisierte Fassung vom 1. Februar 2007

I. Anwendungsbereich

Wann kommt eine Vorabkontrolle in Betracht? Eine Vorabkontrolle ist durchzuführen, wenn entweder

1. *ein automatisiertes Abrufverfahren (§ 8 SächsDSG)*

2. *ein automatisiertes Verfahren zur Verarbeitung besonders schützenswerter Daten (§ 4 Abs. 2 SächsDSG) oder*

3. *ein automatisiertes Verfahren zur Verarbeitung von Beschäftigtendaten (§ 37 SächsDSG)*

erstmals eingesetzt oder wesentlich geändert werden soll.

II. Zuständigkeit und Mitwirkungspflichten

Wer führt die Vorabkontrolle durch? Ist für die *öffentliche* Stelle (i. S. v. § 2 Abs. 1 und 2 SächsDSG), bei der ein o. g. Verfahren eingesetzt oder wesentlich geändert werden soll, ein für diese zuständiger Datenschutzbeauftragter (i. S. v. § 11 SächsDSG) bestellt, so führt dieser die Vorabkontrolle durch, andernfalls der Sächsische Datenschutzbeauftragte. Die Anzeigepflicht für ein solches Verfahren obliegt der Daten verarbeitenden Stelle. Sie hat dafür die zur Prüfung erforderlichen Unterlagen frühestmöglich zur Verfügung zu stellen.

Ergeben sich bei der Vorabkontrolle durch den nach § 11 SächsDSG bestellten Datenschutzbeauftragten Zweifelsfälle, so hat er sich nach vorheriger Unterrichtung des Leiters der öffentlichen Stelle an den Sächsischen Datenschutzbeauftragten zu wenden (vgl. § 11 Abs. 4 Satz 2 Nr. 4 SächsDSG). Außerdem hat er gemäß § 10 Abs. 4 Satz 6 SächsDSG, wenn ein Verfahren auch von nachgeordneten öffentlichen Stellen eingesetzt werden soll, das Ergebnis seiner Vorabkontrolle diesen sowie dem Sächsischen Datenschutzbeauftragten mitzuteilen.

III. Inhalt, Zweck und Grenzen der Vorabkontrolle

Weil die o. g. *automatisierten* Verfahren spezifische Datenschutzrisiken für betroffene Personen beinhalten, unterliegen sie der Prüfung *vor Beginn* des Einsatzes.

Die Vorabkontrolle stellt für die einzuführenden automatisierten Verfahren[1] den Schutzbedarf und die Risiken fest und bewertet, insbesondere unter Berücksichtigung der getroffenen technischen und organisatorischen Maßnahmen gemäß § 9 SächsDSG, ob und wie Gefahren für die informationelle Selbstbestimmung Betroffener angemessen verhindert werden können. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand, insbesondere unter Berücksichtigung der Art der zu schützenden personenbezogenen Daten, in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht (vgl. § 9 Abs. 1 Satz 1 SächsDSG).

Eine Vorabkontrolle ist *rechtzeitig vor ihrem erstmaligen* Einsatz oder *vor einer wesentlichen Änderung* durchzuführen und auf ihre Vereinbarkeit mit den datenschutzrechtlichen Anforderungen zu überprüfen. Der *erstmalige Einsatz* beginnt spätestens mit der Nutzung des Verfahrens im Betrieb (auch Probebetrieb) im realen Arbeitsumfeld mit Echtdaten.

Wesentlich sind *Änderungen*, soweit sie den betroffenen Personenkreis erweitern oder den Schutz bisher Betroffener vermindern. Diese können insbesondere vorliegen, wenn neue (schützenswerte) Datenarten in die Verarbeitung einbezogen werden, neue regelmäßige Datenverarbeitungen (z. B. Übermittlungen) auf weitere Empfänger ausgedehnt werden oder Soft- oder Hardware den Schutz der Betroffenen entscheidend vermindert. Ein Indiz dafür, dass ein Verfahren wesentliche Änderungen erfährt, findet sich im Katalog des § 9 Abs. 2 Nrn. 1 bis 6 SächsDSG.

Die Vorabkontrolle ist mit einer Stellungnahme abzuschließen. Sie ist der Behördenleitung bzw. dem Verfahrensverantwortlichen zuzuleiten und soll innerhalb *eines Monats* abgegeben werden (vgl. § 10 Abs. 4 Satz 3 SächsDSG). Die Monatsfrist beginnt erst, wenn alle für die Vorabkontrolle erforderlichen Unterlagen eingegangen sind. Das Ergebnis der Vorabkontrolle wird Bestandteil des Datenschutz- und Datensicherheitskonzeptes. Aus Revisionsgründen sollte in dem Verfahrensverzeichnis auf die durchgeführte Vorabkontrolle verwiesen werden.

[1] Eine automatisierte Verarbeitung personenbezogener Daten liegt nach § 3 Abs. 5 SächsDSG vor, wenn diese durch den Einsatz eines elektronischen Datenverarbeitungssystems (Rechner und Software) programmgesteuert durchgeführt wird. Ein automatisiertes Verfahren ist die Gesamtheit der einzelnen automatisierten Verarbeitungen mit einem bestimmten Verwendungszweck.

Sofern die Personalvertretung bei der Einführung des Verfahrens zu beteiligen ist, ist dieser gemäß § 10 Abs. 4 Satz 4 SächsDSG die Stellungnahme zur Vorabkontrolle zuzuleiten.

Die Vorabkontrolle als eine vorausgehende Zulässigkeitskontrolle findet i. d. R. gelöst von ihrer Einsatzumgebung statt. Daher besteht die Notwendigkeit, während des Betriebes der neuen Technologie bzw. des automatisierten Verfahrens weitere Kontroll- und Revisionstätigkeiten durchzuführen.

IV. Die Verfahrensarten im Einzelnen

IV.1 Automatisierte Abrufverfahren

Durchzuführen ist die Vorabkontrolle für ein automatisiertes Verfahren, das eine Übermittlung personenbezogener Daten an Dritte durch Abruf ermöglicht (vgl. § 8 Abs. 1 Satz 1 erster Halbsatz SächsDSG). Ein automatisiertes Abrufverfahren ist ein von mindestens zwei Daten verarbeitenden Stellen gemeinsam eingerichtetes und betriebenes Verfahren, durch das die abrufende Stelle personenbezogene Daten aus einer von der bereithaltenden Stelle eingerichteten Datei abrufen kann. Die abrufende Stelle (Datenempfänger) bestimmt allein darüber, ob und wann sie welche Daten (innerhalb eines vorgegebenen Rahmens) abruft.

IV.2 Automatisierte Verarbeitung besonders schützenswerter Daten

Durchzuführen ist die Vorabkontrolle für ein automatisiertes Verfahren, mit dem personenbezogene Daten verarbeitet werden, aus denen die rassische oder ethnische Herkunft, politische Meinung, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie Daten über Gesundheit oder Sexualleben (vgl. § 4 Abs. 2 SächsDSG). Die Verarbeitung dieser Daten ist nur zu den in § 4 Abs. 2 SächsDSG genannten Zwecken zulässig.

IV.3 Automatisierte Verarbeitung von Beschäftigtendaten

Durchzuführen ist die Vorabkontrolle für ein automatisiertes Verfahren, in dem Daten von Beschäftigten oder Bewerbern zur Eingehung, Durchführung, Beendigung oder Abwicklung des Dienst- oder Arbeitsverhältnisses oder zur Durchführung organisatorischer, personeller und sozialer Maßnahmen, insbesondere auch zu Zwecken der Personalplanung und des Personaleinsatzes, oder ein Gesetz, ein Tarifvertrag oder eine Dienstvereinbarung dies vorsieht, verarbeitet werden (vgl. § 37 Abs. 1 SächsDSG).

V. Inhaltliche Erläuterungen zum Verfahrensverzeichnis

Es wird empfohlen, das in der Anlage zu dieser Bekanntmachung abgedruckte Muster zu verwenden. Für jedes Verfahren ist ein gesondertes Datenblatt anzulegen. Beim Ausfüllen sollte beachtet werden:

1. Bezeichnung und Anschrift der Daten verarbeitenden Stelle

Es ist die Stelle (im funktionalen Sinn) zu bezeichnen, bei der die Verarbeitung erfolgt (z. B. das Einwohnermeldeamt der Stadt). Wird das Verfahren von mehreren Stellen genutzt, ist - soweit möglich - eine zusammenfassende Bezeichnung anzugeben oder sind die Stellen einzeln zu nennen.

2. Bezeichnung des Verfahrens

Als Bezeichnung des Verfahrens ist der allgemein übliche oder ein möglichst „sprechender“ Begriff zu wählen. Darüber hinaus sollten Angaben zur eingesetzten Software (z. B. Bezeichnung, Version, Hersteller) gemacht werden.

3. Vorliegende Unterlagen

Die Verfahrensbeschreibung enthält zum einen eine Darstellung der eingesetzten Programme, der Beziehung zu anderen Programmen sowie der Schnittstellen und der Teile, die als Auftragsdatenverarbeitung ausgelagert sind. Zum anderen ist die Einsatzumgebung (eingesetzte Hard- und Standardsoftware, z. B. Betriebssystem) darzustellen.

Verträge über Auftragsdatenverarbeitung oder Wartungsarbeiten sind gemäß § 7 Abs. 2 Satz 2 SächsDSG schriftlich zu schließen. Dabei sind Weisungsbefugnisse, ausreichend sichere Maßnahmen gemäß § 9 SächsDSG, die Möglichkeit der Kündigung bei Datenschutzverstößen sowie ein eventueller Einsatz von Unterauftragnehmern nur mit Zustimmung des Auftraggebers sicherzustellen.

Das Datenschutz- und Sicherheitskonzept enthält Ausführungen, wie den Anforderungen von § 9 Abs. 2 SächsDSG entsprochen wird. Dazu können ggf. vorhandene Dienstvereinbarungen und Dienstanweisungen vorgelegt werden. Ich weise aber ausdrücklich darauf hin, dass nur eine Dienstvereinbarung einen normativen Charakter i. S. d. § 4 Abs. 1 Satz 1 SächsDSG hat.

4. Zweck und Rechtsgrundlage der Verarbeitung personenbezogener Daten

Es ist zu prüfen, ob der angegebene Zweck der Datenverarbeitung (z. B. Lohn- und Ge-

haltsabrechnung) von der entsprechenden gesetzlichen Ermächtigung gedeckt ist.

5. Betroffene Personengruppen und Art der zu verarbeitenden Daten

Es ist zu prüfen, ob die für den betroffenen Personenkreis geplante Verarbeitung der konkret anzugebenden personenbezogenen Daten jeweils rechtmäßig ist.

6. Empfänger und Art zu übermittelnder Daten

Es ist zu prüfen, ob die für den betroffenen Personenkreis geplante Übermittlung der konkret anzugebenden personenbezogenen Daten und Empfänger jeweils rechtmäßig ist.

7. Beabsichtigte Übermittlung in Drittländer

Es ist zu prüfen, ob die für den betroffenen Personenkreis geplante Übermittlung der konkret anzugebenden personenbezogenen Daten und Empfänger in Drittländer jeweils rechtmäßig ist.

8. Regelfristen für die Löschung der Daten

Es ist zu prüfen, ob die Regelfristen für die Löschung den Anforderungen aus § 20 SächsDSG entsprechen.

9. Personelle, technische, und organisatorische Maßnahmen

Die gemäß § 9 SächsDSG getroffenen Maßnahmen sind jeweils zu beschreiben. Dabei kann **Vertraulichkeit** z.B. neben einer Sicherung durch Schließsysteme auch durch differenzierte Zugangs- und Zugriffsberechtigungen, die durch Passwörter oder Chipkarten abgesichert werden, erreicht werden. Zur Sicherstellung der **Integrität** können Schreibrechte sowie die Nutzung von Schnittstellen und mobilen Medien eingeschränkt oder personenbezogene Daten verschlüsselt werden. Regelmäßige Datensicherungen sowie Ausfallsicherungen dienen der **Verfügbarkeit** der für die Datenverarbeitung erforderlichen Daten sowie der entsprechenden Hard- und Software. **Authentizität** kann durch die Verwendung von elektronischen Signaturen, Passwörtern oder Chipkarten erreicht werden. Zur Sicherstellung der **Revisionsfähigkeit** sind die vorgenommenen Verarbeitungen zu protokollieren. **Transparenz** wird schließlich über detaillierte Dokumentationen der Verfahren erreicht, aus denen sich ergibt, welche Daten wie verarbeitet werden, wie die Rechte Betroffener gewahrt werden bzw. wie diese ihre Rechte selbst wahrnehmen können.

Besondere Risikofaktoren sind Gefährdungen, die über die üblicherweise bestehenden hinausgehen und demzufolge bei der Risikoabwägung besonders zu berücksichtigen

sind. Um eine solche Gefährdung handelt es sich zum Beispiel bei dem zunehmenden Einsatz von drahtlosen Netzwerken in der öffentlichen Verwaltung. Der Aufbau kabelloser Netze oder die Anbindung von Peripheriegeräten mittels Funkkommunikation ermöglichen das Abhören, Kopieren und Manipulieren von Daten in Abhängigkeit von Umweltbedingungen und Sendeleistung. Die Reichweiten können zwischen 10 m bis 100 m betragen. Passwörter oder andere sensible Daten könnten mitgehört werden, falls keine ausreichend sichere Verschlüsselung genutzt wird.

10. Stellungnahme

Eine automatisierte Datenverarbeitung darf nur eingeführt werden, wenn den erheblichen Gefahren für das Persönlichkeitsrecht durch ausreichend starke Schutzmaßnahmen entgegengewirkt werden kann und das Restrisiko unter Anwendung des Verhältnismäßigkeitsgrundsatzes tragbar ist. Ist das Restrisiko zu hoch, muss geprüft werden, ob durch eine Nachbesserung technischer oder organisatorischer Maßnahmen eine datenschutzgerechte Verarbeitung ermöglicht werden könnte. Ist das nicht der Fall, kann das Verfahren nicht eingeführt oder geändert werden.

Dresden, den 1. Februar 2007
Der Sächsische Datenschutzbeauftragte
Schurig

Anlage

Vorabkontrolle gemäß § 10 Abs. 4 SächsDSG

wegen:

☐ eines Verfahrens nach § 8

☐ eines automatisierten Verfahrens, in dem Daten im Sinne des § 4 Abs. 2 verarbeitet werden

☐ eines automatisierten Verfahrens, in dem Daten von Beschäftigten im Sinne des § 37 verarbeitet werden

1. Bezeichnung und Anschrift der Daten verarbeitenden Stelle

2. Bezeichnung des Verfahrens

3. Vorliegende Unterlagen

☐ Verfahrensbeschreibungen bzw. Benutzer-Handbücher,

☐ gegebenenfalls schriftliche Regelungen zur Auftragsdatenverarbeitung bzw. Wartung

☐ Datenschutz- und Datensicherheitskonzepte für das zu prüfende Verfahren gemäß § 9 Abs. 2 SächsDSG (vgl. dazu unten unter 9.)

☐ Dienstvereinbarung / Dienstanweisung

4. Zweck und Rechtsgrundlage der Verarbeitung personenbezogener Daten

Zweck	Rechtsgrundlage	Ergebnis der Prüfung

5. Betroffene Personengruppen und Art der zu verarbeitenden Daten

Personengruppe	Art der zu verarbeitenden Daten	Ergebnis der Prüfung

6. Empfänger und Art zu übermittelnder Daten

Empfänger	Art der zu übermittelnden Daten	Ergebnis der Prüfung

7. Beabsichtigte Übermittlung in Drittländer gemäß § 17 SächsDSG

Empfänger	Art der zu übermitteln-den Daten	Rechtsgrundlage	Ergebnis der Prüfung

8. Regelfristen für die Löschung der Daten

Art der Daten	Zeitraum	Ergebnis der Prüfung

9. Das Datenschutz- und Datensicherheitskonzept

umfasst mindestens

☐ die differenzierte Vergabe von Zugriffsrechten (Benutzerprofile) für Mitarbeiter,

☐ die Dokumentation zulässiger Auswertungen,

☐ die Gewährleistung von Rechten der Betroffenen (Auskunft, Berichtigung, Löschung, Sperrung),

☐ ein ausreichend sicheres Passwortverfahren oder andere Authentifikationsverfahren (Chipkarte, PIN, elektronische Signatur),

☐ die Protokollierung und Log-Auswertungen (Fehlanmeldungen - Missbrauchsversuche),

☐ regelmäßige Backups von Programmen und Daten,

☐ die Überwachung von Administrations- und Wartungsarbeiten,

Gibt es besondere Risikofaktoren?

Wie ist sichergestellt, dass

a) nur Befugte personenbezogene Daten zur Kenntnis nehmen können (Vertraulichkeit),

b) personenbezogene Daten während der Verarbeitung unversehrt, vollständig und aktuell bleiben (Integrität),

c) personenbezogene Daten zeitgerecht zur Verfügung stehen und ordnungsgemäß verarbeitet werden können (Verfügbarkeit),

d) jederzeit personenbezogene Daten ihrem Ursprung zugeordnet werden können (Authentizität),

e) festgestellt werden kann, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat (Revisionsfähigkeit),

f) die Verfahrensweisen bei der Verarbeitung personenbezogener Daten vollständig, aktuell und in einer Weise dokumentiert sind, dass sie in zumutbarer Zeit nachvollzogen werden können (Transparenz)?

10. Stellungnahme

Ort, Datum: ……. **Stempel, Unterschrift:** ……..

16.2 Entschließungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder

16.2.1 Entschließung der 70. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 27./28. Oktober 2005 in der Hansestadt Lübeck: Gravierende Datenschutzmängel beim Arbeitslosengeld II endlich beseitigen

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder stellt fest, dass bei der Umsetzung der Zusammenlegung von Arbeitslosenhilfe und Sozialhilfe weiterhin erhebliche datenschutzrechtliche Mängel bestehen. Die Rechte der Betroffenen werden dadurch stark beeinträchtigt. Zwar ist das Verfahren der Datenerhebung durch die unter Beteiligung der Datenschutzbeauftragten des Bundes und der Länder überarbeiteten Antragsvordrucke auf dem Weg, datenschutzkonform ausgestaltet zu werden. Bei der Leistungs- und Berechnungssoftware A2LL gibt es jedoch entgegen den Zusagen des Bundesministeriums für Wirtschaft und Arbeit (BMWA) und der Bundesagentur für Arbeit (BA) immer noch keine erkennbaren Fortschritte.

Weder ist ein klar definiertes Zugriffsberechtigungskonzept umgesetzt, noch erfolgt eine Protokollierung der lesenden Zugriffe. Damit ist es über 40.000 Mitarbeiterinnen und Mitarbeitern in der BA und den Arbeitsgemeinschaften nach SGB II (ARGEn) nach wie vor möglich, voraussetzungslos auf die Daten aller Leistungsempfänger und -empfängerinnen zuzugreifen, ohne dass eine Kontrolle möglich wäre.

Dies gilt auch für das elektronische Vermittlungsverfahren coArb, das ebenfalls einen bundesweiten lesenden Zugriff erlaubt. Äußerst sensible Daten, wie z.B. Vermerke über Schulden-, Ehe- oder Suchtprobleme, können so eingesehen werden. Den Datenschutzbeauftragten sind bereits Missbrauchsfälle bekannt geworden. Einzelne ARGEn reagieren auf die Probleme und speichern ihre Unterlagen wieder in Papierform. Es muss sichergestellt sein, dass das Nachfolgesystem VerBIS, das Mitte 2006 einsatzbereit sein soll, grundsätzlich nur noch einen engen, regionalen Zugriff zulässt und ein detailliertes Berechtigungs- und Löschungskonzept beinhaltet. Der Datenschutz muss auch bei der Migration der Daten aus coArb in VerBIS beachtet werden.

Mit Unterstützung der Datenschutzbeauftragten des Bundes und der Länder hat die BA den Antragsvordruck und die Zusatzblätter überarbeitet. Soweit die Betroffenen auch die ergänzenden neuen Ausfüllhinweise erhalten, wird ihnen ein datenschutzgerechtes Ausfüllen der Unterlagen ermöglicht und damit eine Erhebung von nicht erforderlichen Daten vermieden. Doch ist immer noch festzustellen, dass die bisherigen Ausfüllhinweise nicht überall verfügbar sind. Es ist daher zu gewährleisten, dass allen Be-

troffenen nicht nur baldmöglichst die neuen Antragsvordrucke, sondern diese gemeinsam mit den Ausfüllhinweisen ausgehändigt werden („Paketlösung“).

Es handelt sich bei den ARGEn um eigenverantwortliche Daten verarbeitende Stellen, die uneingeschränkt der Kontrolle der Landesbeauftragten für Datenschutz unterliegen. Dies haben die Bundesanstalt und die ARGEn zu akzeptieren. Es ist nicht hinnehmbar, dass über die Verweigerung einer Datenschutzkontrolle rechtsfreie Räume entstehen und damit in unzumutbarer Weise in die Rechte der Betroffenen eingegriffen wird.

Die Datenschutzbeauftragten des Bundes und der Länder fordern die BA und die sonstigen verantwortlichen Stellen auf Bundes- und Länderebene auf, selbst und im Rahmen ihrer Rechtsaufsicht die Datenschutzmissstände beim Arbeitslosengeld II zu beseitigen. Für den Fall einer völligen Neugestaltung des Systems A2LL wegen der offenbar nicht zu beseitigenden Defizite erwarten die Datenschutzbeauftragten ihre zeitnahe Beteiligung. Es ist sicherzustellen, dass die datenschutzrechtlichen Vorgaben, wie die Protokollierung der lesenden Zugriffe und ein klar definiertes Zugriffsberechtigungs- und Löschungskonzept, ausreichend berücksichtigt werden, um den Schutz des informationellen Selbstbestimmungsrechts zu gewährleisten.

16.2.2 Entschließung der 70. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 27./28. Oktober 2005 in der Hansestadt Lübeck: Appell der Datenschutzbeauftragten des Bundes und der Länder: Eine moderne Informationsgesellschaft braucht mehr Datenschutz

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder sieht für die 16. Legislaturperiode des Deutschen Bundestags großen Handlungsbedarf im Bereich des Datenschutzes. Der Weg in eine freiheitliche und demokratische *Informationsgesellschaft* unter Einsatz modernster Technologie zwingt alle Beteiligten, ein verstärktes Augenmerk auf den Schutz des Rechts auf informationelle Selbstbestimmung zu legen. Ohne wirksameren Datenschutz werden die Fortschritte vor allem in der Informations- und der Biotechnik nicht die für Wirtschaft und Verwaltung notwendige gesellschaftliche Akzeptanz finden.

Es bedarf einer grundlegenden *Modernisierung des Datenschutzrechtes*. Hierzu gehört eine Ergänzung des bisher auf Kontrolle und Beratung basierenden Datenschutzrechtes um Instrumente des wirtschaftlichen Anreizes, des Selbstdatenschutzes und der technischen Prävention. Es ist daher höchste Zeit, dass in dieser Legislaturperiode vom Deutschen Bundestag ein Datenschutz-Auditgesetz erarbeitet wird. Datenschutzkonforme Technikgestaltung als Wettbewerbsanreiz liegt im Interesse von Wirtschaft, Ver-

waltung und Bevölkerung. Zugleich ist die ins Stocken geratene umfassende Novellierung des Bundesdatenschutzgesetzes mit Nachdruck voranzutreiben. Eine Vereinfachung und Konzentration der rechtlichen Regelungen kann Bürokratie abbauen und zugleich den Grundrechtsschutz stärken.

Die Bürgerinnen und Bürger müssen auch in Zukunft frei von Überwachung sich informieren und miteinander kommunizieren können. Nur so können sie in der Informationsgesellschaft ihre Grundrechte selbstbestimmt in Anspruch nehmen. Dem laufen Bestrebungen zuwider, mit dem Argument einer vermeintlich höheren Sicherheit immer mehr alltägliche Aktivitäten der Menschen elektronisch zu registrieren und für Sicherheitszwecke auszuwerten. Die längerfristige Speicherung auf Vorrat von Verkehrsdaten bei der Telekommunikation, die zunehmende Videoüberwachung im öffentlichen Raum, die anlasslose elektronische Erfassung des Straßenverkehrs durch Kfz-Kennzeichenabgleich, die Erfassung biometrischer Merkmale der Bevölkerung oder Bestrebungen zur Ausdehnung der Rasterfahndung betreffen ganz überwiegend völlig unverdächtige Bürgerinnen und Bürger und setzen diese der Gefahr der *Ausforschung ihrer Lebensgewohnheiten* und einem ständig wachsenden Anpassungsdruck aus, ohne dass dem immer ein adäquater Sicherheitsgewinn gegenübersteht. Freiheit und Sicherheit bedingen sich wechselseitig Angesichts zunehmender Überwachungsmöglichkeiten kommt der Freiheit vor staatlicher Beobachtung und Ausforschung sowie dem Grundsatz der Datensparsamkeit und Datenvermeidung eine zentrale Bedeutung zu.

Den Sicherheitsbehörden steht bereits ein breites Arsenal an gesetzlichen Eingriffsbefugnissen zur Verfügung, das teilweise überstürzt nach spektakulären Verbrechen geschaffen worden ist. Diese Eingriffsbefugnisse der Sicherheitsbehörden müssen einer umfassenden systematischen *Evaluierung durch unabhängige Stellen* unterworfen und öffentlich zur Diskussion gestellt werden. Unangemessene Eingriffsbefugnisse, also solche, die mehr schaden als nützen, sind wieder zurückzunehmen.

Die Kontrolle der Bürgerinnen und Bürger wird auch mit den Argumenten der Verhinderung des Missbrauchs staatlicher Leistungen und der Erhöhung der Steuerehrlichkeit vorangetrieben. So richtig es ist, in jedem Einzelfall die Voraussetzungen für staatliche Hilfen zu prüfen und bei hinreichenden Anhaltspunkten Steuerhinterziehungen nachzugehen, so überflüssig und rechtsstaatlich problematisch ist es, alle Menschen mit einem Pauschalverdacht zu überziehen und Sozial- und Steuerverwaltung mit dem Recht auszustatten, verdachtsunabhängig Datenabgleiche mit privaten und öffentlichen Datenbeständen vorzunehmen. Es muss verhindert werden, dass mit dem Argument der *Leistungs- und Finanzkontrolle* die Datenschutzgrundsätze der Zweckbindung und der informationellen Gewaltenteilung auf der Strecke bleiben.

Die Entwicklung in Medizin und Biotechnik macht eine Verbesserung des Schutzes des Patientengeheimnisses notwendig. Telemedizin, der Einsatz von High-Tech im Gesundheitswesen, gentechnische Verfahren und eine intensivierte Vernetzung der im Gesundheitsbereich Tätigen kann zu einer Verbesserung der Qualität der Gesundheitsversorgung und zugleich zur Kosteneinsparung beitragen. Zugleich drohen die Vertraulichkeit der Gesundheitsdaten und die Wahlfreiheit der Patientinnen und Patienten verloren zu gehen. Diese bedürfen dringend des gesetzlichen Schutzes, u. a. durch ein modernes Gendiagnostikgesetz und durch datenschutz- und patientenfreundliche Regulierung der Computermedizin.

Persönlichkeitsrechte und Datenschutz sind im Arbeitsverhältnis vielfältig bedroht, insbesondere durch neue Möglichkeiten der Kontrolle bei der Nutzung elektronischer Kommunikationsdienste, Videotechnik, Funksysteme und neue biotechnische Verfahren. Schranken werden bisher nur im Einzelfall durch Arbeitsgerichte gesetzt. Das seit vielen Jahren vom Deutschen Bundestag geforderte *Arbeitnehmerdatenschutzgesetz* muss endlich für beide Seiten im Arbeitsleben Rechtsklarheit und Sicherheit schaffen.

Die *Datenschutzkontrolle* hat mit der sich fast explosionsartig entwickelnden Informationstechnik nicht Schritt gehalten. Immer noch findet die Datenschutzkontrolle in manchen Ländern durch nachgeordnete Stellen statt. Generell sind Personalkapazität und technische Ausstattung unzureichend. Dem steht die europarechtliche Anforderung entgegen, die Datenschutzaufsicht in völliger Unabhängigkeit auszuüben und diese adäquat personell und technisch auszustatten.

Die Europäische Union soll ein „Raum der Freiheit, der Sicherheit und des Rechts“ werden. Die Datenschutzbeauftragten des Bundes und der Länder sind sich bewusst, dass dies zu einer verstärkten Zusammenarbeit der Strafverfolgungsbehörden bei der Verbrechensbekämpfung in der Europäischen Union führen wird.

Die grenzüberschreitende Zusammenarbeit von Polizei- und Justizbehörden darf jedoch nicht zur Schwächung von Grundrechtspositionen der Betroffenen führen. Der vermehrte Austausch personenbezogener Daten setzt deshalb ein hohes und gleichwertiges Datenschutzniveau in allen EU-Mitgliedstaaten voraus. Dabei ist von besonderer Bedeutung, dass die Regelungen in enger Anlehnung an die Datenschutzrichtlinie 95/46/EG erfolgen, damit ein möglichst einheitlicher *Datenschutz in der Europäischen Union* gilt, der nicht zuletzt dem Ausgleich zwischen Freiheitsrechten und Sicherheitsbelangen dienen soll.

Die Datenschutzbeauftragten des Bundes und der genannten Länder appellieren an die Fraktionen im Bundestag und an die künftige Bundesregierung, sich verstärkt für den Grundrechtsschutz in der Informationsgesellschaft einzusetzen.

16.2.3 Entschließung der 70. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 27./28. Oktober 2005 in der Hansestadt Lübeck: Telefonbefragungen von Leistungsbeziehern und Leistungsbezieherinnen von Arbeitslosengeld II datenschutzgerecht gestalten

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist anlässlich von durch die Bundesanstalt mit Hilfe privaten Callcentern durchgeführten Telefonbefragungen bei Leistungsbeziehern und Leistungsbezieherinnen von Arbeitslosengeld II darauf hin, dass es den Betroffenen unbenommen ist, sich auf ihr Grundrecht auf informationelle Selbstbestimmung zu berufen. Da die Befragung freiwillig war, hatten sie das Recht, die Beantwortung von Fragen am Telefon zu verweigern.

Die Ablehnung der Teilnahme an einer solchen Befragung rechtfertigt nicht den Verdacht auf Leistungsmissbrauch. Wer seine Datenschutzrechte in Anspruch nimmt, darf nicht deshalb des Leistungsmissbrauchs bezichtigt werden.

Die Konferenz fordert daher das Bundesministerium für Wirtschaft und Arbeit und die Bundesanstalt für Arbeit dazu auf, die Sach- und Rechtslage klarzustellen und bei der bereits angekündigten neuen Telefonaktion eine rechtzeitige Beteiligung der Datenschutzbeauftragten sicherzustellen.

16.2.4 Entschließung der 70. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 27./28. Oktober 2005 in der Hansestadt Lübeck: Keine Vorratsdatenspeicherung in der Telekommunikation

Die Europäische Kommission hat den Entwurf einer Richtlinie über die Vorratsspeicherung von Daten über die elektronische Kommunikation vorgelegt. Danach sollen alle Telekommunikationsanbieter und Internet-Provider verpflichtet werden, systematisch eine Vielzahl von Daten über jeden einzelnen Kommunikationsvorgang über einen längeren Zeitraum (ein Jahr bei Telefonaten, sechs Monate bei Internet-Nutzung) für mögliche Abrufe von Sicherheitsbehörden selbst dann zu speichern, wenn sie diese Daten für betriebliche Zwecke (z. B. zur Abrechnung) gar nicht benötigen. Die Annahme dieses Vorschlags oder des gleichzeitig im Ministerrat beratenen, weiter gehenden Entwurfs eines Rahmenbeschlusses und ihre Umsetzung in nationales Recht würde einen Dammbruch zulasten des Datenschutzes unverdächtiger Bürgerinnen und Bürger bedeuten. Sowohl das grundgesetzlich geschützte Fernmeldegeheimnis als auch der durch die Europäische Menschenrechtskonvention garantierte Schutz der Privatsphäre

drohen unverhältnismäßig eingeschränkt und in ihrem Wesensgehalt verletzt zu werden.

Die Datenschutzbeauftragten des Bundes und der Länder bekräftigen ihre bereits seit 2002 geäußerte grundsätzliche Kritik an jeder Pflicht zur anlassunabhängigen Vorratsdatenspeicherung. Die damit verbundenen Eingriffe in das Fernmeldegeheimnis und das informationelle Selbstbestimmungsrecht lassen sich auch nicht durch die Bekämpfung des Terrorismus rechtfertigen, weil sie unverhältnismäßig sind. Insbesondere gibt es keine überzeugende Begründung dafür, dass eine solche Maßnahme in einer demokratischen Gesellschaft zwingend notwendig wäre.

Die anlassunabhängige Vorratsdatenspeicherung aller Telefon- und Internetdaten ist von großer praktischer Tragweite und widerspricht den Grundregeln unserer demokratischen Gesellschaft. Erfasst würden nicht nur die Daten über die an sämtlichen Telefongesprächen und Telefax-Sendungen beteiligten Kommunikationspartner und -partnerinnen, sondern auch der jeweilige Zeitpunkt und die Dauer der Einwahl ins Internet, die dabei zugeteilte IP-Adresse, ferner die Verbindungsdaten jeder einzelnen E-Mail und jeder einzelnen SMS sowie die Standorte jeder Mobilkommunikation. Damit ließen sich europaweite Bewegungsprofile für einen Großteil der Bevölkerung für einen längeren Zeitraum erstellen.

Die von einigen Regierungen (z. B. der britischen Regierung nach den Terroranschlägen in London) gemachten Rechtfertigungsversuche lassen keinen eindeutigen Zweck einer solchen Maßnahme erkennen, sondern reichen von den Zwecken der Terrorismusbekämpfung und der Bekämpfung des organisierten Verbrechens bis hin zur allgemeinen Straftatenverfolgung. Alternative Regelungsansätze wie das in den USA praktizierte anlassbezogene Vorhalten („Einfrieren“ auf Anordnung der Strafverfolgungsbehörden und „Auftauen“ auf richterlichen Beschluss) sind bisher nicht ernsthaft erwogen worden.

Mit einem Quick-freeze Verfahren könnte man dem Interesse einer effektiven Strafverfolgung wirksam und zielgerichtet nachkommen.

Der Kommissionsvorschlag würde zu einer personenbezogenen Datensammlung von beispiellosem Ausmaß und zweifelhafter Eignung führen. Eine freie und unbefangene Telekommunikation wäre nicht mehr möglich. Jede Person, die in Zukunft solche Netze nutzt, würde unter Generalverdacht gestellt. Jeder Versuch, die zweckgebundene oder befristete Verwendung dieser Datensammlung auf Dauer sichern zu wollen, wäre zum Scheitern verurteilt. Derartige Datenbestände würden Begehrlichkeiten wecken, aufgrund derer die Hürde für einen Zugriff auf diese Daten immer weiter abgesenkt werden könnten. Auch aus diesem Grund muss bereits den ersten Versuchen, eine solche Vor-

ratsdatenspeicherung einzuführen, entschieden entgegengetreten werden. Zudem ist eine Ausweitung der Vorratsdatenspeicherung auch auf Inhaltsdaten zu befürchten. Schon jetzt ist die Trennlinie zwischen Verkehrs- und Inhaltsdaten gerade bei der Internetnutzung nicht mehr zuverlässig zu ziehen. Dieselben - unzutreffenden - Argumente, die jetzt für eine flächendeckende Speicherung von Verkehrsdaten angeführt werden, würden bei einer Annahme des Kommissionsvorschlags alsbald auch für die anlassfreie Speicherung von Kommunikationsinhalten auf Vorrat ins Feld geführt werden.

Die Konferenz appelliert an die Bundesregierung, den Bundestag und das Europäische Parlament, einer Verpflichtung zur systematischen und anlasslosen Vorratsdatenspeicherung auf europäischer Ebene nicht zuzustimmen. Auf der Grundlage des Grundgesetzes wäre eine anlasslose Vorratsdatenspeicherung verfassungswidrig.

16.2.5 Entschließung der 70. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 27./28. Oktober 2005 in der Hansestadt Lübeck: Unabhängige Datenschutzkontrolle in Deutschland gewährleisten

Anlässlich eines von der Europäischen Kommission am 5. Juli 2005 eingeleiteten Vertragsverletzungsverfahrens gegen die Bundesrepublik Deutschland zur Unabhängigkeit der Datenschutzkontrolle fordert die Konferenz erneut eine völlig unabhängige Datenschutzkontrolle.

Die Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (EG-Datenschutzrichtlinie) verlangt, dass die Einhaltung datenschutzrechtlicher Vorschriften in den Mitgliedstaaten von Stellen überwacht wird, die die ihnen zugewiesenen Aufgaben in völliger Unabhängigkeit wahrnehmen. In Deutschland ist indessen die Datenschutzkontrolle der Privatwirtschaft überwiegend in den Weisungsstrang der jeweiligen Innenverwaltung eingebunden. Diese Aufsichtsstruktur bei der Datenschutzkontrolle der Privatwirtschaft verstößt nach Ansicht der Europäischen Kommission gegen Europarecht.

Die Datenschutzbeauftragten des Bundes und der Länder können eine einheitliche Datenschutzkontrolle des öffentlichen und privaten Bereichs in völliger Unabhängigkeit sicherstellen. Sie sollten dazu in allen Ländern und im Bund als eigenständige Oberste Behörden eingerichtet werden, die keinen Weisungen anderer administrativer Organe unterliegen.

Demgegenüber ist die in Niedersachsen beabsichtigte Rückübertragung der Datenschutzkontrolle des privatwirtschaftlichen Bereichs vom Landesdatenschutzbeauftragten auf das Innenministerium ein Schritt in die falsche Richtung. Die Konferenz wendet

sich entschieden gegen diese Planung und fordert den Bund sowie alle Länder auf, zügig europarechtskonforme Aufsichtsstrukturen im deutschen Datenschutz zu schaffen.

16.2.6 Entschließung der 70. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 27./28. Oktober 2005 in der Hansestadt Lübeck: Schutz des Kernbereichs privater Lebensgestaltung bei verdeckten Datenerhebungen der Sicherheitsbehörden

Aus dem Urteil des Bundesverfassungsgerichts vom 27. Juli 2005 zur präventiven Telekommunikationsüberwachung nach dem niedersächsischen Polizeigesetz folgt, dass der durch die Menschenwürde garantierte unantastbare Kernbereich privater Lebensgestaltung im Rahmen aller verdeckten Datenerhebungen der Sicherheitsbehörden uneingeschränkt zu gewährleisten ist. Bestehen im konkreten Fall Anhaltspunkte für die Annahme, dass eine Überwachungsmaßnahme Inhalte erfasst, die zu diesem Kernbereich zählen, ist sie nicht zu rechtfertigen und muss unterbleiben (Erhebungsverbot). Für solche Fälle reichen bloße Verwertungsverbote nicht aus.

Die Gesetzgeber in Bund und Ländern sind daher aufgerufen, alle Regelungen über verdeckte Ermittlungsmethoden diesen gerichtlichen Vorgaben entsprechend auszugestalten.

Diese Verpflichtung erstreckt sich auch auf die Umsetzung der gerichtlichen Vorgabe zur Wahrung des rechtsstaatlichen Gebots der Normenbestimmtheit und Normenklarheit. Insbesondere im Bereich der Vorfeldermittlungen verpflichtet dieses Gebot die Gesetzgeber auf Grund des hier besonders hohen Risikos einer Fehlprognose, handlungsbegrenzende Tatbestandselemente für die Tätigkeit der Sicherheitsbehörden zu normieren.

Im Rahmen der verfassungskonformen Ausgestaltung der Vorschriften sind die Gesetzgeber darüber hinaus verpflichtet, die gerichtlichen Vorgaben im Hinblick auf die Wahrung des Verhältnismäßigkeitsgrundsatzes - insbesondere die Angemessenheit der Datenerhebung - und eine strikte Zweckbindung umzusetzen.

In der Entscheidung vom 27. Juli 2005 hat das Gericht erneut die Bedeutung der - zuletzt auch in seinen Entscheidungen zum Großen Lauschangriff und zum Außenwirtschaftsgesetz vom 3. März 2004 dargelegten - Verfahrenssicherungen zur Gewährleistung der Rechte der Betroffenen hervorgehoben. So verpflichtet beispielsweise das Gebot der effektiven Rechtsschutzgewährung die Sicherheitsbehörden, Betroffene über die verdeckte Datenerhebung zu informieren.

Diese Grundsätze sind sowohl im Bereich der Gefahrenabwehr als auch im Bereich der Strafverfolgung, u. a. bei der Novellierung der §§ 100a und 100b StPO, zu beachten.

Die Konferenz der DSB erwartet, dass nunmehr zügig die erforderlichen Gesetzgebungsarbeiten in Bund und Ländern zum Schutz des Kernbereichs privater Lebensgestaltung bei allen verdeckten Ermittlungsmaßnahmen aufgenommen und die Vorgaben des Bundesverfassungsgerichts ohne Abstriche umgesetzt werden.

16.2.7 Entschließung der 70. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 27./28. Oktober 2005 in der Hansestadt Lübeck: Telefonieren mit Internettechnologie (Voice over IP - VoIP)

Die Internet-Telefonie verbreitet sich rasant. Mittlerweile bieten alle großen Provider in Deutschland das Telefonieren über das Internet an. Dabei ist den Kunden und Kundinnen oft nicht bekannt, dass diese Verbindungen in den meisten Fällen noch wesentlich unsicherer sind als ein Telefongespräch über das herkömmliche Festnetz.

Bei Telefongesprächen über das Internet kommt die Internet-Technologie Voice over IP (VoIP) zum Einsatz. In zunehmendem Maße wird angeboten, Telefongespräche mit Hilfe der Internet-Technologie VoIP zu führen. Das Fernmeldegeheimnis ist auch für die Internettelefonie zu gewährleisten. Während jedoch bei separaten, leitungsvermittelten Telekommunikationsnetzen Sicherheitskonzepte vorzulegen sind, ist dies bei VoIP bisher nicht die Praxis. Vielmehr werden diese Daten mit Hilfe des aus der Internetkommunikation bekannten Internet-Protokolls (IP) in Datenpakete unterteilt und paketweise über bestehende lokale Computernetze und/oder das offene Internet übermittelt.

Eine derartige Integration von Sprache und Daten in ein gemeinsames Netzwerk stellt den Datenschutz vor neue Herausforderungen. Die aus der Internetnutzung und dem Mail-Verkehr bekannten Unzulänglichkeiten und Sicherheitsprobleme können sich bei der Integration der Telefonie in die Datennetze auch auf die Inhalte und näheren Umstände der VoIP-Kommunikation auswirken und den Schutz des Fernmeldegeheimnisses beeinträchtigen. Beispielsweise können VoIP-Netzwerke durch automatisierte Versendung von Klingelrundrufen oder Überflutung mit Sprachpaketen blockiert, Inhalte und nähere Umstände der VoIP-Kommunikation mangels Verschlüsselung ausgespäht, kostenlose Anrufe durch Erschleichen von Authentifizierungsdaten geführt oder Schadsoftware wie Viren oder Trojaner aktiv werden. Darüber hinaus ist nicht auszuschließen, dass das Sicherheitsniveau der vorhandenen Datennetze negativ beeinflusst wird, wenn sie auch für den VoIP-Sprachdaten-Verkehr genutzt werden. Personenbezogene Daten der VoIP-Nutzenden können außerdem dadurch gefährdet sein, dass Anbieter von VoIP-Diensten ihren Sitz mitunter im außereuropäischen

Ausland haben und dort möglicherweise weniger strengen Datenschutzanforderungen unterliegen als Anbieter mit Sitz in der Europäischen Union (EU).

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert deshalb Hersteller und Herstellerinnen, Anbieter und Anbieterinnen sowie Anwender und Anwenderinnen von VoIP-Lösungen auf, das grundgesetzlich geschützte Fernmeldegeheimnis auch bei VoIP zu wahren und hierfür

- angemessene technische und organisatorische Maßnahmen zu treffen, um eine sichere und datenschutzgerechte Nutzung von VoIP in einem Netzwerk zu ermöglichen,
- Verschlüsselungsverfahren für VoIP anzubieten bzw. angebotene Verschlüsselungsmöglichkeiten zu nutzen,
- Sicherheits- und Datenschutzmängel, die die verwendeten Protokolle oder die genutzte Software bisher mit sich bringen, durch Mitarbeit an der Entwicklung möglichst schnell zu beseitigen,
- auf die Verwendung von offenen, standardisierten Lösungen zu achten beziehungsweise die verwendeten Protokolle und Algorithmen offenzulegen,
- VoIP-Kunden über die Gefahren und Einschränkungen gegenüber dem klassischen, leitungsvermittelten Telefondienst zu informieren und
- bei VoIP alle datenschutzrechtlichen Vorschriften genauso wie bei der klassischen Telefonie zu beachten.

In den benutzten Netzen, auf den beteiligten Servern und an den eingesetzten Endgeräten müssen angemessene Sicherheitsmaßnahmen umgesetzt werden, um die Verfügbarkeit, die Vertraulichkeit, die Integrität und die Authentizität der übertragenen Daten zu gewährleisten.

16.2.8 Entschließung zwischen der 70. und 71. Konferenz der Konferenz der Datenschutzbeauftragen des Bundes und der Länder vom 15. Dezember 2005: Sicherheit bei eGovernment durch Nutzung des Standards OSCI

In modernen eGovernment-Verfahren werden personenbezogene Daten zahlreicher Fachverfahren zwischen unterschiedlichen Verwaltungsträgern in Bund, Ländern und Kommunen übertragen. Die Vertraulichkeit, Integrität und Zurechenbarkeit der übertragenen Daten kann nur gewährleistet werden, wenn dem Stand der Technik entsprechende Verschlüsselungs- und Signaturverfahren genutzt werden.

Mit dem Online Services Computer Interface (OSCI) steht bereits ein bewährter Sicherheits-Standard für eGovernment-Anwendungen zur Verfügung. Verfahren, die diese Standards berücksichtigen, bieten die Gewähr für eine durchgehende Sicherheit bei der Datenübermittlung vom Versand bis zum Empfang (Ende-zu-Ende-Sicherheit) und

erlauben somit auch rechtsverbindliche Transaktionen zwischen den beteiligten Kommunikationspartnerinnen und -partnern.

Die durchgehende Sicherheit darf nicht dauerhaft durch Vermittlungs- und Übersetzungsdienste, die nicht der OSCI-Spezifikation entsprechen, beeinträchtigt werden. Werden solche Dienste zusätzlich in die behördlichen Kommunikationsströme eingeschaltet, wird das mit OSCI-Transport erreichbare Sicherheitsniveau abgesenkt. Der Einsatz von sogenannten Clearingstellen, wie sie zunächst für das automatisierte Meldeverfahren vorgesehen sind, kann daher nur eine Übergangslösung sein.

Werden Programme und Schnittstellen auf der Basis derartiger Standards entwickelt, ist sichergestellt, dass die Produkte verschiedener Anbieterinnen und Anbieter im Wettbewerb grundlegende Anforderungen des Datenschutzes und der Datensicherheit in vergleichbar hoher Qualität erfüllen. Gleichzeitig erleichtern definierte Standards den öffentlichen Verwaltungen die Auswahl datenschutzkonformer, interoperabler Produkte.

Vor diesem Hintergrund begrüßt die Konferenz der Datenschutzbeauftragten des Bundes und der Länder die vom Koordinierungsausschuss Automatisierte Datenverarbeitung (KoopA ADV), dem gemeinsamen Gremium von Bund, Ländern und Kommunalen Spitzenverbänden, getroffene Festlegung, in eGovernment-Projekten den Standard OSCI-Transport für die Übermittlung von personenbezogenen Daten einzusetzen. Um die angestrebte Ende-zu-Ende-Sicherheit überall zu erreichen, empfiehlt sie einen flächendeckenden Aufbau einer OSCI-basierten Infrastruktur.

16.2.9 Entschließung der 71. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 16./17. März 2006 in Magdeburg: Mehr Datenschutz bei der polizeilichen und justiziellen Zusammenarbeit in Strafsachen

Auf europäischer Ebene wird verstärkt über die Ausweitung des grenzüberschreitenden Informationsaustauschs für Zwecke der Polizei und Justiz mit dem Ziel diskutiert, einen Raum der Freiheit, der Sicherheit und des Rechts zu schaffen. Der Austausch personenbezogener Informationen zwischen den Strafverfolgungsbehörden der Mitgliedstaaten setzt ein hohes und gleichwertiges Datenschutzniveau bei allen beteiligten Stellen voraus.

Die Datenschutzbeauftragten des Bundes und der Länder begrüßen, dass die EU-Kommission einen Rahmenbeschluss zur Harmonisierung und zum Ausbau des Datenschutzes bei den Polizei- und Justizbehörden vorgelegt hat*. Sie betonen, dass die Regelungen in enger Anlehnung an die allgemeine Datenschutzrichtlinie (95/46/EG)

* KOM (2005) 475 vom 4. Oktober 2005

erfolgen müssen, damit der Datenschutz in der EU auf einem einheitlich hohen Niveau gewährleistet wird.

Die Datenschutzbeauftragten des Bundes und der Länder unterstützen die Forderungen der Europäischen Datenschutzkonferenz in ihrem Beschluss vom 24. Januar 2006. Auch sie treten dafür ein, den Datenschutz im Zusammenarbeitsbereich der sog. „Dritten Säule“ der EU im Sinne der EU-Grundrechte-Charta zu gestalten.

Dies bedeutet u. a., dass Eingriffe in Freiheitsrechte nur im überwiegenden öffentlichen Interesse und im Rahmen der Verhältnismäßigkeit zulässig sind. Die Rahmenrichtlinie muss die Voraussetzungen der Datenverarbeitung und -übermittlung nach den jeweiligen Rollen der Verfahrensbeteiligten (Beschuldigte, Verdächtigte, Zeugen und Zeuginnen, Opfer) normenklar und differenziert regeln. Zudem müssen die Rechte der Betroffenen auf Auskunft, Berichtigung und Löschung gewährleistet werden. Die Datenverarbeitung muss umfassend durch unabhängige Datenschutzbehörden kontrolliert werden können. Die Datenschutzkontrollrechte müssen - unter Beachtung der richterlichen Unabhängigkeit - gewahrt werden. Sie dürfen nicht mit der Begründung eingeschränkt werden, dass ein laufendes Verfahren vorliege oder die Gefahrenabwehr bzw. die Strafverfolgung behindert werde. Einheitliche Datenschutzregelungen müssen zudem alle Formen der Datenverarbeitung - auch sofern sie in Akten erfolgt - einbeziehen.

Daten von europäischen Polizei- und Justizbehörden dürfen an Drittstaaten außerhalb der EU nur übermittelt werden, wenn ihre Verarbeitung im Zielland nach rechtsstaatlichen Grundsätzen erfolgt und ein angemessener Datenschutz sichergestellt ist. Bei der polizeilichen und justiziellen Zusammenarbeit in Strafsachen muss ferner der Grundsatz der Zweckbindung beachtet werden. Abweichungen des ersuchenden Staates vom angegebenen Verwendungszweck müssen auf Ausnahmefälle von besonderem Gewicht beschränkt bleiben. Die Ausnahmen müssen für den ersuchten Staat umfassend und zeitnah kontrollierbar sein.

Zur Schaffung eines hohen und einheitlichen Datenschutzstandards in der Dritten Säule der EU gibt es keine Alternative. Es darf nicht dazu kommen, dass auf europäischer Ebene weitere Eingriffsbefugnisse für die Sicherheitsbehörden mit immer tieferen Einschnitten in die Grundrechte beschlossen werden, ohne dass gleichzeitig die Freiheitsrechte der hier lebenden Bürgerinnen und Bürger gestärkt und geschützt werden. Aus diesem Grund hält es die Konferenz für dringend erforderlich, entsprechende Datenschutzbestimmungen zügig zu verabschieden und umzusetzen, bevor der Datenaustausch weiter ausgebaut wird.

16.2.10 Entschließung der 71. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 16./17. März 2006 in Magdeburg: Keine kontrollfreien Räume bei der Leistung von ALG II

Die Datenschutzbeauftragten des Bundes und der Länder haben die Bundesagentur für Arbeit (BA) und die sonstigen verantwortlichen Stellen auf Bundes- und Länderebene in ihrer Entschließung vom 27./28. Oktober 2005 aufgefordert, die Datenschutzmissstände beim Arbeitslosengeld II zu beseitigen. Zu diesen Missständen gehört die wiederholte Weigerung der BA, Landesbeauftragten für den Datenschutz zu ermöglichen, ihre Kontrollaufgaben bei den Arbeitsgemeinschaften nach dem SGB II (ARGEn) zu erfüllen. Mit einer „Weisung“ vom 31. Januar 2006 versucht die BA, nunmehr alle ARGEn auf diese Linie zu verpflichten. Den Landesdatenschutzbeauftragten soll der für Kontrollzwecke notwendige Zugriff auf die zentralen automatisierten Verfahren verwehrt werden.

Der Bundesbeauftragte für den Datenschutz und die Landesdatenschutzbeauftragten bekräftigen ihre gemeinsame Auffassung, dass es sich bei den ARGEn um eigenverantwortliche Daten verarbeitende Stellen der Länder handelt, die uneingeschränkt der Kontrolle der Landesbeauftragten für den Datenschutz unterliegen. Dass die BA Ressourcen für die Arbeitsgemeinschaften bereitstellt, ändert nichts an diesem Ergebnis.

Es muss gewährleistet sein, dass die Verarbeitung von Sozialdaten in den ARGEn von den jeweils zuständigen Landesbeauftragten umfassend und ohne inhaltliche Beschränkungen datenschutzrechtlich überprüft werden kann. Eine rechtliche Konstellation, durch die die Landesbeauftragten für den Datenschutz von der Kontrolle der ARGEn ausgeschlossen würden, würde gegen die bundesstaatliche Kompetenzordnung verstoßen und wäre einer effektiven Datenschutzkontrolle abträglich. Sie würde den Grundrechtsschutz der betroffenen Bürgerinnen und Bürger empfindlich beeinträchtigen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Bundesregierung dazu auf, umgehend einen rechtskonformen Zustand herzustellen.

16.2.11 Entschließung der 71. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 16./17. März 2006 in Magdeburg: Listen der Vereinten Nationen und der Europäischen Union über Terrorverdächtige

In den vergangenen Monaten sind die vom Sanktionsausschuss der Vereinten Nationen (VN) erstellten Listen über terrorverdächtige Personen und Organisationen, die von der Europäischen Gemeinschaft durch entsprechende Verordnungen umgesetzt worden

sind, in den Blickpunkt der Öffentlichkeit gerückt. Personen, die auf diesen Listen erscheinen, unterliegen umfangreichen Beschränkungen, die von Wirtschafts- und Finanzsanktionen über Einreiseverbote bis hin zum Einfrieren ihrer Gelder und anderer Vermögenswerte reichen.

Ein Eintrag in den genannten Listen greift in das informationelle Selbstbestimmungsrecht der betreffenden Personen ein und kann darüber hinaus gravierende existentielle Folgen haben, die z. B. die Verweigerung von Sozialleistungen umfassen können. Vielfach sind diese Personen nicht eindeutig bezeichnet. Auch in Deutschland lebende Personen sind von entsprechenden Maßnahmen betroffen. In jüngster Zeit gab es Verwechslungen mit schwer wiegenden Folgen für völlig unverdächtige Personen. Besonders kritisch ist zu werten, dass gegen die Aufnahme in die Listen kein Rechtsschutz besteht.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher die Bundesregierung auf, bei den Vereinten Nationen und in der Europäischen Union auf die Einhaltung der rechtsstaatlich gebotenen Standards zu dringen. Dazu gehören insbesondere ein transparentes Listing-Verfahren, Entscheidungen auf einer gesicherten Tatsachenbasis, ein zweifelsfreier Identitätsnachweis und effektiver Rechtsschutz.

16.2.12 Entschließung der 71. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 16./17. März 2006 in Magdeburg: Keine Aushöhlung des Fernmeldegeheimnisses im Urheberrecht

Das Bundesministerium der Justiz hat den Referentenentwurf eines „Gesetzes zur Verbesserung der Durchsetzung von Rechten des geistigen Eigentums“ vorgelegt, das in Umsetzung einer europäischen Richtlinie stärkere Instrumente zum Schutz des Urheberrechts und anderer gewerblicher Schutzrechte einführen soll.

Der Gesetzentwurf gesteht den Rechteinhabenden in bestimmten Fällen Auskunftsansprüche auch gegenüber unbeteiligten Dritten zu, die selbst keine Urheberrechtsverletzungen begangen haben. So sollen etwa Internet-Provider auch über - durch das Fernmeldegeheimnis geschützte - Daten ihrer Nutzerinnen und Nutzer zur Auskunft verpflichtet werden. Damit sollen beispielsweise Anbietende und Nutzende illegal kopierter Musik- oder Videodateien oder Software leichter ermittelt werden können.

Die Datenschutzbeauftragten des Bundes und der Länder warnen vor der hiermit eingeleiteten Entwicklung. Zwar sind die vorgesehenen Eingriffe in das Fernmeldegeheimnis in dem Entwurf an formale Hürden geknüpft; insbesondere müssen Rechteinhabende eine richterliche Anordnung erwirken. Jedoch lassen die europarechtlichen Vorgaben den Mitgliedstaaten zugunsten des Datenschutzes so viel Spielraum, dass

Eingriffe in das Fernmeldegeheimnis vermieden werden können. Das Bundesverfassungsgericht hat betont, dass gemeinschaftsrechtliche Spielräume zu nutzen sind.

Nachdem das grundrechtlich geschützte Fernmeldegeheimnis in den letzten Jahren immer stärker und in immer kürzeren Abständen für Zwecke der Strafverfolgung und der Geheimdienste eingeschränkt wurde, soll es nun auch erstmals zugunsten privater wirtschaftlicher Interessen nicht unerheblich weiter eingeschränkt werden. Es ist zu befürchten, dass damit ähnliche Begehrlichkeiten weiterer privater Interessengruppen geweckt werden. Dem grundrechtlich geschützten Fernmeldegeheimnis unterliegende Daten stünden am Ende der Entwicklung für kaum noch zu übersehende Zwecke zur Verfügung.

Es ist zu befürchten, dass durch die Auskunftsansprüche gegen Internet-Provider die gerade für die Verfolgung schwerer Straftaten beschlossene Verpflichtung zur Vorratsdatenspeicherung von Verkehrsdaten für die Durchsetzung privater Interessen genutzt wird. Angesichts der Tendenz, die Internet-Anbietenden in immer stärkerem Maße für die Kommunikationsinhalte ihrer Kunden verantwortlich zu machen, ist zudem zu befürchten, dass die Firmen vorsichtshalber weitere Verkehrsdaten speichern, um im Falle von Rechtsverletzungen Auskünfte erteilen zu können.

Die Datenschutzbeauftragten des Bundes und der Länder appellieren deshalb an die Bundesregierung und an den Gesetzgeber, auf eine weitere Einschränkung des Fernmeldegeheimnisses - erstmals zur Durchsetzung wirtschaftlicher Interessen - zu verzichten. Es wäre völlig unakzeptabel, wenn Daten, deren zwangsweise Speicherung mit der Abwehr terroristischer Gefahren begründet wurde, nun auf breiter Basis für die Verfolgung von Urheberrechtsverletzungen genutzt würden. Musik- und Filmindustrie müssen selbst dafür Sorge tragen, dass durch technische Maßnahmen und neue Geschäftsmodelle unrechtmäßigen Nutzungen die Grundlage entzogen wird.

16.2.13 Entschließung zwischen der 71. und 72. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 11. Oktober 2006 (bei Enthaltung von Schleswig-Holstein): Sachgemäße Nutzung von Authentisierungs- und Signaturverfahren

Die Datenschutzbeauftragten des Bundes und der Länder beobachten einen Trend, abweichend von den bislang geltenden Vorgaben zur Nutzung der qualifizierten elektronischen Signatur in der öffentlichen Verwaltung zunehmend ungeeignete oder weniger sichere Verfahren zuzulassen. So soll beispielsweise infolge des Gesetzentwurfes der Bundesregierung zum Jahressteuergesetz 2007 (BR-Drs. 622/06) beim Verfahren Elster Online der Finanzverwaltung das in § 87a AO Abs. 3 geforderte Verfahren zur qualifizierten elektronischen Signatur durch ein Verfahren ersetzt werden, das lediglich zur

Authentisierung der Datenübermittler geeignet ist. Auch die Planungen zum Verfahren für den elektronischen Einkommensnachweis ELENA sehen zumindest für einen Übergangszeitraum den Verzicht auf die qualifizierte elektronische Signatur vor. Einer derartigen Fehlentwicklung muss mit Nachdruck entgegengetreten werden.

Obwohl Signatur- und Authentisierungsverfahren mit der asymmetrischen Verschlüsselung vergleichbare technische Verfahren nutzen, unterscheiden sie sich im Inhalt ihrer Aussagen und müssen unterschiedliche Rechtsfolgen für die Nutzenden nach sich ziehen. Der grundlegende Unterschied dieser Verfahren muss sowohl bei der Planung als auch bei ihrem Einsatz in Verwaltungsverfahren berücksichtigt werden.

Elektronische Signaturen liefern Aussagen über elektronische Dokumente, insbesondere über deren Authentizität und Integrität. Ausschließlich die qualifizierte elektronische Signatur ist durch rechtliche Regelungen der eigenhändigen Unterschrift in weiten Bereichen gleichgestellt und dient dem Nachweis der Echtheit elektronischer Dokumente. Zudem sind nur Verfahren zur Erzeugung elektronischer Signaturen rechtlich geregelt und sicherheitstechnisch genau definiert.

Authentisierungsverfahren liefern hingegen lediglich eine Aussage über die Identität einer Person oder einer Systemkomponente. Solche Verfahren sind beispielsweise zur Authentifizierung einer Person oder eines IT-Systems gegenüber Kommunikationspartnern oder zur Anmeldung an einem IT-System geeignet. Die hierbei ausgetauschten Informationen unterliegen in der Regel nicht dem Willen und dem Einfluss der Rechnernutzenden bzw. der Kommunikationspartner und beziehen sich ausschließlich auf den technischen Identifizierungsprozess. Daher dürfen an die Authentizität und Integrität solcher Daten nicht die gleichen Rechtsfolgen geknüpft werden wie an eine qualifizierte elektronische Signatur.

Die Aufrechterhaltung der unterschiedlichen Funktionalität und Verbindlichkeit von Signatur und Authentisierung liegt sowohl im Interesse von Bürgerinnen und Bürgern als auch der Verwaltung und ist rechtlich geboten. Die unsachgemäße Anwendung oder in Kauf genommene Funktionsvermischung dieser Verfahren mindert die Transparenz, die Sicherheit und die Verlässlichkeit bei der elektronischen Datenverarbeitung. Darüber hinaus sind erhebliche Nachteile für die Nutzenden zu erwarten.

Wird ein Authentisierungsschlüssel zum Signieren verwendet,

- kann fälschlicher Weise behauptet werden, dass Nutzende elektronische Dokumente signiert haben; da sie das Gegenteil nicht beweisen können, müssen sie befürchten, die damit verbundenen Rechtsfolgen tragen zu müssen,

- besteht die Möglichkeit, dass Authentisierungsverfahren (Single Sign On, Challenge Response etc.) gezielt missbräuchlich verwendet werden,
- wird den Nutzenden keine "Warnfunktion" mehr angeboten wie bei der ausschließlichen Verwendung des Signaturschlüssels zum Signieren und
- sind die Verfahren und die daraus resultierenden Konsequenzen für die Nutzenden nicht mehr transparent.

Vor diesem Hintergrund fordert die Konferenz der Datenschutzbeauftragten des Bundes und der Länder, dass der Gesetzgeber weder ungeeignete noch weniger sichere Verfahren zulässt. Dies bedeutet, dass

- Nutzenden die Möglichkeit eröffnet werden muss, die elektronische Kommunikation mit der Verwaltung durch eine qualifizierte elektronische Signatur abzusichern,
- immer dann Signaturverfahren eingesetzt werden müssen, wenn Aussagen über Dokumente oder Nachrichten gefordert sind und Authentisierungsverfahren nur dort verwendet werden dürfen, wo es um Aussagen über eine Person oder eine Systemkomponente geht,
- die Transparenz der Verfahren und die Nutzbarkeit der Authentisierungsfunktion erhalten bleiben müssen.

Die Datenschutzbeauftragten appellieren darüber hinaus an die Verantwortlichen in der Verwaltung und bei den Projektträgern, gemeinsam die offenen Fragen beim Einsatz der qualifizierten elektronischen Signatur zu lösen und insbesondere die Entwicklung interoperabler, ökonomischer Verfahren zur Prüfung qualifizierter elektronischer Signaturen zu unterstützen. Hierfür ist die konstruktive Zusammenarbeit der Verantwortlichen von großen Anwendungsverfahren wie Elster Online, ELENA und Elektronische Gesundheitskarte unabdingbar.

Die Bundesregierung sollte verstärkt die Einführung von Verfahren mit qualifizierter elektronischer Signatur unterstützen, weil diese Verfahren für die sichere und authentische Kommunikation zwischen Bürgerinnen und Bürgern und der Verwaltung besonders geeignet sind. Die qualifizierte elektronische Signatur muss eine zentrale Komponente in eGovernment-Anwendungen sein, und darf nicht durch ungeeignete oder weniger sichere Verfahren ersetzt werden. Die Bundesregierung sollte daher die Verbreitung von Chipkarten mit qualifiziertem Zertifikat fördern. Erst der flächendeckende Einsatz von qualifizierten elektronischen Signaturen ermöglicht niedrige Kosten bei der Bereitstellung der Karten und führt darüber hinaus zu rationellen und somit kostengünstigen Verwaltungsabläufen.

16.2.14 Entschließung der 72. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27. Oktober 2006 in Naumburg: Das Gewicht der Freiheit beim Kampf gegen den Terrorismus

Seit dem 11. September 2001 wandelt sich der Staat immer mehr zu einem Präventionsstaat, der sich nicht darauf beschränkt, Straftaten zu verfolgen und konkrete Gefahren abzuwehren. Der Staat verlagert seine Aktivitäten zunehmend in das Vorfeld der Gefahrenabwehr. Sicherheitsbehörden gehen der abstrakten Möglichkeit von noch nicht einmal geplanten Taten nach. Immer mehr Daten werden auf Vorrat gesammelt und damit eine Vielzahl unverdächtiger Menschen erfasst. Auch unbescholtene Bürgerinnen und Bürger werden als Risikofaktoren behandelt, ohne dass diese dafür Anlass gegeben haben. Dieses neue Verständnis von innerer Sicherheit führt zu gravierenden Einschränkungen der Freiheitsrechte. Beispiele sind die von der Europäischen Union beschlossene Speicherung der Telekommunikationsverkehrsdaten oder die im Jahr 2002 verfassungswidrig durchgeführten Rasterfahndungen.

In diesem Zusammenhang ist auch der „Entwurf eines Gesetzes zur Ergänzung des Terrorismusbekämpfungsgesetzes" kritisch zu bewerten. Die ursprünglich zur Terrorismusbekämpfung geschaffenen Befugnisse werden immer weiter ausgedehnt und nicht mehr nur auf Terrorverdächtige beschränkt.

Bei allen Gesetzen und Maßnahmen zur Terrorbekämpfung stellt sich die Frage nach deren Eignung und Verhältnismäßigkeit. Mehr Überwachung führt nicht automatisch zu mehr Sicherheit, aber stets zu weniger Freiheit. Es gibt keine absolute Sicherheit.

Die verfassungsrechtlich notwendige wissenschaftliche Evaluation der bisherigen Vorschriften zur Terrorismusbekämpfung durch eine unabhängige Stelle fehlt bislang. Der „Bericht der Bundesregierung zu den Auswirkungen des Terrorismusbekämpfungsgesetzes" ist keine vollwertige Evaluation der bisherigen Vorschriften. Damit steht sowohl die Notwendigkeit einer Verlängerung als auch die Erforderlichkeit der Schaffung neuer Befugnisse in Zweifel.

Zunehmende Befugnisse verlangen nach zusätzlichen Kontrollen. Daher ist es unerlässlich, einen angemessenen Ausgleich zwischen den Befugnissen der Sicherheitsbehörden und den Kompetenzen der Kontrollorgane zu schaffen. Insbesondere müssen die Handlungsmöglichkeiten der parlamentarischen Kontrollorgane entsprechend ausgestaltet sein.

16.2.15 Entschließung der 72. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27. Oktober 2006 in Naumburg: Verfassungsrechtliche Grundsätze bei Antiterrordatei-Gesetz beachten

Mit dem Entwurf eines Gesetzes zur Errichtung gemeinsamer Dateien von Polizeibehörden und Nachrichtendiensten des Bundes und der Länder (Gemeinsame-Dateien-Gesetz-BT-Drs. 16/2950) - verschärft durch Forderungen aus dem Bundesrat - sollen in der Bundesrepublik Deutschland erstmals die rechtlichen Grundlagen für die Errichtung gemeinsamer Dateien von Polizeibehörden und Nachrichtendiensten geschaffen werden. Von besonderer Bedeutung ist die beim Bundeskriminalamt zur Aufklärung und Bekämpfung des internationalen Terrorismus einzurichtende Antiterrordatei, in welcher umfangreiches Datenmaterial der beteiligten Sicherheitsbehörden zusammengeführt werden soll.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder verkennt nicht die zur Begründung des Gesetzentwurfs geltend gemachte hohe Bedrohung durch den internationalen Terrorismus und die Notwendigkeit zur Optimierung des Informationsaustauschs. Jede Intensivierung der informationellen Zusammenarbeit zwischen Polizeibehörden und Nachrichtendiensten muss jedoch den verfassungsrechtlichen Vorgaben, insbesondere dem Recht auf informationelle Selbstbestimmung, dem Grundsatz der Verhältnismäßigkeit und dem - in einigen Landesverfassungen ausdrücklich genannten - Trennungsgebot zwischen Polizei und Nachrichtendiensten entsprechen. Der vorliegende Entwurf zur Antiterrordatei enthält schwerwiegende verfassungs- und datenschutzrechtliche Risiken.

Insbesondere den folgenden brisanten Aspekten wird im Rahmen der anstehenden parlamentarischen Beratungen besondere Beachtung zu schenken sein:

- Die Anti-Terror-Datei sieht gravierende Erweiterungen des Datenaustauschs vor. Deshalb ist zumindest eine weitergehende Präzisierung der zu erfassenden Personen erforderlich. Insoweit ist insbesondere zu berücksichtigen, dass die Nachrichtendienste in der Antiterrordatei auch Personen erfassen, bei denen nur auf weichen Informationen beruhende tatsächliche Anhaltspunkte für eine Zuordnung zum internationalen Terrorismus bestehen. Diese Anhaltspunkte können auf legalem Verhalten beruhen, mit der Folge, dass auch unbescholtene Personen in der Antiterrordatei erfasst werden und deren Daten allen zugriffsberechtigten Behörden zur Verfügung stehen. Dass im Bereich der Vorfeldermittlungen ein besonders hohes Risiko einer Fehlprognose besteht, ist auch bereits verfassungsgerichtlich festgestellt.

- Die Definition der in der Datei zu erfassenden sog. Kontaktpersonen muss präzisiert werden und der Kreis der Betroffenen ist einzuschränken. Dies gilt insbesondere für

solche Kontaktpersonen, gegen die keinerlei belastende Erkenntnisse vorliegen. Es muss sichergestellt werden, dass nicht bereits unverdächtige soziale Kontakte zu einer Erfassung von Personen aus dem Umfeld Verdächtigter führen.

- Die Aufnahme besonderer Bemerkungen, ergänzender Hinweise und Bewertungen in Freitextform eröffnet den am Verbund teilnehmenden Behörden die Möglichkeit, eine Vielzahl, auch weicher personenbezogener Informationen (z.B. nicht überprüfte Hinweise oder Vermutungen) ohne Bindung an hinreichend konkrete Festlegungen des Gesetzgebers in der Datei zu erfassen. Deshalb sollte darauf verzichtet werden.

- In diesem Zusammenhang ist auch der Zugriff von Polizeibehörden auf Vorfelderkenntnisse der Nachrichtendienste im Hinblick auf das Trennungsgebot kritisch zu hinterfragen. Besonders bedenklich erscheint dabei die Zulassung von Ausnahmen vom verfassungsrechtlichen Trennungsgebot in den sog. Eilfällen, in welchen den beteiligten Behörden ein unmittelbarer Online-Zugriff auf alle Daten gestattet wird.

- Die zugriffsberechtigten Sicherheitsbehörden sind nicht klar genug bezeichnet. Aufgrund der Speicherung auch höchst sensibler personenbezogener Vorfelddaten muss der Gesetzgeber aus rechtsstaatlichen Gründen selbst festlegen, welche Stellen zugriffsberechtigt sein sollen.

- Im Übrigen sind auch die bereits jetzt erkennbaren Tendenzen zu einer Erweiterung der Antiterrordatei über die Terrorismusbekämpfung hinaus nicht akzeptabel. Dies gilt insbesondere für die im Gesetzentwurf vorgesehene Nutzung der Datei im Rahmen der Strafverfolgung. Es darf nicht zu einer immer niedrigeren Eingriffsschwelle kommen.

16.2.16 Entschließung der 72. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27. Oktober 2006 in Naumburg: Verbindliche Regelungen für den Einsatz von RFID-Technologien

Der Einsatz von RFID-Tags (Radio Frequency Identification) hält unaufhaltsam Einzug in den Alltag. Schon jetzt werden sowohl im öffentlichen als auch im privatwirtschaftlichen Bereich viele Gegenstände mit diesen miniaturisierten IT-Systemen gekennzeichnet. Es ist zu erwarten, dass neben bereits jetzt mit RFID-Technik gekennzeichneten Lebensmitteln künftig auch Personalausweise, Geldscheine, Kleidungsstücke und Medikamentenpackungen mit RFID-Tags versehen werden. In wenigen Jahren könnten somit praktisch alle Gegenstände des täglichen Lebens weltweit eindeutig gekennzeichnet sein.

Die flächendeckende Einführung derart gekennzeichneter Gegenstände birgt erhebliche Risiken für das Recht auf informationelle Selbstbestimmung in sich. Die RFID-Kennungen verschiedenster Gegenstände können sowohl miteinander als auch mit weiteren personenbezogenen Daten der Nutzenden - in der Regel ohne deren Wissen und Wollen - zusammengeführt werden. Auf diese Weise werden detaillierte Verhaltens-, Nutzungs- und Bewegungsprofile von Betroffenen ermöglicht.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder erwartet von allen Stellen, in deren Verantwortungsbereich RFID-Tags verwendet werden, insbesondere von Herstellern und Anwendern im Handels- und Dienstleistungssektor, alle Möglichkeiten der datenschutzgerechten Gestaltung dieser Technologie zu entwickeln und zu nutzen, und vor allem die Prinzipien der Datensparsamkeit, Zweckbindung, Vertraulichkeit und Transparenz zu gewährleisten. Der schnellen Umsetzung dieser Forderungen kann auch eine verbindliche Selbstverpflichtung von Herstellern und Anwendern der RFID-Technologie im Handels- und Dienstleistungssektor dienen.

Das Bundesverfassungsgericht hat den Gesetzgeber mehrfach darauf hingewiesen, dass wegen des schnellen und für den Grundrechtsschutz riskanten informationstechnischen Wandels die technischen Entwicklungen aufmerksam zu beobachten sind und notfalls durch ergänzende Rechtsetzung korrigierend einzugreifen ist. Daher sind die besonderen Gegebenheiten, die mit dem Einsatz der RFID-Technologie verbunden sind, vom Gesetzgeber daraufhin zu untersuchen, ob für alle Risiken adäquate und rechtliche Schutzmechanismen vorhanden sind. In den Bereichen, in denen diese fehlen, hat der Gesetzgeber einzugreifen. Dies gilt insbesondere für den Fall, dass die Hersteller und Anwender sich auf eine verbindliche Selbstverpflichtung nicht einlassen.

Für den Schutz der Persönlichkeitsrechte Betroffener sind generell folgende Forderungen zu berücksichtigen:

- Transparenz

  Alle Betroffenen müssen umfassend über den Einsatz, Verwendungszweck und Inhalt von RFID-Tags informiert werden.

- Kennzeichnungspflicht

  Nicht nur die eingesetzten RFID-Tags selbst, sondern auch die Kommunikationsvorgänge, die durch die Chips ausgelöst werden, müssen für die Betroffenen leicht zu erkennen sein. Eine heimliche Anwendung darf es nicht geben.

- Keine heimliche Profilbildung

Daten von RFID-Tags aus verschiedenen Produkten dürfen nur so verarbeitet werden, dass personenbezogene Verhaltens-, Nutzungs- und Bewegungsprofile ausschließlich mit Wissen und Zustimmung der Betroffenen erstellt werden können. Soweit eine eindeutige Identifizierung einzelner Gegenstände für einen bestimmten Anwendungszweck nicht erforderlich ist, muss auf eine Speicherung eindeutig identifizierender Merkmale auf den RFID-Tags verzichtet werden.

- Vermeidung der unbefugten Kenntnisnahme

Das unbefugte Auslesen der gespeicherten Daten muss beispielsweise durch Verschlüsselung bei ihrer Speicherung und Übertragung unterbunden werden.

- Deaktivierung

Es muss vor allem im Handels- und Dienstleistungssektor die Möglichkeit bestehen, RFID-Tags dauerhaft zu deaktivieren, bzw. die darauf enthaltenen Daten zu löschen, insbesondere dann, wenn Daten für die Zwecke nicht mehr erforderlich sind, für die sie auf dem RFID-Tag gespeichert wurden.

16.2.17 Entschließung der 72. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27. Oktober 2006 in Naumburg: Keine Schülerstatistik ohne Datenschutz

Seit einigen Jahren arbeitet die Kultusministerkonferenz an der Einführung eines bundesweit einheitlichen Schulstatistiksystems, in dem weit über das bisherige Maß hinaus Daten aus dem Schulbereich personenbezogen verarbeitet werden sollen. Es soll auf Landesebene in einer Datei für jede Schülerin und jeden Schüler sowie für jede Lehrerin und jeden Lehrer für das gesamte „Schulleben“ ein umfangreicher Datensatz angelegt werden. Hierzu erhält jede Person eine Identifikationsnummer, was auf ein pseudonymisiertes Register hinausläuft. Die Länderdateien sollen überdies zu einer bundesweiten Datenbank zusammengefasst werden. Die spätere Ergänzung des Schülerdatensatzes mit so genannten sozialökonomischen Daten über das Elternhaus sowie eine Einbeziehung der Kindergarten- und Hochschulzeit ist beabsichtigt. Eine präzise und einheitliche Zweckbestimmung lässt sich den bisherigen Äußerungen der Kultusministerkonferenz nicht entnehmen.

In datenschutzrechtlicher Hinsicht sind folgende Vorgaben zu beachten:

Wie das Bundesverfassungsgericht festgestellt hat, ist eine Totalerhebung nur zulässig, wenn der gleiche Erfolg nicht mit weniger einschneidenden Maßnahmen erreicht werden kann. Im Hinblick auf die bereits gewonnenen Ergebnisse aus stichprobenartigen

und weitgehend auf Freiwilligkeit beruhenden wissenschaftlichen Untersuchungen (wie PISA, IGLU oder TIMSS) erscheint die Notwendigkeit der geplanten Einrichtung eines bundesweiten zentralen schüler- bzw. lehrerbezogenen "Bildungsregisters" nicht dargetan. Ein solches Register wäre ein nicht erforderlicher und damit unverhältnismäßiger Eingriff in das informationelle Selbstbestimmungsrecht.

Deshalb fordern die Datenschutzbeauftragten von der Kultusministerkonferenz bei diesem Vorhaben nachdrücklich den Verzicht auf eine ID-Nummer. Jede Möglichkeit einer Reidentifizierung von Individualdatensätzen ist durch geeignete Verfahren auszuschließen (kein schüler- oder lehrerbeziehbares Bildungsregister!).

Im Übrigen sind folgende verfassungsrechtliche Vorgaben und Grenzen unabdingbar:

- Der Umfang des Erhebungsprogramms ist auf den für die Statistikzwecke dienlichen Umfang zu beschränken.
- Bei allen Festlegungen sind die Grundsätze der Erforderlichkeit und Verhältnismäßigkeit zu beachten.
- Bei der Datenverarbeitung ist das Gebot der personellen, organisatorischen, räumlichen und verfahrensmäßigen Trennung von Verwaltungsvollzug und Statistik einzuhalten und das Statistikgeheimnis zu gewährleisten.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt, dass Schulministerien in mehreren Ländern das bisherige, datenschutzrechtlich bedenkliche Konzept nicht mehr weiter verfolgen, und strebt dies auch als Gesamtergebnis der mit der Kultusministerkonferenz zu führenden Gespräche und des angekündigten Workshops an.

16.2.18 Entschließung der 73. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8./9. März 2007 in Erfurt: GUTE ARBEIT in Europa nur mit gutem Datenschutz

Die Ministerinnen und Minister für Beschäftigung und Soziales in Europa haben am 19. Januar 2007 neun Schlussfolgerungen für GUTE ARBEIT aufgestellt: GUTE ARBEIT bedeute Arbeitnehmerrechte und Teilhabe, faire Löhne, Sicherheit und Gesundheitsschutz bei der Arbeit sowie eine familienfreundliche Arbeitsorganisation. Gute und faire Arbeitsbedingungen sowie angemessener sozialer Schutz seien unabdingbar für die Akzeptanz der Europäischen Union bei den Bürgerinnen und Bürgern.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder nimmt diese Initiative zum Anlass und fordert dazu auf, auch den Beschäftigtendatenschutz zu stärken. Angesichts stetig wachsender technischer Möglichkeiten muss klar geregelt

werden, welche Daten Unternehmen über ihre Beschäftigten erheben dürfen, wie sie damit verfahren müssen und wozu sie die Daten nutzen dürfen.

Deshalb fordert die Konferenz seit langem ein Arbeitnehmerdatenschutzgesetz. Bereits 2003 hat sie darauf hingewiesen, dass Persönlichkeitsrechte und Datenschutz im Arbeitsverhältnis vielfältig bedroht sind, zum Beispiel durch

- die Sammlung von Beschäftigtendaten in leistungsfähigen Personalinformationssystemen, die zur Erstellung von Persönlichkeitsprofilen genutzt werden,
- die Übermittlung von Beschäftigtendaten zwischen konzernangehörigen Unternehmen, für die nicht der Datenschutz der EG-Datenschutzrichtlinie gilt,
- die Überwachung des Arbeitsverhaltens durch Videokameras, die Protokollierung der Nutzung von Internetdiensten am Arbeitsplatz,
- die Erhebung des Gesundheitszustands, Drogen-Screenings und psychologische Testverfahren bei der Einstellung.

Die Achtung des Grundrechts auf informationelle Selbstbestimmung der Arbeitnehmerinnen und Arbeitnehmer zählt ebenso zu guten und fairen Arbeitsbedingungen wie Chancengleichheit oder gerechte Bezahlung. Beschäftigtendatenschutz erhöht zudem die Motivation, trägt und fördert die Arbeitszufriedenheit und bedeutet damit einen nicht zu unterschätzenden Standortvorteil.

Die Konferenz fordert die Bundesregierung auf, sich für einen hohen gemeinsamen Mindeststandard des Arbeitnehmerdatenschutzes in Europa einzusetzen und in Deutschland zeitnah einen entsprechenden Gesetzentwurf vorzulegen.

16.2.19 Entschließung der 73. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8./9. März 2007 in Erfurt: Anonyme Nutzung des Fernsehens erhalten!

Seit einiger Zeit werden in der Öffentlichkeit Pläne der großen privaten Fernsehveranstalter diskutiert, gemeinsam mit den Betreibern von Übertragungskapazitäten (Satellit, Kabel und DVB-T) ihre Programme nur noch verschlüsselt zu übertragen. Dabei werden vorrangig solche Geschäftsmodelle favorisiert, bei denen die kostenpflichtige Entschlüsselung des Signals nur mit personenbezogenen Smartcards möglich sein soll.

Die Datenschutzbeauftragten des Bundes und der Länder betrachten diese Entwicklung mit Sorge. Nachdem vor allem durch zahlreiche staatliche Eingriffe die verfassungsrechtlich gebotene unbeobachtete Nutzung von Telekommunikation und Internet kaum noch möglich ist, steht nun auch der seit jeher selbstverständliche anonyme und nicht registrierte Empfang von Rundfunkprogrammen auf dem Spiel. Gerade durch die Ver-

marktung individuell zugeschnittener Programmpakete im digitalen Rundfunk kann bei personenbezogener Abrechnung nachvollzogen werden, wer welche Angebote nutzt. Die entstehenden technischen Infrastrukturen werden zudem auch Möglichkeiten bieten, die konkrete Nutzung einzelner Sendungen zu registrieren. Damit wird die allgegenwärtige Bildung von Persönlichkeitsprofilen um detaillierte Kenntnisse über den Rundfunkkonsum ergänzt.

Die bisher bekannt gewordenen Pläne der Unternehmen widersprechen dem im Rundfunkstaatsvertrag geregelten Gebot, die Inanspruchnahme von Rundfunk und deren Abrechnung anonym zu ermöglichen und verstoßen gegen das Prinzip der Datenvermeidung. Dies wäre nicht akzeptabel, zumal datenschutzfreundliche Varianten der Abrechnung - beispielsweise durch den Einsatz von vorbezahlten Karten - ohne wirtschaftliche Einbußen zur Verfügung stehen.

Die Datenschutzbeauftragten des Bundes und der Länder fordern deshalb die Länder auf, die Einhaltung der datenschutzrechtlichen Anforderungen des Rundfunkstaatsvertrages gegenüber den Veranstaltern durchzusetzen, und eine anonyme Nutzung von Rundfunkprogrammen auch in Zukunft sicherzustellen.

Angesichts der immer umfassenderen Individualisierung und Registrierbarkeit des Mediennutzungsverhaltens erinnert die Konferenz der Datenschutzbeauftragten des Bundes und der Länder an ihre Forderung, das grundgesetzlich geschützte Fernmeldegeheimnis zu einem allgemeinen Mediennutzungsgeheimnis weiterzuentwickeln.

16.2.20 Entschließung der 73. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 8./9. März 2007 in Erfurt: Elektronischer Einkommensnachweis muss in der Verfügungsmacht der Betroffenen bleiben

Mit dem Verfahren ELENA (elektronische Einkommensnachweise) sollen die Einkommensdaten sämtlicher abhängig Beschäftigter in einem bundesweiten Register gespeichert werden. Dieses Verfahren ist angesichts der Sensibilität und des Umfangs der dabei erfassten personenbezogenen Daten von erheblicher datenschutzrechtlicher Brisanz.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist darauf hin, dass ein derartiges Register nur dann eingerichtet werden darf, wenn die verfassungsrechtlichen Voraussetzungen erfüllt und die gesetzlichen und technisch-organisatorischen Vorkehrungen zum Schutz der dort gespeicherten Daten getroffen werden.

Zu den wesentlichen verfassungsrechtlichen Voraussetzungen für die Einrichtung des Registers gehören der Nachweis der Erforderlichkeit und die Verhältnismäßigkeit.

Angesichts bestehender Zweifel daran, dass diese Voraussetzungen gegeben sind, muss belastbar dargelegt werden, dass die Daten für die jeweiligen Zwecke tatsächlich benötigt werden und dass der angestrebte Zweck nicht mit einem geringeren Eingriff in das Recht auf informationelle Selbstbestimmung erreicht werden kann.

Im Hinblick auf den vom Bundesministerium für Wirtschaft und Arbeit erarbeiteten Referentenentwurf sieht die Konferenz darüber hinaus in den folgenden Punkten Klärungsbedarf:

- Es muss gesetzlich festgelegt werden, dass die Daten aus der Datenbank nur mit Mitwirkung der Teilnehmerinnen und Teilnehmer des Verfahrens zu entschlüsseln sind.
- Das Verfahren muss so ausgestaltet werden, dass die Ver- und Entschlüsselung der Daten ohne Vorliegen der Signaturkarte des Betroffenen nur in klar definierten Ausnahmefällen durch eine unabhängige Treuhänderstelle möglich ist.
- Sämtliche im Rahmen des Verfahrens verarbeiteten Daten müssen einem gesetzlichen Beschlagnahmeschutz unterworfen sein.
- Die technischen Komponenten müssen auf der Basis einer unabhängigen Prüfung zertifiziert werden.

16.2.21 Entschließung der 73. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8./9. März 2007 in Erfurt: Keine heimliche Online-Durchsuchung privater Computer

Bisher ist nur die offene Durchsuchung privater Computer gesetzlich geregelt. Trotzdem wollen staatliche Behörden auch heimliche Online-Durchsuchungen durchführen. Bei einer Online-Durchsuchung dringen Sicherheitsbehörden mittels sog. „Trojaner“ heimlich in den Rechner ein und verschaffen sich Zugriff auf alle gespeicherten Daten.

Der Bundesgerichtshof hat in seinem Beschluss vom 31. Januar 2007 (StB 18/06) die Auffassung der Datenschutzbeauftragten des Bundes und der Länder bestätigt, dass eine heimliche Online-Durchsuchung im Bereich der Strafverfolgung rechtswidrig ist. Weder die Bestimmungen zur Wohnungsdurchsuchung noch zur Telekommunikationsüberwachung können zur Rechtfertigung der heimlichen Durchsuchung und Ausforschung privater Computer herangezogen werden.

Die Datenschutzbeauftragten des Bundes und der Länder wenden sich entschieden gegen die Einführung entsprechender Eingriffsgrundlagen sowohl im repressiven als auch im präventiven Bereich. Sie appellieren an die Gesetzgeber, es beim bisherigen Rechtszustand des „offenen Visiers“ zu belassen. Der Staat darf nicht jede neue technische Möglichkeit ungeachtet ihrer Eingriffstiefe zur Ausforschung einsetzen. Dies gilt auch dann, wenn wichtige Belange, wie z. B. die Strafverfolgung, betroffen sind.

Hier ist ein Umdenken erforderlich. Es muss ein Raum der Privatsphäre bleiben, der nicht durch heimliche staatliche Überwachungsmaßnahmen ausgehöhlt werden darf.

Eine heimliche Online-Durchsuchung greift tief in die Privatsphäre ein. Die auf einem Computer gespeicherten Daten können aufgrund ihrer Vielzahl und besonderen Sensibilität Einblick in die Persönlichkeit der Betroffenen geben. Der Schutz des Kernbereichs privater Lebensgestaltung wird gefährdet, wenn der Staat heimlich und fortdauernd in private Computer eindringt, um dort personenbezogene Daten auszuspähen. Dies gilt umso mehr, wenn Nachrichtendienste die Möglichkeit heimlichen Zugriffs auf diese Informationen erhalten, obwohl ihnen nicht einmal die offene Erlangung durch eine Beschlagnahme gestattet ist.

Es ist Aufgabe des Staates dafür Sorge zu tragen, dass den Einzelnen die Möglichkeit zur Entfaltung ihrer Persönlichkeit bleibt. Diese Möglichkeit würde unvertretbar eingeschränkt, wenn Durchsuchungsmaßnahmen zugelassen würden, bei denen aufgrund ihrer Heimlichkeit keine Person wissen kann, ob, wann und in welchem Umfang sie von ihnen bereits betroffen ist oder in Zukunft betroffen sein wird. Der Gesetzgeber sollte deshalb davon absehen, derartige neue Eingriffsbefugnisse zu schaffen, nur weil sie ihm technisch möglich erscheinen und ihre Zweckmäßigkeit behauptet wird. Die technische Entwicklung allein kann nicht der Maßstab für die Rechtfertigung von Eingriffen sein.

Die Konferenz befürchtet massive Sicherheitseinbußen, weil zu erwarten ist, dass sich Computernutzer vor staatlicher Ausforschung zu schützen versuchen, indem sie etwa Softwaredownloads unterlassen. Somit werden aber auch die sicherheitstechnisch wichtigen Software-Updates verhindert und Computer anfälliger gegen Angriffe Krimineller. Die Einführung von Befugnissen zur Online-Durchsuchung würde das Ansehen des Rechtsstaats und das Vertrauen in die Sicherheit von Informationstechnik, insbesondere von E-Government und E-Commerce, massiv beschädigen. Schließlich würden die hohen Aufwendungen für IT-Sicherheit in Staat und Wirtschaft konterkariert. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert deshalb an die Bundesregierung, die Landesregierungen und die Parlamente, auf die Einführung derartiger Befugnisnormen zu verzichten.

16.2.22 Entschließung der 73. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8./9. März 2007 in Erfurt: Pläne für eine öffentlich zugängliche Sexualstraftäterdatei verfassungswidrig

In der aktuellen Diskussion um einen verbesserten Schutz von Kindern vor Sexualstraftätern wird u. a. die Einrichtung einer öffentlich zugänglichen Sexualstraftäterdatei mit Wohnsitzangaben gefordert. Es wird vorgeschlagen, die Namen und Adressen von

verurteilten Sexualstraftätern z.B. über das Internet zu veröffentlichen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder betont, dass an Kindern begangene Sexualstraftaten mit allen zur Verfügung stehenden rechtsstaatlichen Mitteln bekämpft werden müssen. Dies schließt jedoch die Anwendung eindeutig rechtsstaatswidriger Mittel aus. Um ein solches verfassungswidriges Mittel würde es sich aber bei einer solchen Datei handeln. Dadurch würden die Betroffenen an eine Art elektronischen Pranger gestellt. Sie würden durch die öffentliche Bloßstellung sozial geächtet. Tätern würde die Möglichkeit der Resozialisierung genommen, die ihnen nach unserer Rechtsordnung zusteht.

Der Vorschlag ist lediglich dazu geeignet, Misstrauen und Selbstjustiz zu fördern. Die Betroffenen könnten damit eher zu einem erhöhten Gefahrenpotenzial werden. Er sollte deshalb nach Auffassung der Datenschutzbeauftragten des Bundes und der Länder nicht weiter verfolgt werden.

16.2.23 Entschließung der 73. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8./9. März 2007 in Erfurt: Vorratsdatenspeicherung, Zwangsidentifikation im Internet, Telekommunikationsüberwachung und sonstige verdeckte Ermittlungsmaßnahmen

Die gesetzlichen Regelungen der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sollen nach der Ankündigung der Bundesregierung unter Berücksichtigung der Rechtsprechung des Bundesverfassungsgerichts einer umfassenden Neuregelung unterzogen werden. Die Bundesregierung will in diesem Zusammenhang auch die europäische Richtlinie zur Vorratsspeicherung von Telekommunikationsverkehrsdaten umsetzen. Das Bundesministerium der Justiz hat zwischenzeitlich einen Referentenentwurf vorgelegt.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder betont erneut, dass die Vorratsdatenspeicherung deutschem Verfassungsrecht widersprechen würde. Nach der Rechtsprechung des Bundesverfassungsgerichts ist die Speicherung von Daten auf Vorrat zu nicht hinreichend bestimmbaren Zwecken verfassungswidrig. Zudem würde die für eine freiheitliche Gesellschaft konstitutive unbefangene Kommunikation erheblich beeinträchtigt. Die Konferenz fordert die Bundesregierung auf, die Umsetzung der Europäischen Richtlinie zur Vorratsdatenspeicherung zumindest solange zurückzustellen, bis der bereits angerufene Europäische Gerichtshof über deren Rechtmäßigkeit entschieden hat.

Die geplante Ausweitung der Vorratsdatenspeicherung geht weit über die europarechtliche Umsetzungsverpflichtung hinaus und wäre ein zusätzlicher unverhältnismäßiger

Eingriff in die Kommunikationsfreiheit der Bürgerinnen und Bürger. So sollen die Daten auch zur Verfolgung von Straftaten von erheblicher Bedeutung sowie mittels Telekommunikation begangener Straftaten genutzt werden. Zudem soll die Möglichkeit zur anonymen E-Mail-Kommunikation abgeschafft und die Nutzenden öffentlich zugänglicher E-Mail-Dienste sollen zur Angabe ihres Namens und ihrer Adresse verpflichtet werden. Diese Angaben sollen außerdem einer Vielzahl von Behörden zum Online-Abruf zur Verfügung gestellt werden, darunter der Polizei, den Staatsanwaltschaften, den Nachrichtendiensten, dem Zoll und der Bundesanstalt für Finanzdienstleistungsaufsicht. Auch dies begegnet erheblichen datenschutzrechtlichen Bedenken.

Zwar stärken einige der vorgesehenen Änderungen der Strafprozessordnung die rechtsstaatlichen und grundrechtlichen Sicherungen bei verdeckten strafprozessualen Ermittlungsmaßnahmen. Es besteht jedoch noch erheblicher Verbesserungsbedarf, insbesondere im Hinblick auf den Schutz des Kernbereichs privater Lebensgestaltung, den Schutz von Berufsgeheimnisträgerinnen und Berufsgeheimnisträgern und die Voraussetzungen der Telekommunikationsüberwachung:

- Mit einer erneuten Ausweitung des Straftatenkatalogs für die Telekommunikationsüberwachung würde die Tendenz zunehmender Überwachungsmaßnahmen in verstärktem Maße fortgesetzt. Der Katalog sollte deshalb mit dem Ziel einer deutlichen Reduzierung kritisch überprüft werden. Es sollten nur Straftaten aufgenommen werden, deren Aufklärung in besonderem Maße auf die Telekommunikationsüberwachung angewiesen ist, die mit einer bestimmten gesetzlichen Mindeststrafe (z. B. ein Jahr) bedroht sind und die auch im Einzelfall schwer wiegen.

- Die vorgesehene Kernbereichsregelung ist ungenügend. Sie nimmt in Kauf, dass regelmäßig auch kernbereichsrelevante Informationen erfasst werden. Für solche Informationen muss stattdessen grundsätzlich ein Erhebungsverbot gelten. Erkenntnisse aus dem Kernbereich der privaten Lebensgestaltung, die dennoch erlangt werden, müssen zudem einem absoluten Verwertungsverbot unterliegen, nicht nur für Strafverfahren.

- Der Schutz des Kernbereichs privater Lebensgestaltung ist nicht nur in den Bereichen der Wohnraum- und Telekommunikationsüberwachung zu gewährleisten. Auch für alle anderen verdeckten Ermittlungsmaßnahmen ist eine Regelung zum Schutz des Kernbereichs zu treffen.

- Für die Kommunikation mit Berufsgeheimnisträgerinnen und Berufsgeheimnisträgern sollte ein absolutes Erhebungs- und Verwertungsverbot geschaffen werden, das dem jeweiligen Zeugnisverweigerungsrecht entspricht. Dieses sollte unterschiedslos für alle Berufsgeheimnisträgerinnen und Berufsgeheimnisträger und deren Berufshelferinnen und Berufshelfer gelten. Die im Entwurf enthaltene Differenzierung

zwischen bestimmten Gruppen von Berufsgeheimnisträgerinnen und Berufsgeheimnisträgern ist sachlich nicht gerechtfertigt.

- Für Angehörige i. S. v. § 52 StPO sollte ein Erhebungs- und Verwertungsverbot für die Fälle vorgesehen werden, in denen das öffentliche Interesse an der Strafverfolgung nicht überwiegt. Die besonderen verwandtschaftlichen Vertrauensverhältnisse dürfen nicht ungeschützt bleiben.

- Für teilnehmende Personen von Kernbereichsgesprächen, die weder Berufsgeheimnisträgerinnen und Berufsgeheimnisträger noch Angehörige i. S. v. § 52 StPO sind, sollte insoweit ein Aussageverweigerungsrecht aufgenommen werden. Andernfalls bleibt der Kernbereich teilweise ungeschützt.

- Für die sog. Funkzellenabfrage, die alle Telefonverbindungen im Bereich einer oder mehrerer Funkzellen erfasst, sollten klare und detaillierte Regelungen mit engeren Voraussetzungen normiert werden. Diese sollten vorsehen, dass im Rahmen einer besonderen Verhältnismäßigkeitsprüfung die Anzahl der durch die Maßnahmen betroffenen unbeteiligten Dritten berücksichtigt und die Maßnahme auf den räumlich und zeitlich unbedingt erforderlichen Umfang begrenzt wird. Die Unzulässigkeit der Maßnahme zur Ermittlung von Tatzeuginnen und Tatzeugen sollte ins Gesetz aufgenommen werden.

- Die aufgrund einer Anordnung der Staatsanwaltschaft bei Gefahr in Verzug erlangten Daten dürfen nicht verwertet werden, wenn die Anordnung nicht richterlich bestätigt wird. Dieses Verwertungsverbot darf nicht - wie im Entwurf vorgesehen - auf Beweiszwecke begrenzt werden.

- Art und Umfang der Begründungspflicht für den richterlichen Beschluss der Anordnung der Telekommunikationsüberwachung sollte wie bei der Wohnraumüberwachung im Gesetz festgeschrieben werden. Im Sinne einer harmonischen Gesamtregelung sollten darüber hinaus qualifizierte Begründungspflichten für sämtliche verdeckte Ermittlungsmaßnahmen geschaffen werden.

- Zur Gewährleistung eines effektiven Rechtsschutzes ist sicherzustellen, dass sämtliche Personen, die von heimlichen Ermittlungsmaßnahmen betroffen sind, nachträglich von der Maßnahme benachrichtigt werden, soweit diese bekannt sind oder ihre Identifizierung ohne unverhältnismäßige weitere Ermittlungen möglich ist und nicht überwiegende schutzwürdige Belange anderer Betroffener entgegenstehen. Darüber hinaus sollte bei Massendatenerhebungen über eine ergänzende Benachrichtigung durch eine öffentliche Bekanntmachung der Maßnahme nachgedacht werden.

- Die für die Telekommunikationsüberwachung vorgesehenen Berichts- und Statistikpflichten sollten um Angaben zur Dauer der Überwachung, zur Anzahl der Gespräche und zur Benachrichtigung Betroffener ergänzt werden.

- Die im Entwurf enthaltenen erweiterten Eingriffsgrundlagen sollten befristet und einer unabhängigen, gründlichen und wissenschaftlich unterstützten Evaluation unterzogen werden.

16.2.24 Entschließung zwischen der 73. und 74. Konferenz der Datenschutzbeauftragten des Bundes und der Länder: Telekommunikationsüberwachung und heimliche Ermittlungsmaßnahmen dürfen Grundrechte nicht aushebeln

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder wendet sich mit Nachdruck gegen die von Bundesregierung und Bundesratsgremien geplante Einführung der Vorratsspeicherung von Telekommunikationsverkehrsdaten und die Verschärfungen verdeckter Ermittlungsmaßnahmen, vor allem durch Telekommunikationsüberwachung:

Die Datenschutzbeauftragten haben am 8./9. März 2007 auf ihrer Konferenz in Erfurt einen ersten Gesetzentwurf als verfassungswidrig beanstandet. Insbesondere haben sie vor heimlichen Online-Durchsuchungen und der Vorratsdatenspeicherung gewarnt. Damit würde tief in die Privatsphäre eingegriffen und das Kommunikationsverhalten der gesamten Bevölkerung - ob via Telefon oder Internet - pauschal und anlasslos erfasst.

Die einhellige Kritik der Datenschutzbeauftragten und ihre Aufforderung, stattdessen verhältnismäßige Eingriffsregelungen zu schaffen, wurden von der Bundesregierung nicht beachtet. In ihrem Gesetzentwurf vom 27. April 2007 wird demgegenüber der Schutz der Zeugnisverweigerungsberechtigten verringert, Benachrichtigungspflichten gegenüber betroffenen Personen werden aufgeweicht, Voraussetzungen für die Erhebung von Standortdaten in Echtzeit und für den Einsatz des IMSI-Catchers erheblich ausgeweitet und die Verwendungszwecke für die auf Vorrat gespeicherten Daten über die europarechtlichen Vorgaben hinaus auch auf leichte Straftaten, auf Zwecke der Gefahrenabwehr und sogar der Nachrichtendienste erstreckt.

Die nun im Bundesratsverfahren erhobenen zusätzlichen Forderungen zeugen von mangelndem Respekt vor den Freiheitsrechten der Bürgerinnen und Bürger. Dies zeigen folgende Beispiele: Die ohnehin überzogene Speicherdauer aller Verkehrsdaten wird von 6 auf 12 Monate verlängert. Die Überwachungsintensität erhöht sich durch eine Verschärfung der Prüfpflichten der Telekommunikationsunternehmen - bis zum Erfor-

dernis des Ablichtens und Aufbewahrens von Identitätsnachweisen aller Personen, die Prepaid-Produkte nutzen wollen. Die Sicherheitsbehörden erhalten Auskunft über Personen, die bestimmte dynamische IP-Adressen nutzen. Ausschüsse des Bundesrates wollen die Nutzung dieser Daten sogar zur zivilrechtlichen Durchsetzung der Rechte an geistigem Eigentum gestatten und bewegen sich damit weit jenseits des durch die EG-Richtlinie zur Vorratsspeicherung abgesteckten Rahmens, die Nutzung auf die Verfolgung schwerer Straftaten zu beschränken. Weiterhin ist eine Ausdehnung der Auswertung von Funkzellendaten von Mobiltelefonen mit dem Ziel der Ermittlung des Aufenthaltes von möglichen Zeuginnen und Zeugen geplant. Daten, die Beweiserhebungs- oder -verwertungsverboten unterliegen, sollen nicht unmittelbar gelöscht, sondern nur gesperrt werden.

Ganz nebenbei will der Innenausschuss des Bundesrats eine Rechtsgrundlage für die heimliche Online-Durchsuchung von Internet-Computern schaffen. Allein die Zulassung dieser Maßnahme würde rechtsstaatlichen Grundsätzen eklatant widersprechen und das Vertrauen in die Sicherheit der Informationstechnik massiv beschädigen.

Das Bundesverfassungsgericht hat in letzter Zeit eine Reihe von Sicherheitsgesetzen mit heimlichen Erhebungsmaßnahmen aufgehoben. Auch europäische Gerichte haben Sicherheitsmaßnahmen für rechtswidrig erklärt. Eine Entscheidung des Europäischen Gerichtshofs über die Verpflichtung zur Vorratsdatenspeicherung von Telekommunikationsverbindungsdaten sollte abgewartet werden ebenso wie die Entscheidung des Bundesverfassungsgerichtes zur nordrhein-westfälischen Regelung, die dem Verfassungsschutz die Online-Durchsuchung erlaubt.

Die Forderungen im Gesetzgebungsverfahren zeugen von einem überzogenen Sicherheitsdenken. Sie führen dazu, dass die Freiheitsrechte der Bevölkerung untergraben werden. Sicherheit in der Informationsgesellschaft ist nicht mit überbordenden Überwachungsregelungen zu erreichen, sondern nur durch maßvolle Eingriffsbefugnisse mit effektiven grundrechtssichernden Verfahrensregelungen und durch deren besonnene Anwendung. Die betroffenen Grundrechte verkörpern einen zu hohen Wert, als dass sie kurzfristigen Sicherheitsüberlegungen geopfert werden dürfen.

16.2.25 Entschließung der 74. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25./26. Oktober 2007 in Saalfeld: Gesetzesinitiative der Bundesregierung zu Auskunfteien und Scoring: Nachbesserung bei Auskunfteienregelungen gefordert

Die fortschreitende technologische Entwicklung führt zu immer weitreichenderer Erfassung und Verknüpfung von persönlichen Daten und ermöglicht deren Auswertung

für Kontroll- und Präventionszwecke. In der Privatwirtschaft ist daher ein engmaschiges Netz verschiedener Auskunftssysteme und branchenübergreifender Zentraldateien entstanden, die durch Profilbildung das Verhalten eines jeden Menschen ohne dessen Wissen und Wollen abbilden und bewerten können.

Vor diesem Hintergrund begrüßt die Konferenz der Datenschutzbeauftragten des Bundes und der Länder, dass das Bundesministerium des Innern endlich damit begonnen hat, die gesetzlichen Regelungen zu den Auskunfteien zu überarbeiten und neue Regelungen zum Scoring zu schaffen.

Die vorgesehenen Regelungen zu den Auskunfteien verschlechtern die Rechtsposition der Betroffenen. Sie tragen dem sich ständig weiter entwickelnden Auskunfteimarkt und den dadurch hervorgerufenen Bedrohungen für das Recht auf informationelle Selbstbestimmung nicht hinreichend Rechnung. Ziel einer gesetzlichen Regelung muss es sein, den rasant wachsenden, branchenübergreifenden Datenaustausch zu beschränken. Es kann nicht hingenommen werden, dass Auskunfteidienste nur einseitig das Informationsinteresse der angeschlossenen Unternehmen bedienen. Sie müssen auch in stärkerem Maße die schutzwürdigen Belange der betroffenen Bürgerinnen und Bürgern berücksichtigen. Mit der im Entwurf vorgesehenen Möglichkeit, die Auskunftstätigkeit auf jegliche rechtliche und wirtschaftliche Risiken zu erstrecken, wäre zu befürchten, dass letztlich bei allen vertraglichen Beziehungen - also auch bei Versicherungs- und Arbeitsverträgen - vorab Auskunfteien eingeschaltet werden. Damit würden die allgemeinen Vertragsrisiken im Wirtschaftsleben in nicht mehr angemessener Weise einseitig auf die Kundinnen und Kunden verlagert.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert den Gesetzgeber auf, die Situation der Verbraucherinnen und Verbraucher deutlich zu verbessern und mit dem Gesetzesvorhaben einen fairen Ausgleich zwischen den Interessen der Wirtschaft und der betroffenen Verbraucherinnen und Verbraucher zu schaffen. Die Konferenz hält es für dringend erforderlich, die Auskunfteitätigkeit auf kreditorische Risiken zu begrenzen. Zudem fordert die Konferenz, Auskunfteidienste branchenspezifisch zu begrenzen.

Der vorgelegte Referentenentwurf eines Gesetzes zur Änderung des Bundesdatenschutzgesetzes sieht beim Scoring nun Ansätze für ein transparenteres Verfahren für die Betroffenen vor. Es muss jedoch darauf geachtet werden, dass dieser Ansatz auch vorbehaltlos umgesetzt wird. Das Scoring, bei dem mittels einer mathematisch-statistischen Formel das zukünftige vertragstreue Verhalten eines Menschen durch einen Zahlenwert ausgedrückt wird, dringt seit Jahren in immer mehr Bereiche des Wirtschaftslebens vor. Den Betroffenen wurde jedoch bisher das Wissen darüber, wie sich der Scorewert zusammensetzt, vorenthalten. Diese Praxis soll der Gesetzentwurf beenden. Die Be-

troffenen sollen Auskunft darüber erhalten, welche Daten mit welcher Gewichtung in den jeweiligen Scorewert eingeflossen sind. Die vorgeschlagenen Regelungen gehen jedoch noch nicht weit genug. Unbedingt zu streichen ist etwa eine im Entwurf enthaltene Regelung, wonach die Auskunft mit der Begründung verweigert werden kann, es würden Geschäftsgeheimnisse offenbart.

16.2.26 Entschließung der 74. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25./26. Oktober 2007 in Saalfeld: Nein zur Online-Durchsuchung

Der Computer hat im täglichen Leben der meisten Menschen eine zentrale Bedeutung für die Aufbewahrung und Gestaltung privatester Informationen, wie Fotografien, Reiseberichte, Tagebuchaufzeichnungen, persönliche Briefe, Eindrücke, Vorstellungen und Gefühle. Die heimliche Online-Durchsuchung führt deshalb zu erheblichen Eingriffen in Grundrechte (informationelles Selbstbestimmungsrecht, Unverletzlichkeit der Wohnung, Telekommunikationsgeheimnis usw.). Die Installation von Überwachungssoftware etwa mit Hilfe des Internets oder die Versendung von E-Mails unter dem Namen einer anderen Behörde wird erwogen, sogar das unbemerkte Eindringen in Wohnungen zu diesem Zweck wird nicht ausgeschlossen.

Bei dem geforderten heimlichen Zugriff auf informationstechnische Systeme geht es nicht nur um „Online-Durchsicht“ als einmalige Durchsuchung und die damit verbundene Übertragung von Festplatteninhalten an die Strafverfolgungs- oder Sicherheitsbehörden, sondern auch um die anhaltende Überwachung, um das Ausspähen von Passworten und die Protokollierung aller elektronischen Aktivitäten. Auch sollen andere Kommunikations- und Datenverarbeitungssysteme, wie Computernetze, Mobiltelefone, PDA usw. in die heimliche Durchsuchung einbezogen werden. Dabei ist die Feststellung des Computers einer Zielperson technisch ohne Zusatzinformationen nicht ohne weiteres möglich. Die Gefahr ist daher sehr groß, dass von einer solchen Maßnahme eine Vielzahl von - auch unverdächtigen - Nutzerinnen und Nutzern betroffen sein werden.

Es steht fest, dass sich der unantastbare Kernbereich privater Lebensgestaltung bei Online-Durchsuchungen durch technische Mittel bei der Datenerhebung nicht schützen lässt. Ein automatisierter Kernbereichsschutz ist somit nicht realisierbar.

Darüber hinaus wird eingeräumt, dass sich mit Hilfe der entsprechenden Software die auf den Festplatten gespeicherten Inhalte manipulieren ließen, was die Beweiseignung der gewonnenen Erkenntnisse und damit - jedenfalls bei der Verfolgung von Straftaten - die Geeignetheit der Online-Durchsuchung in Frage stellt.

Derzeit wird zwar versichert, dass der Einsatz nur auf die Bekämpfung des Terrorismus sowie die Verfolgung schwerster Straftaten und insgesamt auf wenige Fälle beschränkt wird. Die Erfahrungen zeigen aber, dass solche Beschränkungen nicht von langer Dauer sein werden. So begründen z.B. die drohende Aufweichung der Zweckbindung der Mautdaten und die Entwicklung der Telekommunikationsüberwachung die Befürchtung, dass Online-Durchsuchungen entsprechend dem technischen Fortschritt als Standardmaßnahme künftig auch bei Gefahren und Straftaten von geringerer Bedeutung eingesetzt werden. Zudem ist davon auszugehen, dass Terrorverdächtige Mittel und Wege finden werden, durch geeignete Gegenmaßnahmen eine erfolgreiche Online-Durchsuchung zu verhindern. Die heimliche Online-Durchsuchung führt deshalb voraussichtlich nicht zu mehr Sicherheit, aber sicher zur Einschränkung der Freiheit.

Die Datenschutzbeauftragten des Bundes und der Länder bekräftigen daher ihre im Rahmen der 73. Konferenz im März 2007 erhobene Forderung an die Bundesregierung, die Landesregierungen und die Parlamente, auf die Einführung der repressiven und präventiven Online-Durchsuchung zu verzichten.

Sie halten es für zwingend notwendig, dass das Urteil des Bundesverfassungsgerichts in dem Verfahren gegen die Online-Durchsuchung im Verfassungsschutzgesetz Nordrhein-Westfalens abgewartet wird.

16.2.27 Technische Aspekte der Online-Durchsuchung, erarbeitet durch den Arbeitskreis „Technische und organisatorische Datenschutzfragen“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder

0 Vorbemerkung

Das vorliegende Dokument soll den Ablauf und die technischen Verfahren der geplanten Online-Durchsuchung erläutern und aus technischer Sicht bewerten.

In den Abschnitten 1 bis 4 wird die Online-Durchsuchung beschrieben. Diese Beschreibung basiert auf den Antworten des BMI vom 22. August 2007 zu den Fragenkatalogen des BMJ und der SPD-Bundestagsfraktion. In diesen Abschnitten werden vorwiegend Begriffe verwendet, die aus dem Fragenkatalog stammen, auch wenn sie nicht allgemein anerkannt bzw. akzeptiert sind.

Im Abschnitt 5 werden die Abläufe und Verfahren aus technischer Sicht bewertet. Die Beschreibungen und Schlussfolgerungen hat der AK Technik zusammengestellt. Die Bewertungen gehen von derzeit technisch grundsätzlich möglichen Szenarien aus. In vielen Punkten besteht allerdings noch erheblicher Klärungsbedarf.

1 Begriffe

Informationstechnisches System:

- Gegenstand der Online-Durchsuchung
- System aus Hardware, Software und Daten, das der Erfassung, Speicherung, Verarbeitung, Übertragung und Anzeige von Informationen und Daten dient
- kann bspw. Personalcomputer, Server, vernetzte Verbünde von Computern, Infrastrukturkomponenten (Router, Switche, DE-CIX-Einrichtungen), externe Speichermedien (z. B. CD-ROMs, DVDs, externe Festplatten, USB-Speicher), Fax-Geräte, Mobilgeräte (z. B. Handys, Smartphones, Blackberrys) betreffen

Online-Durchsuchung:

- Oberbegriff für Online-Durchsicht und Online-Überwachung

Online-Durchsicht:

- einmalige Durchsuchung eines informationstechnischen Systems

Online-Überwachung:

- Überwachung eines informationstechnischen Systems über einen gewissen Zeitraum
- Inhalte aktueller Telekommunikationsvorgänge sind nicht Gegenstand der Online-Überwachung

Quellen-TKÜ:

- ausschließliche Erhebung von Telekommunikationsinhalten; betrifft nicht sonstige, auf der Festplatte abgelegte Inhalte

Remote-Forensic-Software (RFS):

- interne Bezeichnung des BKA für die zu verwendende Software

2 Phasen der Online-Durchsuchung
2.1 Technische Vorabklärung
2.1.1 Art der Informationsgewinnung

- Telekommunikationsüberwachung
- Portscan
- herkömmliche Ermittlungsmaßnahmen

- Einsatz von V-Leuten
- Einsatz von verdeckten Ermittlern

2.1.2 Art der zu beschaffenden Informationen über das Zielsystem

- Betriebssystemtyp und -version
- Internetzugang
- Browsertyp und -Version
- installierte Software (Produkte und Versionen)
- Online-Verhalten der Zielperson
- Möglichkeiten der Einbringung der RFS

2.2 Technische Vorbereitung
2.2.1 Einbringungsmöglichkeiten der RFS
2.2.1.1 Aussagen des BMI im Fragenkatalog vom 22. August 2007

Das BMI bleibt bei der Beantwortung der Fragen hinsichtlich der Möglichkeiten der Einbringung sehr unkonkret und beschränkt sich auf Aussagen wie:

„Es gibt eine Vielzahl von Einbringungsmöglichkeiten, die auf Tauglichkeit für den jeweiligen Einsatz überprüft und eventuell angepasst werden müssen."

„Eine generelle Aussage zur genauen Einbringungsmethode ist nicht möglich ..."

„Es besteht Einigkeit darüber, dass kein Interesse daran besteht, Hintertüren in Betriebs- und Anwendungssysteme einzubauen ..."

„Die Einbringung der RFS im Wege der E-Mail-Kommunikation kann je nach Einzelfall ein geeignetes Mittel darstellen."

2.3 Technische Umsetzung
2.3.1 Zielstellung

Online-Durchsicht:

Was hat die Zielperson bezogen auf ihr informationstechnisches System in der Vergangenheit gemacht?

Online-Überwachung:

Was macht die Zielperson bezogen auf ihr informationstechnisches System aktuell?

2.3.2 Informationen/Aktivitäten

Folgende Informationen sollen erhoben bzw. Aktivitäten durchgeführt werden:

Online-Durchsicht:

- Informationen über das System selbst
- auf dem Zielsystem gespeicherte Daten
- Suche nach Dateien mit bestimmten Namen
- Suche nach Dateien mit bestimmten Dateiendungen
- Suche nach Eigenschaften/Attributen (z. B. Zugriffsdaten)
- Schlüsselwortsuche
- Suche in bestimmten Verzeichnissen
- Suche nach Dateien eines bestimmten Dateityps

Online-Überwachung:

- alle Funktionen der Durchsicht und zusätzlich
- Erfassung flüchtiger Daten (Passworteingaben; Texte, die nicht übertragen werden; in Bearbeitung befindliche verschlüsselte Dateien)
- Erfassung von Klartexten vor einer Verschlüsselung
- Erfassung von Klartexten nach einer Entschlüsselung
- Einsatz von Key-Loggern zum Abfangen von Tatstatureingaben, beispielsweise von kryptographischen Schlüsseln

An den Computer angeschlossene oder mit diesem kommunizierende Geräte wie Mikrofone, Webcams oder Scanner sollen nicht überwacht werden. Mit diesen Geräten erhobene und auf dem informationstechnischen System gespeicherte Daten können jedoch Gegenstand der Durchsicht/Überwachung sein.

Online-Durchsicht und Online-Überwachung sollen sich ebenfalls nicht auf Telekommunikationsdaten erstrecken. Die technische Vorgehensweise ist vergleichbar und offensichtlich wird auch der gleiche „technische Baukasten“, wenn auch mit unterschiedlichen Bausteinen, genutzt.

Wie eine Vermischung beider Maßnahmen verhindert werden soll, wird nicht beschrieben.

2.3.3 Auswahl/Eingrenzung der zu erhebenden Informationen

Die zu sichernde Datenmenge soll anhand von vorher festgelegten Suchkriterien begrenzt werden. Folgende Möglichkeiten sollen dabei technisch umsetzbar sein:

- Erfassen der Inhalte von Dateien,

- Recherche mittels Suchbegriffen,
- Recherche in gelöschten Texten,
- Überwachung von Befehlen und genutzten Funktionen,
- Recherche nach und Erhebung von Passwörtern, Signaturen und -schlüsseln,
- Einschränkung auf ein tägliches Überwachungszeitfenster (z. B. 20 - 22.00 Uhr),
- Einschränkung auf bestimmte Nutzer.

2.3.4 Umgehungs-/Überwindungsmöglichkeiten von Kryptierungen

Das BMI sieht mehrere Möglichkeiten, Kryptierungen zu umgehen, von denen jedoch nicht alle genutzt werden sollen.

a) Abzweigen von Klar-Informationen vor der Ver- bzw. nach der Entschlüsselung
- soll genutzt werden
b) Zugriff auf Schlüssel mit Sniffer-Software und/oder Key-Loggern
- ist eine der vorgesehenen Online-Maßnahmen
c) Verwendung von absichtlich geschwächten Verschlüsselungsprodukten
- „Der generelle Einbau von staatlichen Hintertüren ist derzeit politisch nicht gewollt."
d) treuhänderische Hinterlegung von kryptographischen Schlüsseln (key escrow)
- „... in Deutschland politisch nicht durchsetzbar ... und technisch wenig erfolgversprechend..."

2.3.5 Ausleitung der Informationen

Die gewonnenen Ergebnisse werden so lange auf dem informationstechnischen System zwischengelagert, bis eine Internetverbindung durch die Zielperson hergestellt wird. Die Daten werden verschlüsselt abgelegt. Nach der Übertragung auf den Rechner der Sicherheitsbehörde werden die Daten auf dem informationstechnischen System gelöscht.

2.4 Dauer und Beendigung der Maßnahme
2.4.1Dauer der Maßnahme
2.4.1.1 Online-Durchsicht

Die Dauer der Durchsicht und der anschließenden Übermittlung ist abhängig

- von dem Online-Verhalten der Zielperson,
- vom Durchsuchungszweck,
- von der Anzahl und der Größe der zu übertragenden Dateien,
- von der Bandbreite des TK-Anschlusses des Zielsystems,
- vom Betriebszustand des Systems,

- von den Sicherungsmaßnahmen, die die Zielperson getroffen hat.

Die Durchsicht und die anschließende Übertragung kann einen Zeitraum von wenigen Minuten bis zu mehreren Tagen in Anspruch nehmen.

2.4.1.2 Online-Überwachung

Die Überwachungsdauer ist in der Regel wesentlich länger als bei der Online-Durchsicht und soll sich aus dem dann gesetzlich festgelegten Überwachungszeitraum ergeben.

2.4.2 Zeitpunkt und Art der Beendigung

Die Maßnahme soll planmäßig beendet werden, wenn

- die erhobenen Daten als ausreichend angesehen werden,
- der ursprüngliche Verdacht entkräftet wurde,
- die Durchsuchungserlaubnis aufgehoben wurde oder
- der gesetzlich zulässige Überwachungszeitraum erreicht ist.

In diesen Fällen soll sich die RFS auf ein entsprechendes Kommando hin (manuelle Auslösung) selbst deinstallieren.

Darüber hinaus soll die RFS ein Verfallsdatum und Zähler erhalten, die eine Selbst-Deinstallation der Software gewährleisten. Auf diese Weise soll auch eine ungewollte, erneute Aktivierung der RFS etwa nach dem Wiederaufsetzen des Systems mittels Datensicherungen (Back-Up) verhindert werden.

Unter Umständen ist es erforderlich, dass die Maßnahme nicht planmäßig beendet werden muss, bspw.

- bei erfolgloser Kontaktaufnahme mit dem Zielsystem (falls bspw. keine Internet-verbindung durch die Zielperson aufgebaut wird) oder bei
- (der eigentlich ausgeschlossenen) Entdeckung der RFS durch Antivirenprogramme, IDS-Systeme oder ähnliche Tools.

Die Deinstallation soll sich ausschließlich auf die RFS auswirken und keine Beeinträchtigungen des Zielsystems nach sich ziehen.

Es ist nicht beabsichtigt, den „Ursprungszustand“ des Zielsystems nach der Deinstallation der RFS herzustellen, da sich das Zielsystem während der Laufzeit der RFS ohne-

hin ständig verändert. Lediglich Änderungen, die die RFS an der Systemkonfiguration vorgenommen hat, sollen bei der Deinstallation der RFS rückgängig gemacht werden.

3 IT-Sicherheitsrisiko für Zielrechner

Mit der selbstentwickelten Software RFS sollen keine Daten auf dem Zielsystem manipuliert werden. Durch Hinterlegung des Quellcodes der RFS etwa beim genehmigenden Richter soll die Nachprüfbarkeit dieser Aussage in einem späteren Verfahren garantiert werden können.

Sensible Infrastrukturen in Staat und Wirtschaft sollen nicht gefährdet sein, da keine Online-Durchsuchung von Rechnern in Behörden oder Unternehmen vorgesehen ist.

Die Nutzung der RFS durch Dritte für eigene Zwecke soll nicht möglich sein, da „... die Software keine eigenen Verbreitungsroutinen und auch einen wirksamen Schutz gegen Missbrauch beinhaltet."

Es soll sichergestellt sein, dass die Software RFS „... nicht ohne erheblichen Aufwand ..." dazu veranlasst werden kann, an einen anderen als den von den Sicherheitsbehörden benutzten Server zurückzumelden und dass die Software weder von außen erkannt noch angesprochen werden kann.

Der generelle Einbau von „staatlichen Hintertüren" in Verschlüsselungsprodukte ist derzeit politisch nicht gewollt. Es besteht Einigkeit darüber, dass kein Interesse daran besteht, „Hintertüren" in Betriebs- und Anwendungssysteme einzubauen. Sie hätten nicht nur für die IT-Sicherheit, sondern auch für die deutsche Wirtschaft fatale Konsequenzen.

4 Beweissicherheit/Computer-Forensik
4.1 „Konventionelle" Beweiserhebung auf Computersystemen

Das BMI beschreibt die konventionelle Durchführung einer Datenträgeruntersuchung (DTU) nur sehr kurz:

- Kopie anfertigen,
- Verifizierung der Kopie,
- Erstellen einer Sicherheitskopie,
- Auswertungen anhand der Kopie, ausführliche Dokumentation.

4.2 Beweiskraft der Online-Durchsuchung

Das BMI hat keine Zweifel an der Beweiskraft der Online-Durchsuchung und verweist

auf folgendes:

- Die Online-Durchsuchung soll lückenlos dokumentiert werden (z. B. die Einbringung der RFS, alle Remote-Zugriffe, alle auf dem Zielrechner durchgeführte Befehle).

- Die Integrität der übertragenen Daten soll durch Hash-, Verschlüsselungs- und Signaturverfahren sichergestellt werden.

Das BMI räumt jedoch ein, dass eine Wiederholung der Überwachungsaktivitäten „... wegen des dynamischen Charakters ...“ der gesamten Maßnahme nicht möglich ist.

Nach Ansicht des BMI ist die Beweiskraft jedoch nicht immer relevant. Lediglich bei der Nutzung der Online-Durchsuchung im Bereich der Strafverfolgung ist die forensische Beweiserhebung Zweck der Maßnahme. Bei der Nutzung als Maßnahme zur Gefahrenabwehr ist die Erkenntnisgewinnung einziger Zweck.

5 Bewertung und Schlussfolgerungen

5.1 Einbringung der RFS

Der „Erfolg“ der Online-Durchsuchung hängt maßgeblich davon ab, ob es technisch und organisatorisch möglich ist, die RFS unbemerkt in das Zielsystem einzubringen. Nachfolgend werden die Erfolgsaussichten bei den bisher diskutierten Einbringungsmethoden diskutiert und generelle Schutzmaßnahmen erläutert.

5.1.1 Einbringungsmöglichkeiten

Da das BMI nicht detailliert auf Einbringungsmöglichkeiten eingeht (vgl. Punkt 2.2.1.1), werden hier einige Möglichkeiten vorgestellt, die - nach dem derzeitigen Stand der Technik - prinzipiell geeignet sind, fremde Rechner unbemerkt mit Software zu infiltrieren.

a) mit „Hilfe“ der Zielperson:

- verheißungsvolle E-Mails / Instant Messages mit der RFS als Anhang
- offizielle E-Mails von Behörden mit der RFS als Anhang
- E-Mails, bei denen der Absender gefälscht wurde, und dem Adressaten vertrauenswürdig erscheint
- manipulierte Web-Seiten, von denen die RFS heruntergeladen wird
- Herumliegenlassen / Zusenden von CDs, USB-Sticks und ähnlichen Datenträgern

b) ohne Hilfe der Zielperson:

- Ausnutzen von Software-Sicherheitslücken mit spezieller, auf die jeweilige Lücke zugeschnittener Software (sog. Exploits)
  - Zero-Day-Exploit: erscheint meist am selben Tag, an dem eine Sicherheitslücke allgemein bekannt wird
  - Less-Than-Zero-Day-Exploit: wird bereits vor bekannt werden einer Sicherheitslücke angeboten
- von Herstellern eingebaute Hintertüren
- Hintertüren in staatlichen E-Government-Anwendungen
- Infektion von Downloads „on the fly“
- physischer Zugriff auf den Zielrechner durch Eindringen in die von der Zielperson benutzten Räume

5.1.2 „Erfolgsaussichten“ bei der Einbringung

a) mit „Hilfe“ der Zielperson:

- verheißungsvolle E-Mails / Instant Messages mit der RFS als Anhang
  -> geringe Erfolgsaussichten, weil sensibilisierte Zielpersonen kaum solche E-Mails öffnen werden
- offizielle E-Mails von Behörden mit der RFS als Anhang
  -> geringe Erfolgsaussichten, weil sensibilisierte Zielpersonen kaum solche E-Mails öffnen werden
- E-Mails, bei denen der Absender gefälscht wurde, und dem Adressaten vertrauenswürdig erscheint
  -> mittlere Erfolgsaussichten, sofern die Zielperson dem Absender ungeprüft vertraut
- manipulierte Web-Seiten, von denen die RFS heruntergeladen wird
  -> mittlere Erfolgsaussichten, sofern die Zielperson keine Sandbox einsetzt und konfiguriert
- Herumliegenlassen / Zusenden von CDs, USB-Sticks und ähnlichen Datenträgern
  -> geringe Erfolgsaussichten, weil sensibilisierte Zielpersonen kaum ihnen unbekannte Datenträger auf Rechnern mit sensiblen Inhalten nutzen werden

b) ohne Hilfe der Zielperson:

- Ausnutzen von Software-Sicherheitslücken (bekannte Lücken oder Zero-Day-Exploits/Less-Than-Zero-Day-Exploits)
  -> mittlere Erfolgsaussichten bei bereits länger bekannten Lücken, sofern keine aktuellen Patches eingespielt wurden
  -> hohe Erfolgsaussichten bei Zero-Day-Exploits, weil Schutzmöglichkeiten noch nicht verfügbar sind

-> sehr hohe Erfolgsaussichten bei Less-Than-Zero-Day-Exploits, weil praktisch kein Schutz möglich ist
- von Herstellern eingebaute Hintertüren
-> geringe Erfolgsaussichten, sofern die Zielperson Open-Source-Software einsetzt
- Hintertüren in E-Government-Anwendungen
-> geringe Erfolgsaussichten, weil die Zielpersonen solche Anwendungen kaum nutzen werden
- Infektion von Downloads „on the fly“
-> hohe Erfolgsaussichten, da nur wenige Downloads digital signiert sind
-> hohe Erfolgsaussichten auch bei signierten Downloads, sofern die Hersteller mitwirken
- physischer Zugriff auf die IT-Zielsysteme
-> geringe Erfolgsaussichten bei Einzelsystemen, da ständig unter Kontrolle der Nutzer (z. B. Notebooks)
-> hohe Erfolgsaussichten bei komplexen Systemen und Infrastrukturkomponenten, da Eingriffe nur schwer feststellbar sind

5.1.3 Generelle Gegenmaßnahmen und ihre Schutzwirkung

- Nutzung von zwei PCs (ein Online- und ein Offline-System)
  - Daten durchlaufen den Online-PC beim Senden und Empfangen nur verschlüsselt
  - Übertragung der Daten zum Bearbeiten (Lesen, Schreiben) bspw. per USB-Stick auf den Offline-PC
  -> verhindert das Auslesen mit hoher Wahrscheinlichkeit
- Live-System von CD/DVD
  - dauerhafte Änderungen am Betriebssystem mit Hilfe der RFS sind nicht möglich
  - nach jedem Neustart von CD/DVD ist der Originalzustand wieder hergestellt
  -> verhindert das Auslesen mit hoher Wahrscheinlichkeit
- Nutzung eines virtuellen Zweitsystems
  - geschützte Umgebung für das Betriebssystem
  - sicherer Kanal in das Gastsystem möglich
  -> verhindert das Auslesen aus der geschützten Umgebung mit hoher Wahrscheinlichkeit
- Einsatz von Virenscannern
  - einfache Scanner finden nur Schadsoftware mit bekannten Mustern (Signaturen)
  -> RFS soll hochspezialisiert sein und von handelsüblichen Scannern angeblich nicht entdeckt werden

  - gute Produkte suchen nicht nur nach bekannten Mustern, sondern versuchen, das Verhalten von Software zu analysieren (proaktive Verfahren wie Heuristik oder Sandbox-Technologie)
  -> ob hier die RFS unentdeckt bleibt, ist zumindest fraglich
- Einsatz von Intrusion Detection Systemen (IDS)
  - erkennen von Angriffsmustern und von Veränderungen der Systemkonfiguration
  - schon das Erkennen der Tatsache, dass ein System verändert wurde, könnte auf die RFS hindeuten
  -> ob hier die RFS unentdeckt bleibt, ist zumindest fraglich
- Einsatz von Firewalls
  - vom Nutzer zugelassene Kommunikation (E-Mails, Downloads) werden nicht unterbunden
  - verschlüsselter Datenverkehr ist ebenfalls nicht filterbar
  -> Schutz vor RFS kaum realisierbar
- Einsatz des TPM (Trusted Platform Modul)
  - erlaubt dem Betriebssystem, Veränderungen zu erkennen
  - gewollte Downloads werden möglicher Weise nicht als Risiko erkannt
  - Hintertüren von Softwareherstellern werden nicht erkannt
  -> Schutz vor RFS zur Zeit nicht abschließend bewertbar
- Nutzung des Systems ausschließlich nach Anmeldung mit Kennung und Passwort
  - bei Nutzerkennungen ohne Admin-Rechten können Installationsmöglichkeiten eingeschränkt werden
  - Software-Installation nur mit Admin-Rechten zulassen
  -> erschwert das Einbringen der RFS unter bestimmten Umständen
- komplette Festplattenverschlüsselung
  - Installationsmöglichkeiten insbesondere bei physikalischem Zugriff kaum gegeben
  -> erschwert das Einbringen der RFS unter bestimmten Umständen

5.2 Reichweite der Eingriffe

Die Tatsache, dass nicht nur Personalcomputer sondern beispielsweise auch Server (bspw. Mailserver), vernetzte Verbünde von Computern und komplexe Infrastrukturkomponenten (z. B. Router, Switche, DE-CIX-Einrichtungen) von der Online-Durchsuchung betroffen sein können (vgl. Punkt 1), verdeutlicht die Reichweite und damit die Eingriffstiefe dieser Maßnahme. Werden derartige IT-Komponenten überwacht muss davon ausgegangen werden, dass nicht nur Einzelpersonen, sondern immer eine kaum einzugrenzende Anzahl von Betroffenen überwacht wird. Das BMI weist zwar darauf hin, dass bei Systemen, die unter der administrativen Betreuung Dritter stehen, anstelle der Online-Überwachung grundsätzlich der direkte Weg zu den jeweiligen Stellen

gesucht würde, der aktuelle Gesetzentwurf schließt den Einsatz der RFS jedoch auch hier nicht aus.

Zudem lässt sich die Reichweite schon deshalb kaum einschätzen, weil es einer konkreten Definition des Begriffs „Verbund“ mangelt. Es kann sich dabei sowohl um ein kleines lokales Netz handeln als auch um ausgedehnte Firmen-Netze (Intranets). Dass unter diesen Voraussetzungen die Online-Durchsuchung nicht einmal mehr auf Deutschland beschränkt werden kann, bleibt vom BMI völlig unerwähnt.

Im Übrigen ist bereits bei der Online-Durchsuchung von Einzelsystemen wie Personalcomputern oder Laptops davon auszugehen, dass nicht nur Einzelpersonen überwacht werden. Auch in diesen Fällen ist nicht auszuschließen, dass mehrere Personen das System nutzen, und somit von der Maßnahme betroffen sind.

Die Reichweite der Eingriffe kann auch anhand der Art zu erhebenden Informationen (vgl. Punkt 2.3.2) verdeutlicht werden. Die Suche nach bestimmten Dateien bedeutet nämlich in der Praxis, dass bspw. gezielt nach E-Mail-Adressbüchern, Kontaktlisten, Logdateien, Schlüsselbünden, Konfigurationsdateien, Cache-Dateien, Browser-Historien oder Sicherheitskopien gesucht werden kann.

5.3 IT-Sicherheitsrisiko für den Zielrechner

Da grundsätzlich zu bezweifeln ist, dass eine komplexe Software wie die RFS vollständig fehlerfrei programmiert wurde, ist äußerst fraglich, ob

- die Software weder durch Antivirenprogramme noch durch IDS-Systeme entdeckt werden kann,
- die Nutzung der RFS durch Dritte für eigene Zwecke wirklich ausgeschlossen werden kann,
- die RFS nicht doch dazu veranlasst werden kann, Daten an einen anderen als den von den Sicherheitsbehörden benutzten Server zu senden und ob
- die Software tatsächlich einen wirksamen Schutz gegen Missbrauch beinhaltet (vgl. Punkt 3).

Im Übrigen schließt das BMI nicht vollständig aus, dass die RFS missbraucht werden kann. Zitat:

„Speziell wird sichergestellt, dass die Software *nicht ohne erheblichen Aufwand* dazu veranlasst werden kann, an einen anderen als den von den Sicherheitsbehörden benutzten Server zurückzumelden und dass die Software weder von außen erkannt noch angesprochen werden kann.“ Wie hoch der Aufwand tatsächlich ist, wäre zu prüfen.

Jedenfalls ist das BMI in der Pflicht, belastbare Nachweise für die Behauptungen vorzulegen, dass

- tatsächlich keine Daten auf dem Zielsystem manipuliert werden,
- sensible Infrastrukturen in Staat und Wirtschaft nicht gefährdet sind,
- die Nutzung der RFS durch Dritte für eigene Zwecke nicht möglich ist,
- die Software nicht dazu veranlasst werden kann, an einen anderen als den von den Sicherheitsbehörden benutzten Server zurückzumelden,
- die Software weder von außen erkannt noch angesprochen werden kann und
- keine Hintertüren oder absichtlich eingebaute Schwachstellen in Hard- und Software verwendet werden.

5.4 Beweissicherheit

5.4.1 Konventionelle Computer-Forensik

Um elektronisch gespeicherte Daten auf Computersystemen als rechtskräftige Beweise verwenden zu können, sind eine Reihe technisch-organisatorischer Anforderungen umzusetzen. Hansen/Krause erläutern den Ablauf wie folgt:

In der Regel sind vier Schritte erforderlich:

1) Identifizierung

- Klärung, welche Informationen als Beweise erhoben werden sollen
- Festlegen der Vorgehensweise und der Mittel/Werkzeuge

2) Sicherstellung

- Sicherstellung der Zielrechner in Anwesenheit von Zeugen und ggf. Eigner
- ggf. Sicherstellung weiterer Dateninhalte aus flüchtigen Speichern vor der Abschaltung des Systems
- Sicherung der Datenträger gegen nachträgliche Veränderungen (z. B. Schreibschutz, kryptographische Verfahren zur digitalen Signatur)
- Erstellen eine Image Kopie

3) Analyse

- die Analyse durch sachverständige Kriminaltechniker
- Analyse nie am Originalsystem sondern immer an der Kopie

4) Aufbereitung und Präsentation

- Zusammenfassung der Analyse in einem Bericht

5.4.2 Beweissicherheit der Online-Durchsuchung

Im Gegensatz zur konventionellen Computer-Forensik, die auf die garantierte Unveränderthеit des Untersuchungsgegenstandes setzt, ist bei der Online Durchsuchung die Veränderung des Untersuchungsgegenstandes - bedingt durch das Einbringen der RFS - die Voraussetzung für die Beweiserhebung. Schon diese Tatsache widerspricht allen Vorgaben der klassischen Computer-Forensik. Ob mit dem Start der RFS auf dem Zielsystem tatsächlich (weitere) Änderungen sicher ausgeschlossen werden können (vgl. Punkt 3), kann kaum zweifelsfrei bewiesen werden. Damit ist auch der Beweiswert der erhobenen Daten äußerst fraglich.

Ob es darüber hinaus möglich ist, die zu untersuchenden Daten bei der Übertragung zum Server der Sicherheitsbehörde verlässlich vor Manipulation und Veränderung zu schützen, ist fraglich. Es dürfte kaum möglich sein, auf einem fremdkontrollierten Zielsystem (nämlich durch die Zielperson) verlässlich kryptographische Verfahren wie etwa die digitale Signatur durchzuführen.

Auch die angeblich lückenlose Protokollierung aller Aktivitäten und die Hinterlegung des Quellcodes der RFS (vgl. Punkt 4.2) kann nicht garantieren, dass Daten auf dem Zielsystem verändert werden - und sei es durch Software-Fehler in der RFS oder im Betriebssystem des Zielsystems.

Der Nutzen der Hinterlegung des Quellcodes ist ohnehin mehr als fragwürdig. Mit dieser Maßnahme will das BMI offenbar sicherstellen, dass der Quellcode im Bedarfsfall vollständig analysiert werden kann. Zieht man jedoch in Betracht, dass eine Quellcodeanalyse einen erheblichen Aufwand an Zeit und hochqualifiziertem Fachpersonal erfordert, wird eine solche Analyse wohl kaum vor dem Einsatz der Software angefordert werden. Vielmehr ist anzunehmen, dass lediglich eine nachträgliche Quellcode-Analyse angefordert wird, um bspw. in einem strafrechtlichen Verfahren die „ordnungsgemäße“ Funktion der RFS beweisen zu können.

Doch selbst dieser Beweis muss unvollständig bleiben. Es ist davon auszugehen, dass der Vorgang der Online-Durchsuchung von den Sicherheitsbehörden von außen „gesteuert“ wird. So wird beispielsweise die Möglichkeit bestehen, durch „Nachladen“ von Softwarekomponenten im Laufe der Online-Durchsuchung die Originalsoftware zu verändern, um sie aktuellen Anforderungen entsprechend anpassen zu können (etwa Nachladen erweiterter Suchkriterien). Dass durch diese Maßnahme der Beweiswert des hinterlegten Quellcodes nichtig ist, versteht sich von selbst.

Der Beweiswert der mit der Online-Durchsuchung erhobenen Daten bleibt daher in jedem Fall äußerst fragwürdig.

5.5 Schutz des Kernbereichs der privaten Lebensgestaltung

Dass eine Online-Durchsuchung solche Bereiche unberücksichtigt lässt, die durch bestimmte Dateinamen oder Dateiendungen adressiert werden, ist kaum anzunehmen. Allein die Tatsache, dass eine Datei mit „Liebesbrief.doc“ bezeichnet ist, wird sicher nicht dazu führen, dass Inhalte dieser Datei nicht an den Server der Sicherheitsbehörde übertragen werden.

Auch die Suche nach Eigenschaften/Attributen wird kaum zu Einschränkungen führen, weil eine verlässliche Schlussfolgerung auf Inhalte nicht möglich ist.

Ebenso ist die Suche nach Schlüsselworten, die Suche in bestimmten Verzeichnissen oder die Suche nach Dateien eines bestimmten Dateityps keine geeignete Methode, Daten aus dem Kernbereich der privaten Lebensgestaltung zu schützen.

Selbst wenn Erkennungsalgorithmen entwickelt werden könnten, in deren Ergebnis der Kernbereich definiert werden kann, wäre immer eine Durchsuchung des Gesamtdatenbestandes nötig, um entsprechende Indexierungen zu ermöglichen. Es ist somit kein technisches Verfahren erkennbar, mit dem ein „automatisierter Kernbereichsschutz“ realisiert werden kann.

Das BMI räumt folgerichtig ein, dass „... der Schutz des Kernbereichs anderer Nutzer wie auch des Beschuldigten allein mit technischen Mitteln nicht abschließend garantiert werden kann ...“, und dieser Schutz nur im Rahmen der Auswertung der erhobenen Daten gewährleistet werden kann.

Im Ergebnis ist festzustellen, dass der Kernbereich der privaten Lebensgestaltung bei einer Online-Durchsuchung durch technische Mittel nicht angemessen geschützt werden kann.

Die Erklärungen des BMI und des BKA zur Zahl der zu erwartenden Online-Durchsuchungen (bisher wird von maximal 10 Maßnahmen pro Jahr gesprochen) darf nicht dazu führen, den Eingriff in den Kernbereich der privaten Lebensgestaltung zu verharmlosen und in der Folge die Online-Durchsuchung zu legitimieren. Selbst wenn die Online-Durchsuchung - angesichts geringer Fallzahlen - als angemessenes Mittel zur Terrorismus- bzw. Extremismusbekämpfung angesehen werden würde, darf nicht außer acht bleiben, dass der technische Fortschritt sehr schnell dazu führen kann, dass die Online-Durchsuchung zu einem Standardwerkzeug der Sicherheitsbehörden werden kann. Dann wäre vor dem Hintergrund der jetzigen technischen Möglichkeiten ein

Eingriffsinstrument legitimiert worden, das bei fortschreitender Technikentwicklung völlig unangemessen wäre.

Im Übrigen ist angesichts der künftig abnehmenden Anzahl der Festnetzanschlüsse und der zunehmenden Kommunikation per IP-Telefonie ohnehin zu hinterfragen, welche Fallzahlen künftig zu erwarten sind und ob die bisher vom BMI betonte Trennung der Online-Durchsuchung von der „Quellen-TKÜ“ Bestand haben wird. Aus den Aussagen des BMI zum Problem der verschlüsselten Kommunikation wird deutlich, dass die mit der RFS verbundenen technischen Möglichkeiten die Grundlage darstellen sollen, um angesichts der technischen Entwicklungen (Konvergenz der Netze, Verschlüsselung, Vielfalt der Kommunikationsdienste) die Strafverfolgungsbehörden technisch nicht den Anschluss verlieren zu lassen und ihnen die Möglichkeiten zu erhalten, über die sie gegenwärtig bei der TKÜ verfügen.

5.6 Auswirkungen auf das Vertrauen in die IT-Infrastruktur und Folgen für die Akzeptanz von E-Government-Verfahren

IT-Sicherheit und Datenschutz sind die zentralen Akzeptanzkriterien der sich herausbildenden Informationsgesellschaft und der weltweiten Daten- und Kommunikationsnetze. Eine Folge der heimlichen Online-Durchsuchung wird eine tiefgreifende Vertrauenskrise sein. Bürgerinnen und Bürger und möglicherweise auch Unternehmen werden nicht mehr bereit sein, staatliche E-Government-Angebote zu nutzen, da sie den Missbrauch dieser Verfahren für die Zwecke der Online-Durchsuchung befürchten.

So hat beispielsweise die Finanzverwaltung schon jetzt massive Bedenken geäußert, dass ihre Bemühungen um die breite Nutzung der elektronischen Steuererklärung (ELSTER) durch die Diskussionen um die Online-Durchsuchung konterkariert werden. Schon jetzt - vor dem Einsatz der Online-Durchsuchung - werden sinkende Nutzungszahlen erwartet.

Selbst die elektronische Kommunikation zwischen Bürgerinnen und Bürgern bzw. Unternehmen mit staatlichen Stellen per E-Mail wird künftig gemieden werden, weil das BMI nicht ausschließt, dass die RFS mittels E-Mails verbreitet wird.

Auch die elektronische Kommunikation mit der Wirtschaft wird in Mitleidenschaft gezogen werden. Wenn Kunden sich nicht mehr der Vertraulichkeit der elektronischen Kommunikation sicher sein können, werden sie wieder auf die konventionellen Kommunikationswege zurückgreifen. Sie werden dann möglicherweise auf Anwendungen wie Online-Banking und E-Commerce-Verfahren verzichten.

Zudem ist zu befürchten, dass etwa Personalcomputer nicht mehr auf dem aktuellen Sicherheitsstand gehalten werden. Aus Furcht vor infiltrierten Downloads könnten Nutzer beispielsweise auf die regelmäßigen Sicherheits-Updates verzichten. Dies wird zu einem Anstieg der Computerkriminalität führen, da Sicherheitslücken nicht mehr beseitigt werden.

Das BMI weist zwar darauf hin, dass so genannte Hintertüren nicht eingebaut werden sollen. Es ist jedoch - zumindest aus technischer Sicht - mit ziemlicher Sicherheit davon auszugehen, dass vorhandene Hintertüren und unveröffentlichte Sicherheitslücken genutzt werden. Insbesondere damit konterkariert das BMI jedoch die Beteuerungen der Bundesregierung, den Bürgern und der Wirtschaft eine sichere und vertrauenswürdige IT-Infrastruktur zur Verfügung zu stellen. Es ist nämlich zu befürchten, dass (evtl. zunächst nur) dem BMI bekannte Sicherheitslücken nicht so schnell wie möglich publiziert werden, damit Schutzmaßnahmen ergriffen werden können, sondern dass diese Lücken bewusst über längere Zeit offen gehalten werden, um sie für die Zwecke der Online-Durchsuchung zu nutzen. Damit kann insbesondere der Wirtschaft erheblicher Schaden zugefügt werden (Stichwort Computer-Spionage). Die Wahrscheinlichkeit ist nämlich sehr hoch, dass das BMI gerade nicht exklusive „Nutzungsrechte“ an solchen Sicherheitslücken hat.

Fraglich ist in diesem Zusammenhang auch, welche Rolle das Bundesamt für Sicherheit in der Informationstechnik (BSI) künftig spielen soll bzw. noch spielen kann. Das BMI weist zwar ausdrücklich darauf hin, dass das BSI angewiesen wurde, sich nicht aktiv an der Entwicklung der für die Online-Durchsuchung einzusetzenden Software zu beteiligen. Ob das BMI tatsächlich dauerhaft auf den Sachverstand des BSI verzichtet wird, darf zumindest bezweifelt werden. Das Vertrauen in das BSI als glaubwürdigem Berater in Fragen der IT-Sicherheit ist schon jetzt sowohl in der Wirtschaft als auch bei Bürgern nachhaltig beeinträchtigt.

Schließlich darf nicht außer Acht gelassen werden, dass auch Kriminelle das Verfahren der Online-Durchsuchung oder zumindest bewusst in Kauf genommene Sicherheitslücken nutzen werden. Die Tatsache, dass Sicherheitsbehörden beharrlich davon ausgehen, dass die Online-Durchsuchung technisch durchführbar ist, wird Kriminelle in zunehmendem Maße veranlassen, sich diese Methode für ihre Zwecke nutzbar zu machen. Selbst wenn die Online-Durchsuchung für Sicherheitsbehörden nicht verwendet werden dürfte - etwa in Folge einer Entscheidung des Bundesverfassungsgerichts - ist selbstverständlich davon auszugehen, dass Kriminelle alle technischen Möglichkeiten künftig nutzen werden.

Schon allein dieser Aspekt verdeutlicht, wie wichtig es künftig sein wird, alle Nutzer von Informations- und Kommunikations- technik weiter zu sensibilisieren. Es ist

auch Aufgabe der Datenschutzbeauftragten des Bundes und der Länder, sowohl die Verantwortlichen in Wirtschaft und Verwaltung als auch Bürgerinnen und Bürger zu informieren und zu beraten, um auch dadurch ein höheres Sicherheitsbewusstsein zu erreichen.

16.2.28 Entschließung der 74. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25./26. Oktober 2007 in Saalfeld: Zentrale Steuerdatei droht zum Datenmoloch zu werden

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hält es für inakzeptabel, dass die Bundesregierung mit dem Jahressteuergesetz 2008 im Schnelldurchgang ohne ausführliche parlamentarische Beratung die beim Bundeszentralamt für Steuern aufzubauende zentrale Steuerdatei um zusätzliche - teilweise sensible - Daten anreichern will. Zugleich droht die Steueridentifikationsnummer (Steuer-ID) bereits vor ihrer endgültigen Einführung zu einem allgemeinen Personenkennzeichen zu werden.

Der Gesetzentwurf sieht die Ablösung des Lohnsteuerkartenverfahrens durch ein elektronisches Abrufverfahren (ElsterLohn II) ab 2011 vor. Bereits am 9. November 2007 soll das Gesetz abschließend im Bundestag beraten werden. Geplant ist unter anderem, die in Zusammenhang mit der seit dem 1. Juli 2007 vergebenen Steuer-ID errichtete Datenbank um weitere Daten zu ergänzen, etwa um die Religionszugehörigkeit, Ehepartner/Ehepartnerinnen/Kinder und deren Steuer-ID, dazu Angaben über Steuerklassen. Hierbei werden auch zahlreiche Datensätze auf Vorrat aufgenommen, da auch Personen betroffen sind, die (noch) keine Arbeitnehmer/Arbeitnehmerinnen sind.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert vom Bundestag und Bundesrat, dieses Vorhaben der Umstellung auf ein elektronisches Verfahren mit dem Jahressteuergesetz 2008 nicht zu beschließen. Folgende Punkte sind datenschutzrechtlich kritisch:

- Der durch die Vergabe der Steueridentifikationsnummer an alle Steuerpflichtigen und damit für alle Einwohnerinnen und Einwohner der Bundesrepublik entstehende Datenpool erhält eine neue Dimension. Zwar sind die Lohnsteuerabzugsmerkmale auch bisher auf der Lohnsteuerkarte vermerkt. Die Speicherung dieser Daten in einer zentralen Datenbank würde aber erhebliche datenschutzrechtliche Fragen aufwerfen. In den zentralen Datenbestand würden die Daten aller Personen mit Lohnsteuerkarten einfließen, also auch von solchen Personen, die sich nicht in einem lohnsteuerpflichtigen Beschäftigungsverhältnis befinden. Es ist zweifelhaft, ob die Aufnahme dieses Personenkreises dem Erforderlichkeitsgrundsatz entspricht. Nützlichkeitserwägungen sind für eine Datenhaltung auf Vorrat in keinem Fall ausreichend.

- Die Daten würden bundesweit annähernd vier Millionen Arbeitgebern zur Verfügung stehen. Als einzige Sicherung ist dabei vorgesehen, dass nur ein autorisierter Arbeitgeber die Lohnsteuerabzugsmerkmale abrufen kann. Klärungsbedürftig ist allerdings, wie dies sichergestellt werden kann. Zwar ist ein Authentifizierungsverfahren für den Arbeitgeber vorgesehen. Die Frage ist jedoch, ob damit tatsächlich eine rechtswidrige Informationsbeschaffung Dritter auszuschließen ist. Zumindest sollten die Daten aus der zentralen Datenbank nur unter Mitwirkung der Betroffenen abgerufen werden können.

- Die gesetzlich vorgeschriebene Evaluierung des Verfahrens (§ 87a Abs. 6 AO) ist noch nicht erfolgt. Gleichzeitig existieren bereits jetzt Bestrebungen, die Kommunikationsplattform „Elster“ für Nutzungen durch andere Verwaltungszweige zu öffnen (OpenElster). Dies aber bedeutete, dass damit die Steuer-ID auch für die Identitätsfeststellung bei steuerfremden Anwendungen herangezogen werden könnte, ohne damit der strikten Zweckbindung nach § 139b Abs. 5 Abgabenordnung zu rein steuerlichen Zwecken Rechnung zu tragen. Diese Zweckbindung kann nach § 139b Abs. 2 AO auch nicht durch die jeweilige Einwilligung der betroffenen Bürgerinnen und Bürger überwunden werden. Mit OpenElster sollen diese Vorkehrungen offenbar aufgeweicht werden, bevor die Steuer-ID überhaupt eingeführt wurde. Allein dies macht deutlich, dass jede Erweiterung des zentralen Datenbestandes kritisch hinterfragt werden muss.

Schließlich ist zu befürchten, dass die vorgesehene Erweiterung der Datenbank beim BZSt nicht den Schlusspunkt darstellt. Die im neuen Datenpool gespeicherten Daten wären auch für Sozialleistungsträger und Strafverfolgungsbehörden interessant. Es gibt zahlreiche Beispiele, dass Daten, die zunächst nur für einen engen Zweck gespeichert werden dürfen, später für viele andere Zwecke verwendet werden: Die für steuerliche Zwecke erhobenen Daten über Freistellungsaufträge werden mit den ebenfalls beim BZSt gespeicherten Daten der Empfänger von BaföG- und anderen Sozialleistungen abgeglichen. Die Mautdaten, die zunächst nur zur Mautberechnung erhoben wurden, sollen zukünftig auch zur Strafverfolgung verwendet werden. Der zunächst ausschließlich zur Terrorismusbekämpfung und der Bekämpfung der organisierten Kriminalität eingeführte Kontendatenabruf steht heute auch Finanzämtern und anderen Behörden wie z. B. der Bundesagentur für Arbeit über das BZSt offen. Das BZSt enthält so einen einzigartigen aktuellen Datenpool aller Bundesbürgerinnen und -bürger, der wesentliche Meldedaten, Bankkontenstammdaten und Steuerdaten zentral verknüpfen kann.

16.2.29 Entschließung der 74. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25./26. Oktober 2007 in Saalfeld: Zuverlässigkeitsüberprüfungen bei Großveranstaltungen

Anlässlich der Fußball-WM 2006 wurden im Rahmen der Akkreditierung umfassende Zuverlässigkeitsüberprüfungen nach einem auf Verwaltungsebene festgelegten Verfahren durchgeführt. Dabei wurde auf die Datenbestände der Polizei- und Verfassungsschutzbehörden des Bundes und der Länder zurückgegriffen. Dieses gesetzlich nicht vorgesehene Verfahren soll nunmehr beliebigen weiteren Veranstaltungen als Vorbild dienen.

Solche Zuverlässigkeitsüberprüfungen greifen in das Grundrecht auf informationelle Selbstbestimmung ein. Grundrechtseingriffe dürfen nicht unter Umgehung gesetzlicher Vorschriften durchgeführt werden, die Voraussetzungen und Begrenzungen solcher Verfahren regeln. Die Sicherheitsüberprüfungsgesetze des Bundes und der Länder sind für die Durchführung von allgemeinen Zuverlässigkeitsprüfungen, z. B. anlässlich von Veranstaltungen, nicht einschlägig. Eine generelle rechtliche Grundlage für Zuverlässigkeitsüberprüfungen besteht außerhalb der spezialgesetzlichen Bestimmungen nicht.

Einwilligungen können - auch wenn die Betroffenen über die Umstände informiert wurden - diese Maßnahme alleine nicht legitimieren. Dies nicht nur deshalb, weil Betroffene oft Nachteile befürchten müssen, wenn sie die Einwilligung verweigern und insoweit eine echte Freiwilligkeit fehlt. Viele Regelungen zu Überprüfungsverfahren verlangen - zusätzlich - zu den materiellen und verfahrensrechtlichen Regelungen die Mitwirkung der betroffenen Personen in Form einer schriftlichen Erklärung bei der Einleitung einer solchen Überprüfung. Außerdem sollen die Vorschriften ein transparentes Verfahren gewährleisten, in dem u. a. die Rechte Betroffener geregelt sind, so etwa das Recht auf Auskunft oder Anhörung vor negativer Entscheidung. Diese flankierenden Schutzmechanismen sind bei Überprüfungsverfahren unerlässlich.

16.3 Sonstiges

16.3.1 Mustervertrag zur Auftragsdatenverarbeitung gemäß § 7 SächsDSG

Eine Beauftragung ist gemäß § 7 Abs. 1 Satz 1 SächsDSG nur zulässig, soweit gesetzlich nichts anderes bestimmt ist (vgl. z. B. § 203 StGB, § 30 AO, § 80 SGB X, § 33 Abs. 10 SächsKHG).

Die Inhalte des Vertrages sind im Einzelfall aufgabenspezifisch anzupassen.

Vereinbarung

zwischen dem/der

.....
- nachstehend Auftragnehmer genannt -
und dem/der

.....
- nachstehend Auftraggeber genannt -

§ 1 Gegenstand der Vereinbarung

(1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers.

(2) Der Auftrag umfasst folgende Arbeiten:

.....
(Definition der Aufgaben)

§ 2 Pflichten des Auftraggebers

(1) Für die Beurteilung der Zulässigkeit der Datenverarbeitung sowie für die Wahrung der Rechte der Betroffenen ist allein der Auftraggeber verantwortlich.

(2) Der Auftraggeber erteilt alle Aufträge oder Teilaufträge schriftlich. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam abzustimmen.

(3) Der Auftraggeber hat das Recht, Weisungen über Art, Umfang und Verfahren der Datenverarbeitung zu erteilen. Mündliche Weisungen sind unverzüglich schriftlich zu bestätigen.

Weisungsberechtigte Personen des Auftraggebers sind:

.....

Weisungsempfänger beim Auftragnehmer sind:

.....

Bei einem Wechsel oder einer längerfristigen Verhinderung des Ansprechpartners ist dem Vertragspartner unverzüglich schriftlich der Nachfolger bzw. der Vertreter mitzuteilen.

(4) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

(5) Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln.

§ 3 Pflichten des Auftragnehmers

(1) Der Auftragnehmer sichert zu, die Vorschriften des Sächsischen Datenschutzgesetzes zu befolgen. Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers. Er verwendet die zur Datenverarbeitung überlassenen Daten für keine anderen Zwecke. Kopien oder Duplikate werden ohne Wissen des Auftraggebers nicht erstellt.

(2) Der Auftragnehmer sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsmäßige Abwicklung aller vereinbarten Maßnahmen zu. Er sichert zu, dass die verarbeiteten Daten von sonstigen Datenbeständen getrennt werden.

(3) Der Auftragnehmer erklärt sich damit einverstanden, dass der Auftraggeber jederzeit berechtigt ist, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen im erforderlichen Umfang zu kontrollieren, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme.

(4) Die Verarbeitung von Daten in Privatwohnungen ist nur mit Zustimmung des Auftraggebers im Einzelfall gestattet. Soweit die Daten in einer Privatwohnung verarbeitet werden, ist der Zugang zur Wohnung durch den Auftraggeber (§ 3 Abs. 3) vorher mit dem Auftragnehmer abzustimmen. Der Auftragnehmer sichert zu, dass auch die anderen Bewohner dieser Privatwohnung mit dieser Regelung einverstanden sind.

(5) Nicht mehr benötigte Unterlagen mit personenbezogenen Daten und Dateien dürfen erst nach vorheriger Zustimmung durch den Auftraggeber datenschutzgerecht vernichtet werden.
(6) Nach Abschluss der vertraglichen Arbeiten hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen und erstellten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen. Die Datenträger des Auftragnehmers sind danach physisch zu löschen. Test- und Ausschussmaterial ist unverzüglich zu vernichten oder dem Auftraggeber auszuhändigen.
(7) [*1. Alternative*] Die Einschaltung von Subauftragnehmern ist ausgeschlossen. Die Beauftragung von Subunternehmen mit der Verarbeitung von personenbezogenen Daten ist in keinem Fall zulässig.

[*2. Alternative*] Die Beauftragung von Subunternehmen ist nur mit schriftlicher Zustimmung des Auftraggebers zugelassen. Der Auftragnehmer hat in diesem Falle vertraglich sicherzustellen, dass die vereinbarten Regelungen auch gegenüber Subunternehmern gelten. Er hat die Einhaltung dieser Pflichten regelmäßig zu überprüfen. Die Wieterleitung von Daten ist erst zulässig, wenn der Subunternehmer die Verpflichtung nach § 4 erfüllt hat. Zurzeit sind die in Anlage ..... mit Namen und Auftragsinhalt bezeichneten Subunternehmer mit der Verarbeitung von personenbezogenen Daten in dem dort genannten Umfang beschäftigt.
(8) Für die Sicherheit erhebliche Entscheidungen zur Organisation der Datenverarbeitung und zu den angewandten Verfahren sind mit dem Auftraggeber abzustimmen.

§ 4 Datengeheimnis

(1) Der Auftragnehmer verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des Auftraggebers das Datengeheimnis gemäß § 6 SächsDSG zu wahren und seine Mitarbeiter entsprechend zu verpflichten.
(2) Der Auftragnehmer bestätigt, dass ihm die einschlägigen datenschutzrechtlichen Vorschriften bekannt sind. Der Auftragnehmer sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht. Er überwacht die Einhaltung der datenschutzrechtlichen Vorschriften.

(3) Auskünfte darf der Auftragnehmer nur nach vorheriger schriftlicher Zustimmung durch den Auftraggeber erteilen.

§ 5 Datensicherungsmaßnahmen

(1) [*1. Alternative*] Bestandteil dieses Vertrages ist das Sicherheitskonzept vom ….., das den Vorgaben des § 9 SächsDSG und den Anforderungen der IT-Grundschutz-Kataloge des Bundesamtes für Sicherheit in der Informationstechnik (http://www.bsi.bund.de) entspricht.

[2. *Alternative*] Zu den Regelungstatbeständen des § 9 SächsDSG werden folgende technische und organisatorische Maßnahmen verbindlich festgelegt:

1. Vertraulichkeit (nur Befugte können personenbezogene Daten zur Kenntnis nehmen)

……
……
……
……

2. Integrität (Personenbezogene Daten bleiben während der Verarbeitung unversehrt, vollständig und aktuell.)

……
……
……
……

3. Verfügbarkeit (Personenbezogene Daten stehen zeitgerecht zur Verfügung und können ordnungsgemäß verarbeitet werden.)

……
……
……
……

4. Authentizität (Personenbezogene Daten können jederzeit ihrem Ursprung zugeordnet werden.)

……
……
……
……

5. Revisionsfähigkeit (Es kann festgestellt werden, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat.)

……
……
……
……

6. Transparenz (Die Verfahrensweisen bei der Verarbeitung personenbezogener Daten sind vollständig, aktuell und in einer Weise dokumentiert, dass sie in zumutbarer Zeit nachvollzogen werden können.)

……
……
……
……

(2) An der Erstellung der Verfahrensverzeichnisse hat der Auftragnehmer mitzuwirken. Er hat die erforderlichen Angaben dem Auftraggeber zuzuleiten.

(3) Der Auftragnehmer beachtet die Grundsätze ordnungsmäßiger Datenverarbeitung. Er gewährleistet die vertraglich vereinbarten und gesetzlich vorgeschriebenen Datensicherheitsmaßnahmen.

(4) Die technischen und organisatorischen Maßnahmen können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden. Wesentliche Änderungen sind schriftlich zu vereinbaren.

(5) Soweit die beim Auftragnehmer getroffenen Sicherheitsmaßnahmen den Anforderungen des Auftraggebers nicht genügen, benachrichtigt er den Auftraggeber unverzüglich. Entsprechendes gilt für Störungen sowie bei Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten. Er unterrichtet den Auftraggeber unverzüglich, wenn eine vom Auftraggeber erteilte Weisung nach seiner Meinung zu einem Verstoß gegen gesetzliche Vorschriften führen kann. Die Weisung braucht nicht befolgt zu werden, solange sie nicht durch den Auftraggeber geändert oder ausdrücklich bestätigt wird.

§ 6 Vertragsdauer

(1) Der Vertrag

- beginnt am ..... und endet am ...../

- mit Auftragserledigung /

- wird auf unbestimmte Zeit geschlossen.

Er ist mit einer Frist von ..... Monaten zum Quartalsende kündbar.

(2) Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen die Bestimmungen des Sächsischen Datenschutzgesetzes oder dieses Vertrages vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer den Zutritt des Auftraggebers oder der zuständigen Datenschutz-Aufsichtsbehörde verweigert.

§ 7 Vergütung

....

§ 8 Haftung

(1) Der Auftragnehmer haftet dem Auftraggeber für Schäden, die der Auftragnehmer, seine Mitarbeiter bzw. die von ihm mit der Vertragsdurchführung Beauftragten bei der Erbringung der vertraglichen Leistung schuldhaft verursachen.

(2) Für den Ersatz von Schäden, die ein Betroffener wegen einer nach dem Sächsischen Datenschutzgesetz oder anderen Vorschriften für den Datenschutz unzulässigen oder unrichtigen Datenverarbeitung im Rahmen des Auftragsverhältnisses erleidet, ist der Auftraggeber gegenüber den Betroffenen verantwortlich. Soweit der Auftraggeber zum Schadensersatz gegenüber dem Betroffenen verpflichtet ist, bleibt ihm der Rückgriff beim Auftragnehmer vorbehalten.

§ 9 Vertragsstrafe

Bei Verstoß gegen die Abmachungen dieses Vertrages, insbesondere gegen die Einhaltung des Datenschutzes, wird eine Vertragsstrafe von ..... € vereinbart.

§ 10 Nichterfüllung der Leistung

....

§ 11 Sonstiges

(1) Der Auftragnehmer übereignet dem Auftraggeber zur Sicherung die Datenträger, auf denen sich Dateien befinden, die Daten des Auftraggebers enthalten. Diese Datenträger sind besonders zu kennzeichnen.

(2) Sollte das Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen.

(3) Für Nebenabreden ist die Schriftform erforderlich.

(4) Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

§ 12 Wirksamkeit der Vereinbarung

Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

16.3.2 Widerspruch gegen die Weitergabe von Daten durch die Meldebehörde

An
Einwohnermeldeamt der

……..
Stadt/Gemeinde

……..
Straße, Hausnummer

……..
Postleitzahl, Gemeinde

Widerspruch gegen die Weitergabe von Daten durch die Meldebehörde		
Name:	Vorname:	Anschrift:
Hiermit widerspreche ich,		
1. der Weitergabe meiner Daten an öffentlich-rechtliche Religionsgesellschaften, der mein Ehepartner / Ehepartnerin / mein minderjähriges Kind, meine Eltern (nur im Falle der Minderjährigkeit der/des Antragstellenden) angehören – während ich diesen nicht angehöre (§ 30 Abs. 2 Satz 3 SächsMG).		☐
2. der Auskunftserteilung über meiner Meldedaten an Parteien, Wählergruppen und andere Träger von Wahlvorschlägen im Zusammenhang mit Wahlen zu parlamentarischen und kommunalen Vertretungskörperschaften (z.B. bei Landtagswahlen) bzw. der Nutzung der Daten für die Versendung von Wahlwerbung. (§ 33 Abs. 1 i.V.m. § 33 Abs. 4 SächsMG).		☐
3. der Weitergabe meiner Daten an Presse, Rundfunk und andere Medien zum Zwecke der Veröffentlichung von Altersjubilaren. (§ 33 Abs. 2 i.V.m. § 33 Abs. 4 SächsMG).		☐
4. der Weitergabe meiner Daten an Presse, Rundfunk und andere Medien zum Zwecke der Veröffentlichung von Ehejubilaren. (§ 33 Abs. 2 i.V.m. § 33 Abs. 4 SächsMG).		☐
5. der Veröffentlichung meiner Daten in Adressbüchern und ähnlichen Nachschlagewerken oder der Übermittlung meiner Daten an Andere zum Zwecke der Herausgabe solcher Werke (§ 33 Abs. 3 i.V.m. § 33 Abs. 4 SächsMG).		☐
6. Hiermit widerspreche ich der Erteilung der Einfachen Melderegisterauskunft im Wege des automatisierten Abrufes über das Internet (§ 32 Abs. 4 SächsMG).		☐
7. Hiermit widerspreche ich der Erteilung einer Melderegisterauskunft, die erkennbar für Zwecke der Direktwerbung begehrt wird (siehe BVerwG, Urteil v. 21.06.2006- 6 C 05/05; vgl. 13. Tätigkeitsbericht des Sächsischen Datenschutzbeauftragten, Nr. 5.3.5).		☐
Datum:		Unterschrift:

16.3.3 Merkblatt zur Anforderung von Kontoauszügen

Merkblatt zur Anforderung von Kontoauszügen

Um Ihren Antrag bearbeiten zu können, müssen Sie der ARGE die **Kontoauszüge der letzten 4 Wochen** von Ihrem Konto und den Konten der Mitglieder Ihrer Bedarfsgemeinschaft im Rahmen der Mitwirkungspflicht offenbaren (§ 60 Abs. 1 Erstes Buch Sozialgesetzbuch).

Um den Verwaltungsaufwand so gering wie möglich zu halten, werden bei der Antragsabgabe die Original-Kontoauszüge eingesehen und - soweit es erforderlich ist (z. B. bei ergänzenden Daten zum Antrag) - entsprechende Kopien dem Antrag zur weiteren Bearbeitung durch den zuständigen Mitarbeiter beigefügt.

Sie haben - sofern Sie selbst Kopien der Kontoauszüge dem Antrag beifügen wollen - die Möglichkeit, bestimmte Sollbuchungen aus Datenschutzgründen zu schwärzen. Damit Sie keine für die Antragsbearbeitung erheblichen Daten schwärzen, richten Sie sich bitte nach den folgenden **Schwärzungsregeln:**

1. Haben-Buchungen

Einnahmen des Kontoinhabers dürfen vorab nicht geschwärzt werden, da grundsätzlich das gesamte Einkommen bei der Hilfegewährung zu berücksichtigen ist (§ 11 SGB II).

2. Soll-Buchungen mit kleineren Beträgen

Die ausgeführten Buchungstexte zu Abbuchungen mit Beträgen bis 50 € können durch Sie in der Regel geschwärzt werden. Bei Ausgaben, zu denen Sie im Antragsvordruck – insbesondere im Punkt „Vermögen“ befragt wurden (Einzahlung in kapitalbildende Lebensversicherung, Bausparvertragseinzahlung usw.), ist eine Schwärzung unzulässig.

3. Sollbuchungen mit größeren Beträgen

Bei Abbuchungen mit Beträgen ab 50 € bitte vorab nichts schwärzen. Vom Antragsannehmer werden auf Ihr Verlangen hin alle nicht entscheidungserheblichen Daten der Buchungen in Ihrem Beisein eingeschwärzt.

4. Zulässigkeit von Teilschwärzungen

Abbuchungen mit entscheidungserheblichen und darüber hinausgehend weitere persönliche Informationen (z. B. Zahlung an eine Religionsgemeinschaft oder Mitgliedsbeitrag für eine bestimmte Partei/Gewerkschaft) können Sie auch nur zum Teil schwärzen. Wichtig ist, dass der eigentliche Verwendungszweck (z. B. „Spende“ oder „Mitgliedsbeitrag“ im Buchungstext erkennbar bleibt.

… **wenn Sie unsicher sind** ... ist Ihnen die Antragsannahme gern behilflich und schwärzt in Ihrem Beisein alle nicht erforderlichen Daten. - Wichtig ist allerdings, dass Sie die Originale vollständig zur Antragsabgabe mitnehmen.

A C H T U N G !!! Verpflichtung zur Aufbewahrung der Original-Kontoauszüge:
Spätestens 1 Jahr nach der Antragstellung werden die Kopien der Kontoauszüge datenschutzrechtlich vernichtet.
Die Original-Kontoauszüge stellen Beweisunterlagen dar, die Ihre Hilfebedürftigkeit untermauern.
Sie sind daher verpflichtet, alle Kontoauszüge – auch die bereits vorgelegten – aufzubewahren, um diese gegebenenfalls der ARGE für spätere Nachweiszwecke erneut vorlegen zu können.

Stichwortverzeichnis