Sächsischer Landtag
5. Wahlperiode

DRUCKSACHE 5/451

Schutz des Persönlichkeitsrechts im öffentlichen Bereich

14. Tätigkeitsbericht

des

Sächsischen Datenschutzbeauftragten

Dem Sächsischen Landtag

vorgelegt zum 31. März 2009

gemäß § 30 des Sächsischen Datenschutzgesetzes

Eingegangen am: 16. Dezember 2009 Ausgegeben am: 16. Dezember 2009

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: 0351/4935-401
Fax : 0351/4935-490
E-Mail: saechsdsb@slt.sachsen.de
Internet: www.datenschutz.sachsen.de
Besucheranschrift: Devrientstraße 1
01067 Dresden

Vervielfältigung erwünscht.

Herstellung: Parlamentsdruckerei

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.

ALG II-V	Arbeitslosengeld II/Sozialgeld-Verordnung vom 17. Dezember 2007 (BGBl. I S. 2942), zuletzt geändert durch Verordnung vom 23. Juli 2009 (BGBl. I S. 2340)
AO	Abgabenordnung in der Fassung der Bekanntmachung vom 1. Oktober 2002 (BGBl. I S. 3866; 2003 I S. 61), zuletzt geändert durch Art. 2 des Gesetzes vom 30. Juli 2009 (BGBl. I S. 2474)
AufenthG	Aufenthaltsgesetz vom 30. Juli 2004 (BGBl. I S. 1950), zuletzt geändert durch Art. 1 des Gesetzes vom 30. Juli 2009 (BGBl. I S. 2437)
BDSG	Bundesdatenschutzgesetz in der Fassung der Bekanntmachung vom 14. Januar 2003 (BGBl. I S. 66), zuletzt geändert durch Art. 1 des Gesetzes vom 14. August 2009 (BGBl. I S. 2814)
BeamtStG	Beamtenstatusgesetz vom 17. Juni 2008 (BGBl. I S. 1010), zuletzt geändert durch Art. 15 Abs. 16 des Gesetzes vom 5. Februar 2009 (BGBl. I S. 160)
BEEG	Bundeselterngeld- und Elternzeitgesetz vom 5. Dezember 2006 (BGBl. I S. 2748), zuletzt geändert durch Art. 10 des Gesetzes vom 28. März 2009 (BGBl. I S. 634)
BevStatG	Bevölkerungsstatistikgesetz in der Fassung der Bekanntmachung vom 14. März 1980 (BGBl. I S. 308), zuletzt geändert durch Art. 1 des Gesetzes vom 18. Juli 2008 (BGBl. I S. 1290)
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. 4 Abs. 10 des Gesetzes vom 11. August 2009 (BGBl. I S. 2713)

BRAO	Bundesrechtsanwaltsordnung vom 1. August 1959; in der im Bundesgesetzblatt Teil III, Gliederungsnummer 303-8, veröffentlichten bereinigten Fassung, geändert durch Art. 1 des Gesetzes vom 30. Juli 2009 (BGBl. I S. 2449)
BSHG	Bundessozialhilfegesetz in der Fassung der Bekanntmachung vom 23. März 1994 (BGBl. I S. 646, ber. S. 2975), Gesetz aufgehoben durch Art. 68 Abs. 1 Nr. 1 nach Maßgabe des Abs. 2 des Gesetzes vom 27. Dezember 2003 (BGBl. I S. 3022) (SozHiEinOG) mit Wirkung vom 1. Januar 2005; §§ 119 u. 147b treten gem. Art. 68 Abs. 2 am 31. Dezember 2003, § 101a am 1. Juli 2005 u. § 100 Abs. 1 am 31. Dezember 2006 außer Kraft
BStatG	Bundesstatistikgesetz vom 22. Januar 1987 (BGBl. I S. 462, (565)), zuletzt geändert durch Art. 3 des Gesetzes vom 7. September 2007 (BGBl. I S. 2246)
DlStatG	Dienstleistungsstatistikgesetz des Bundes vom 19. Dezember 2000 (BGBl. S. 1765), zuletzt geändert durch Art. 5 vom 17. März 2008 (BGBl. I S. 399)
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)
FeV	Fahrerlaubnis-Verordnung vom 18. August 1998 (BGBl. I S. 2214), zuletzt geändert durch Art. 3 der Verordnung vom 5. August 2009 (BGBl. I S. 2631)
FGG	Gesetz über die Angelegenheiten der freiwilligen Gerichtsbarkeit in der Fassung der Bekanntmachung vom 20. Mai 1898 (RGBl. I S. 771), zuletzt geändert durch Gesetz vom 12. März 2009 (BGBl. I S. 470), außer Kraft getreten am 1. September 2009 aufgrund Gesetz vom 17. Dezember 2008 (BGBl. I S. 2586)
FGO	Finanzgerichtsordnung vom 6. Oktober 1965 in der Fassung der Bekanntmachung vom 28. März 2001 (BGBl. I S. 442, 2262 (2002 I S. 679)), zuletzt geändert durch Art. 6 des Gesetzes vom 30. Juli 2009 (BGBl. I S. 2449)
FVG	Finanzverwaltungsgesetz vom 4. April 2006 (BGBl. I S. 846, 1202), zuletzt geändert durch Art. 6 des Gesetzes vom 10. August 2009 (BGBl. I S. 2702)

GG	Grundgesetz für die Bundesrepublik Deutschland vom 23. Mai 1949, zuletzt geändert durch Gesetz vom 29. Juli 2009 (BGBl. I S. 2248)
GKG	Gerichtskostengesetz vom 5. Mai 2004 (BGBl. I S. 718), zuletzt geändert durch Art. 12 des Gesetzes vom 30. Juli 2009 (BGBl. I S. 2479)
GO-LT	Geschäftsordnung des Landtages des Freistaates Sachsen 4. Wahlperiode vom 19. Oktober 2004 (SächsABl. S. 1226)
GPSG	Gesetz über technische Arbeitsmittel und Verbraucherprodukte - Geräte- und Produktsicherheitsgesetz vom 6. Januar 2004 (BGBl. I S. 2 (219)), zuletzt geändert durch Art. 3 Abs. 33 des Gesetzes vom 7. Juli 2005 (BGBl. I S. 1970)
HGB	Handelsgesetzbuch in der im Bundesgesetzblatt Teil III, Gliederungsnummer 4100-1 veröffentlichten bereinigten Fassung, zuletzt geändert durch Art. 6a des Gesetzes vom 31. Juli 2009 (BGBl. I S. 2512)
IfSG	Gesetz zur Verhütung und Bekämpfung von Infektionskrankheiten beim Menschen - Infektionsschutzgesetz vom 20. Juli 2000 (BGBl. I S. 1045), zuletzt geändert durch Art. 2a des Gesetzes vom 17. Juli 2009 (BGBl. I S. 2091)
JBeitrO	Justizbeitreibungsordnung vom 11. März 1937 im Bundesgesetzblatt Teil III, Gliederungsnummer 365-1 veröffentlichten bereinigten Fassung, zuletzt geändert durch Art. 4 Abs. 9 des Gesetzes vom 29. Juli 2009 (BGBl. I S. 2258)
JuSchG	Jugendschutzgesetz vom 23. Juli 2002 (BGBl. I S. 2730), zuletzt geändert durch Art. 3 Abs. 1 des Gesetzes vom 31. Oktober 2008 (BGBl. I S. 2149)
KomHVO	Verordnung des SMI über die kommunale Haushaltswirtschaft (Kommunalhaushaltsverordnung) vom 26. März 2002 (GVBl. S. 142, ber. S. 176), zuletzt geändert durch Art. 1 der Verordnung vom 7. Oktober 2005 (GVBl. S. 286)
KomKVO	Verordnung des SMI über kommunale Kassenführung vom 28. Februar 2005, zuletzt geändert durch Verordnung vom 22. Juli 2008 (GVBl. S. 524)

KomWO	Verordnung des SMI zur Durchführung des Gesetzes über die Kommunalwahlen im Freistaat Sachsen (Kommunalwahlordnung) vom 5. September 2003 (GVBl. S. 440), zuletzt geändert durch Verordnung vom 18. Februar 2009 (GVBl. S. 78)
KWG	Kreditwesengesetz in der Fassung der Bekanntmachung vom 9. September 1998 (BGBl. I S. 2776), zuletzt geändert durch Art. 4 Abs. 8 des Gesetzes vom 30. Juli 2009 (BGBl. I S. 2437)
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
LeistungsTV-Bund	Tarifvertrag über das Leistungsentgelt für die Beschäftigten des Bundes: Durch den Tarifvertrag über das Leistungsentgelt für die Beschäftigten des Bundes vom 25. August 2006 wird zum 1. Januar 2007 eine Entgeltkomponente für die Tarifbeschäftigten eingeführt, die sich ausschließlich an der individuellen Leistung der/des Beschäftigten orientiert. Die Detailausgestaltung erfolgt durch Dienstvereinbarungen, die den Besonderheiten der einzelnen Bundesbehörden Rechnung tragen.
LuftSiG	Luftsicherheitsgesetz vom 11. Januar 2005 (BGBl. I S. 78), zuletzt geändert durch Art. 7 des Gesetzes vom 29. Juli 2009 (BGBl. I S. 2424)
LuftSiZÜV	Luftsicherheits-Zuverlässigkeitsüberprüfungsverordnung vom 23. Mai 2007 (BGBl. I S. 947), zuletzt geändert durch Art. 3 der Verordnung vom 2. April 2008 (BGBl. I S. 647)
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 29. Juli 2009 (BGBl. I S. 2353)
RGebStV	Rundfunkgebührenstaatsvertrag vom 31. August 1991 (GVBl. S. 426), zuletzt geändert durch Art. 6 des StV vom 18. Dezember 2008 (GVBl. 2009 S. 131, 138)
SAKDG	Gesetz über die Errichtung der Sächsischen Anstalt für kommunale Datenverarbeitung vom 15. Juli 1994 (GVBl. S. 1432), zuletzt geändert durch Art. 5 des Gesetzes vom 7. November 2007 (GVBl. S. 478, 484)
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)

SächsBestG	Sächsisches Gesetz über das Friedhofs-, Leichen- und Bestattungswesen (Sächsisches Bestattungsgesetz) vom 8. Juli 1994 (GVBl. S. 1321), zuletzt geändert durch Gesetz vom 19. Juni 2009 (GVBl. S. 382)
SächsBG	Beamtengesetz für den Freistaat Sachsen in der Fassung der Bekanntmachung vom 14. Juni 1999 (GVBl. S. 370), zuletzt geändert durch Art. 1 des Gesetzes vom 12. März 2009 (GVBl. S. 102)
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), Neufassung vom 14. Dezember 2006 (GVBl. S. 530), zuletzt geändert durch Art. 6 vom 8. Dezember 2008 (GVBl. S. 940, 941)
SächsEAG	Gesetz über den einheitlichen Ansprechpartner im Freistaat Sachsen vom 13. August 2009 (GVBl. S. 446)
SächsFrTrSchulG	Gesetz über Schulen in freier Trägerschaft vom 4. Februar 1992 (GVBl. S. 37), zuletzt geändert durch Art. 19 vom 12. Dezember 2008 (GVBl. S. 866, 885)
SächsGemO	Gemeindeordnung für den Freistaat Sachsen vom 21. April 1993 (GVBl. S. 301), zuletzt geändert durch Art. 2 des Gesetzes vom 26. Juli 2009 (GVBl. S. 323)
SächsHG a. F.	Sächsisches Hochschulgesetz vom 11. Juni 1999 (GVBl. S. 294), geändert durch Art. 13 des Gesetzes vom 15. Dezember 2006 (GVBl. S. 515, 521)
SächsHSG n. F.	Gesetz über die Hochschulen im Freistaat Sachsen - Sächsisches Hochschulgesetz vom 10. Dezember 2008 (GVBl. S. 900), zuletzt geändert durch Art. 10 des Gesetzes vom 26. Juni 2009 (GVBl. S. 375, 377)
SächsJOrgVO	Verordnung des SMJus über die Organisation der Justiz (Sächsische Justizorganisationsverordnung vom 14. Dezember 2007 (GVBl. S. 600), zuletzt geändert durch Art. 4 der Verordnung vom 6. Juni 2008 (GVBl. S. 336)
SächsKiSchG	Sächsisches Kindergesundheits- und Kinderschutzgesetz vom 19. Juni 2009 (GVBl. S. 379)

SächsLJHG	Sächsisches Landesjugendhilfegesetz vom 4. März 1992 (GVBl. S. 61), zuletzt geändert durch Art. 11 des Gesetzes vom 13. August 2009 (GVBl. S. 438)
SächsKHG	Gesetz zur Neuordnung des Krankenhauswesens - Sächsisches Krankenhausgesetz vom 19. August 1993 (GVBl. S. 675), zuletzt geändert durch Art. 49 des Gesetzes vom 29. Januar 2008 (GVBl. S. 138, 177)
SächsLKrO	Landkreisordnung für den Freistaat Sachsen vom 19. Juli 1993 (GVBl. S. 577), zuletzt geändert durch Art. 3 des Gesetzes vom 26. Juli 2009 (GVBl. S. 323, 325)
SächsMeldVO	Verordnung des SMI zur Durchführung des Sächsischen Meldegesetzes (Sächsische Meldeverordnung) vom 13. Dezember 2006 (GVBl. S. 540), zuletzt geändert durch Art. 3 des Gesetzes vom 19. Juni 2009 (GVBl. S. 379, 381)
SächsMG	Sächsisches Meldegesetz vom 21. April 1993 (GVBl. S. 353), zuletzt geändert durch Art. 2 des Gesetzes vom 11. Dezember 2008 (GVBl. S. 938, 939)
SächsNTVO	Verordnung der Sächsischen Staatsregierung über die Nebentätigkeit der Beamten und Richter im Freistaat Sachsen (Sächsische Nebentätigkeitsverordnung) vom 21. Juni 1994 (GVBl. S. 1110), zuletzt geändert durch Art. 1 vom 28. Januar 2004 (GVBl. S. 33)
SächsPersVG	Sächsisches Personalvertretungsgesetz vom 21. Januar 1993 (GVBl. S. 29), zuletzt geändert durch Art. 13 des Gesetzes vom 29. Januar 2008 (GVBl. S. 138, 144)
SächsPetAG	Gesetz über den Petitionsausschuss des Sächsischen Landtags (Sächsisches Petitionsausschussgesetz) vom 11. Juni 1991 (GVBl. S. 90), zuletzt geändert durch Art. 1 des Gesetzes vom 5. Mai 2008 (GVBl. S. 302)
SächsPolG	Polizeigesetz des Freistaates Sachsen, Bekanntmachung vom 13. August 1999 (GVBl. S. 466), zuletzt geändert durch Art. 4 des Gesetzes vom 8. Dezember 2008 (GVBl. S. 940, 941)
SächsPsychKG	Sächsisches Gesetz über die Hilfen und die Unterbringung bei psychischen Krankheiten vom 16. Juni 1994 (GVBl. S. 1097), zuletzt geändert durch Art. 5 des Gesetzes vom 8. Dezember 2008 (GVBl. S. 940, 941)

SächsPVPG	Gesetz über die Verarbeitung personenbezogener Daten in der Personalvermittlungsplattform (Sächsisches Personalvermittlungsplattformgesetz) vom 12. Dezember 2008 (GVBl. S. 866)
SächsQualiVO	Verordnung des SMS über die Anforderungen an die Qualifikation und Fortbildung der pädagogischen Fachkräfte in Kindertageseinrichtungen und der Tagespflegepersonen (Sächsische Qualifikations- und Fortbildungsverordnung pädagogischer Fachkräfte) vom 9. Januar 2004 (GVBl. S. 11)
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)
SächsSÜG	Gesetz über die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen im Freistaat Sachsen (Sächsisches Sicherheitsüberprüfungsgesetz) vom 19. Februar 2004 (GVBl. S. 44), zuletzt geändert durch Art. 18 des Gesetzes vom 29. Januar 2008 (GVBl. S. 138, 159)
SächsVerf	Verfassung des Freistaates Sachsen vom 27. Mai 1992 (GVBl. S. 243)
SächsVwVG	Verwaltungsvollstreckungsgesetz vom 17. Juli 1992 (GVBl. S. 327), zuletzt geändert durch Art. 25 des Gesetzes vom 29. Januar 2008 (GVBl. S. 138, 160)
SächsVwVfG	Vorläufiges Verwaltungsverfahrensgesetz für den Freistaat Sachsen vom 21. Januar 1993 (GVBl. S. 74), zuletzt geändert durch Art. 1 des Gesetzes vom 8. Dezember 2008 (GVBl. S. 940)
SGB I	Erstes Buch Sozialgesetzbuch - Allgemeiner Teil - (Art. 1 des Gesetzes vom 11. Dezember 1975, BGBl I S. 3015), zuletzt geändert durch Art. 7 Abs. 5 des Gesetzes vom 7. Juli 2009 (BGBl. I S. 1707)
SGB II	Zweites Buch Sozialgesetzbuch - Grundsicherung für Arbeitsuchende - (Art. 1 des Gesetzes vom 24. Dezember 2003, BGBl. I S. 2954), zuletzt geändert durch Art. 14b des Gesetzes vom 17. Juli 2009 (BGBl. I S. 1990)
SGB III	Drittes Buch Sozialgesetzbuch - Arbeitsförderung - (Art. 1 des Gesetzes vom 24. März 1997, BGBl. I S. 594), zuletzt geändert durch Art. 4 des Gesetzes vom 16. Juli 2009 (BGBl. I S. 1959)
SGB V	Fünftes Buch Sozialgesetzbuch - Gesetzliche Krankenversicherung (Art. 1 des Gesetzes vom 20. Dezember 1988, BGBl. I S. 2477),

	zuletzt geändert durch Art. 1 des Gesetzes vom 30. Juli 2009 (BGBl. I S. 2495)
SDB VII	Siebtes Buch Sozialgesetzbuch - Gesetzliche Unfallversicherung - (Art. 1 des Gesetzes vom 7. August 1996, BGBl. I S. 1254), zuletzt geändert durch Art. 2 des Gesetzes vom 17. Juli 2009 (BGBl. I S. 1974)
SGB VIII	Achtes Buch Sozialgesetzbuch - Kinder und Jugendhilfe - (Art. 1 des Gesetzes vom 26. Juni 1990, BGBl. I S. 1163), zuletzt geändert durch Art. 12 des Gesetzes vom 6. Juli 2009 (BGBl. I S. 1696)
SGB X	Zehntes Buch Sozialgesetzbuch - Sozialverwaltungsverfahren und Sozialdatenschutz - (Art. 1 des Gesetzes vom 18. August 1980, BGBl. I S. 1469 und Art. 1 des Gesetzes vom 4. November 1982, BGBl. I S. 1450), zuletzt geändert durch Art. 4 Abs. 15 des Gesetzes vom 29. Juli 2009 (BGBl. I S. 2258)
SGB XII	Zwölftes Buch Sozialgesetzbuch - Sozialhilfe - (Art. 1 des Gesetzes vom 27. Dezember 2003, BGBl. I S. 3022), zuletzt geändert durch Art. 4 des Gesetzes vom 30. Juli 2009 (BGBl. I S. 2495)
StGB	Strafgesetzbuch in der Fassung der Bekanntmachung vom 13. November 1998 (BGBl. I S. 3322), zuletzt geändert durch Art. 3 des Gesetzes vom 2. Oktober 2009 (BGBl. I S. 3214)
StPO	Strafprozessordnung in der Fassung der Bekanntmachung vom 7. April 1987 (BGBl. I S. 1074, 1319), zuletzt geändert durch Art. 3 des Gesetzes vom 30. Juli 2009 (BGBl. I S. 2437)
StUG	Stasi-Unterlagen-Gesetz in der Fassung der Bekanntmachung vom 18. Februar 2007 (BGBl. I S. 162), zuletzt geändert durch Art. 15 Abs. 64 des Gesetzes vom 5. Februar 2009 (BGBl. I S. 160)
StVG	Straßenverkehrsgesetz in der Fassung der Bekanntmachung vom 5. März 2003 (BGBl. I S. 310, 919), zuletzt geändert durch Art. 3 des Gesetzes vom 31. Juli 2009 (BGBl. I S. 2507)
StVollzG	Strafvollzugsgesetz vom 16. März 1976 (BGBl. I S. 581, 2088), zuletzt geändert durch Art. 2 des Gesetzes vom 29. Juli 2009 (BGBl. I S. 2274)
StVollStrO	Verwaltungsvorschrift des SMJus über die Strafvollstreckungsordnung vom 20. März 2001 (SächsABl. S. 446), zuletzt geändert am 10. Dezember 2007 (SächsABl.SDr. S. 516)

TKG	Telekommunikationsgesetz vom 22. Juni 2004 (BGBl. I S. 1190), zuletzt geändert durch Art. 2 des Gesetzes vom 14. August 2009 (BGBl. I S. 2821)
TMG	Telemediengesetz vom 26. Februar 2007 (BGBl. I S. 179): ersetzt das TDDSG ab 1. März 2007; zuletzt geändert durch Art. 2 des Gesetzes vom 14. August 2009 (BGBl. I S. 2814)
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)
TVöD	Tarifvertrag für den öffentlichen Dienst vom 13. September 2005 (nicht amtlich veröffentlicht),
VwVfG	Verwaltungsverfahrensgesetz in der Fassung der Bekanntmachung vom 23. Januar 2003 (BGBl. I S. 102), zuletzt geändert durch Art. 2 Abs. 1 des Gesetzes vom 14. August 2009 (BGBl. I S. 2827)
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 des Gesetzes vom 24. September 2009 (BGBl. I S. 3145)

Sonstiges

a. a. O.	am angegebenen Ort
a. F.	alte Fassung
ARGE	Arbeitsgemeinschaft nach SGB II
ASGFFJ	Ausschuss für Soziales, Gesundheit, Familie, Frauen und Jugend des Sächsischen Landtages
BA	Bundesagentur für Arbeit
BfDI	Bundesbeauftragter für den Datenschutz und Informationsfreiheit
BMAS	Bundesministerium für Arbeit und Soziales
BMG	Bundesministerium für Gesundheit
BMI	Bundesministerium des Innern
BMJ	Bundesministerium der Justiz

BMWi	Bundesministerium für Wirtschaft und Technologie
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
DSK	Datenschutzkonferenz (halbjährlich stattfindende Konferenz der Datenschutzbeauftragten des Bundes und der Länder)
DuD	Datenschutz und Datensicherheit
DVBl.	Deutsches Verwaltungsblatt
EDPS	European Data Protection Supervisor, Europäischer Datenschutzbeauftragter
EG	Europäische Gemeinschaft
eGK	Elektronische Gesundheitskarte
EPA	Elektronische Patientenakte
EU	Europäische Union
e. V.	Eingetragener Verein
FAZ	Frankfurter Allgemeine Zeitung

GEZ	Gebühreneinzugszentrale der öffentlich-rechtlichen Rundfunkanstalten
GVBl.	Sächsisches Gesetz- und Verordnungsblatt
ICD	Die Internationale statistische Klassifikation der Krankheiten und verwandter Gesundheitsprobleme (ICD, engl.: International Statistical Classification of Diseases and Related Health Problems) ist das wichtigste, weltweit anerkannte Diagnoseklassifikationssystem der Medizin. Es wird von der Weltgesundheitsorganisation (WHO) herausgegeben.
IMI	Internal Market Information System; Datenbank, die auf einen Server der EU-Kommission in Luxemburg gespeichert ist
INPOL	Polizeiliches Informationssystem des Bundes u. der Länder
JVA	Justizvollzugsanstalt
KKM	Kommunales Kernmelderegister
KMK	Kultusministerkonferenz
KV	Kassenärztliche Vereinigung
LD	Landesdirektion (bis 31. Juli 2008 Regierungspräsidium)
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
LPK	Lehr- und Praxiskommentar
LRA	Landratsamt
LSG	Landessozialgericht
LT-DS	Landtags-Drucksache
MDK	Medizinischer Dienst der Krankenversicherung

MDR	Mitteldeutscher Rundfunk
MfS	Ministerium für Staatssicherheit der ehemaligen DDR
MMR	Multimedia und Recht
NADIS	Nachrichtendienstliches Informationssystem
NJW	Neue Juristische Wochenschrift
NStZ	Neue Zeitschrift für Strafrecht
NVwZ	Neue Zeitschrift für Verwaltungsrecht
NZS	Neue Zeitschrift für Sozialrecht
OFD	Oberfinanzdirektion
OLG	Oberlandesgericht
OVG	Sächsisches Oberverwaltungsgericht
PASS	Polizeiliches Auskunftssystem Sachsen
RP	Regierungspräsidium (ab 1. August 2008 in Landesdirektion umbenannt)
SAB	Sächsische Aufbaubank
SächsABl.	Sächsisches Amtsblatt
SächsVerfGH	Verfassungsgerichtshof des Freistaates Sachsen
SAKD	Sächsische Anstalt für Kommunale Datenverarbeitung
SG	Sozialgericht
SK	Sächsische Staatskanzlei
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
SMWA	Sächsisches Staatsministerium für Wirtschaft und Arbeit
SMWK	Sächsisches Staatsministerium für Wissenschaft und Kunst
SRH	Sächsischer Rechnungshof
SSG	Sächsischer Städte- und Gemeindetag
StaLa	Statistisches Landesamt des Freistaates Sachsen
ThLfD	Thüringer Landesbeauftragter für den Datenschutz
VG	Verwaltungsgericht
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 Datenschutz im Informationszeitalter

Datenschützer haben in der Vergangenheit oft geklagt, dass ihrem Anliegen zu wenig Aufmerksamkeit zuteil werden würde. Dies hat sich im Berichtszeitraum geändert. Mehrere Skandale bei deutschen Großunternehmen, über die ausgiebig berichtet wurde, haben dazu geführt, dass die Gefahren für die Privatsphäre deutlich ins Blickfeld einer breiten Öffentlichkeit gerückt sind. Doch nicht nur die Medien haben sich stärker dem Datenschutz gewidmet. Das Bundesverfassungsgericht hat wohl bisher noch nie so viel datenschutzrechtlich relevante Entscheidungen wie im Berichtszeitraum gefasst. Höhepunkt war die Definition eines eigenständigen Grundrechts „auf Gewährleistung der Vertraulichkeit und der Integrität informationstechnischer Systeme“ - erstmals seit dem Volkszählungsurteil 1983 mit dem „Recht auf informationelle Selbstbestimmung“. Die Reaktion der Politik ließ nicht auf sich warten. Nachdem lange Zeit auf Bundesebene immer nur Ankündigungen zu einer Reform des Datenschutzrechts zu finden waren, gab es jetzt erste Schritte in dieser Richtung. Unter Datenschützern ist unbestritten, dass dies nur ein Anfang sein kann.

All dies ist Reflex einer Entwicklung, die sich in den letzten Jahren abspielte. Wir sind in der vielbeschworenen Informationsgesellschaft angekommen.

Technische Mittel sind erschwinglich geworden. In unserer Alltagswelt haben E-Mail, Handy, Home-PC, MP3-Player, Web-Kameras, Internet, Social Communities, E-Banking, Online-Shopping mittlerweile ihren festen Platz. Schon an den Begriffen wird die Globalisierung deutlich. Aber nicht nur räumlich, sondern auch zeitlich sind sie allgegenwärtig. Es gibt keine Stelle in unserer Lebenswirklichkeit, wo die Informationsgesellschaft uns nicht berühren würde. Auch das neue Grundrecht ist ein Reflex dieser Entwicklung, der den neuesten Trend aufgreift, die Entstehung sogenannter „smarter Umgebungen“, in denen Geräte ohne unser Wissen miteinander kommunizieren und dabei Daten austauschen und speichern, die in der Endkonsequenz ein umfassendes Profil unserer Persönlichkeit ermöglichen.

Sich dieser Entwicklung zu versagen, ist unmöglich. Ob gewollt, genötigt oder gezwungen, elektronische Informationsverarbeitung gehört zu unserer Lebenswirklichkeit. Hier einen ausgewogenen Umgang zu finden zwischen staatlichen und unternehmerischen Bedürfnissen und Begehrlichkeiten einerseits und den zu schützenden Grundrechten der Einzelnen auf der anderen Seite. Dies ist eine Aufgabe für alle Beteiligten, Unternehmer, Politiker, Behörden, Bürger, Kunden, Aufsichtsstellen, Medien, Interessenverbände. Datenschutz ist kein Spartenthema mehr, sondern zentrales gesellschaftliches Anliegen in der Informationsgesellschaft. Auch in Sachsen muss dem

Datenschutz über das bereits bestehende Maß hinaus Aufmerksamkeit geschenkt werden. Zwar spielen sich entscheidende datenschutzrechtliche Entwicklungen auf europäischer und deutscher gesamtstaatlicher Ebene ab. Aber Landespolitiker und -behörden sind nicht aus dem Spiel. Durchaus können neue Ansätze zum Datenschutz auch auf Landesebene aufgenommen und verstärkt werden. Am Anfang des Datenschutzes in Deutschland stand 1970 mit einem ersten Datenschutzgesetz ein einzelnes Bundesland, Hessen. Jetzt ist der deutsche Datenschutz ein international wirksamer Exportschlager. Wir in Sachsen sollten da in unserem Bemühen nicht zurückstehen.

1.2 Nichtzulassung zum Zweiten Juristischen Staatsexamen

Im Berichtszeitraum hat das in 12/1.8 angesprochene Beanstandungsverfahren seinen Abschluss gefunden, dessen zugrunde liegender Sachverhalt mittlerweile auch Gegenstand medialer Aufmerksamkeit sowie mehrerer Kleiner Anfragen geworden ist. Die Sächsische Justizverwaltung hat sich über einen langen Zeitraum hinweg bemüht, zum Teil im Zusammenwirken mit den Justizprüfungsämtern anderer Bundesländer sowie mit der Verwaltung einer Universität, dem Petenten die Zulassung zur Zweiten Juristischen Staatsprüfung zu verwehren. Der Petent hatte nach zwei vergeblichen Versuchen, in den alten Bundesländern die Erste Juristische Staatsprüfung abzulegen, 1993 an einer ostdeutschen Universität ein Jurastudium erfolgreich als Diplomjurist abgeschlossen und war in den juristischen Vorbereitungsdienst des Freistaates Sachsen aufgenommen worden. Die Entlassung des Petenten aus dem juristischen Vorbereitungsdienst sowie aus dem Beamtenverhältnis auf Widerruf erfolgte erstmals 1995, wurde kurz darauf aus formalen Gründen zurückgenommen und wurde endgültig 1996 kurz vor dem Abschluss des Zweiten Juristischen Staatsexamens ausgesprochen. Die darauf folgenden juristischen Auseinandersetzungen dauern bis heute an.

Ich habe das SMJus - wegen des dort angesiedelten Landesjustizprüfungsamtes - in drei Fällen und das OLG Dresden als für die Referendarsausbildung zuständige Behörde in ebenfalls drei Fällen beanstandet.

Das Landesjustizprüfungsamt hatte, nachdem es von anderer Seite auf den Petenten aufmerksam gemacht wurde, ohne entsprechende Rechtsgrundlage Informationen über ihn übermittelt bzw. erhalten. Das OLG hatte Schriftstücke aus der Personalakte des Petenten ausgesondert, um diesem eine Kenntnisnahme bei einer Akteneinsicht zumindest zu erschweren. Außerdem hatten beide Behörden in den rechtlichen Auseinandersetzungen einen Sachverhalt unzutreffend dargestellt.

SMJus und OLG haben die Beanstandungen weitgehend zurückgewiesen; allerdings hat sich das OLG bereit erklärt, die Personalakte des Petenten zu berichtigen. Dies ist er-

folgt. Damit ist das Beanstandungsverfahren - sofern keine neuen Tatsachen festgestellt werden können - beendet. Leider konnte die noch im 12. Tätigkeitsbericht erhoffte einvernehmliche Lösung des eigentlichen Problems nicht erzielt werden. Mit einem verständnisvollen und abwägenden Handeln der beteiligten Behörden zu einem frühen Zeitpunkt - natürlich innerhalb eines vorhandenen Rechtsrahmens - hätte allen Beteiligten viel Beschwernis erspart werden können.

1.3 Neuer Internetauftritt

Im September 2008 ging mein neuer Internetauftritt unter www.datenschutz.sachsen.de online. Die Internetadresse ist gleich geblieben, Inhalt und Gestaltung aber sind zum großen Teil unter Nutzung eines Open-Source-CMS (Joomla) erneuert und verbessert worden. Viel Aufwand wurde zudem betrieben, um den Internetauftritt für jeden besser zugänglich zu machen und behindertenfreundlich zu gestalten. Dies umfasst auch die Möglichkeit, sich die Texte vorlesen zu lassen.

Nachdem ich seit 2007 sowohl Kontrollbehörde für die öffentlichen Stellen als auch Aufsichtsbehörde für die nicht-öffentlichen Stellen in Sachsen bin, wurde das Informationsangebot in einen „öffentlichen“ und „nicht-öffentlichen Bereich“ übersichtlich eingeteilt. Neben eingängigen Informationen und Kontaktmöglichkeiten über die Behörde enthält die neu gestaltete Webseite eine neue Rubrik „Datenschutz für den Bürger“ und einen erweiterten Bereich mit Informationen, Tätigkeitsberichten, Formularen und Arbeitshilfen, die von Bürgern und öffentlichen sowie nicht-öffentlichen Stellen genutzt werden können.

Neu hinzugekommen ist ebenfalls ein „aktuelles Thema“. Hier wird regelmäßig ein aktuelles Schwerpunktthema ausgewählt und dargestellt. Ich beabsichtige, künftig auch die Möglichkeit anzubieten, einen RSS-feed zu abonnieren.

Hinweisen möchte ich noch darauf, dass selbstverständlich nicht die Daten der Besucher der Internetseite mittels personenbeziehbarer IP-Adressen bei Nutzerzugriffen gespeichert werden (vgl. dazu 13/14.1).

1.4 Vorabkontrollen und Verfahrensverzeichnisse von KISA-Kunden

Kurz nach Ende des Berichtszeitraums erhielt ich auf Nachfrage von der Kommunalen Informationsverarbeitung Sachsen - KdöR (KISA) die Verfahrensverzeichnisse für die automatisierten Verarbeitungen personenbezogener Daten, die sie im Auftrag sächsischer Kommunen unter jeweils identischen datenschutzrechtlichen und -technischen

Konditionen durchführt. Diese Übersendung gehört gemäß § 10 Abs. 2 SächsDSG zwar zu den Pflichten der jeweiligen Kommunen, welche diese Aufgabe jedoch auf die KISA übertragen haben (Nachdem die Verfahrensverzeichnisse keine personenbezogenen Daten enthalten, war bei der Beauftragung § 7 SächsDSG nicht zu beachten.). Eine entsprechende Übersendung von Verfahrensverzeichnissen durch die KISA wird nach einer Vereinbarung mit mir auch künftig stattfinden. Hinzu kommt die Durchführung von Vorabkontrollen gemäß § 10 Abs. 4 SächsDSG. Zwar werden diese letztendlich gemäß § 10 Abs. 4 SächsDSG durch mich durchgeführt, ich kann hierfür jedoch das Ergebnis der übersandten Unterlagen verwenden.

Sollten die Kommunen gemäß § 11 SächsDSG einen behördlichen Datenschutzbeauftragten bestellt haben, so ist dieser für die Führung der Verfahrensverzeichnisse und die Vorabkontrollen zuständig. Eine Übersendung der Verfahrensverzeichnisse und der Unterlagen zur Vorabkontrolle durch die KISA hat daher nicht nur an mich, sondern auch an diese zu erfolgen.

Durch diesen auf meine Anregung hin vorgenommenen Bürokratieabbau werden sowohl die Kommunen als auch ich entlastet.

1.5 Öffentliche Stellen nach dem Sächsischen Datenschutzgesetz: Beliehene

Zum Teil erreichen mich Anfragen zur Datenverarbeitung von Stellen, bei denen zunächst nicht klar ist, ob personenbezogene Daten nach dem Sächsischen Datenschutzgesetz oder nach dem Bundesdatenschutzgesetz verarbeitet werden, vgl. auch 13/1.3 und 12/1.7.

Nicht-öffentliche Stellen verarbeiten keine Daten nach dem Sächsischen Datenschutzgesetz, es sei denn sie werden von öffentlichen Stellen im Sinne von § 2 Abs. 1 SächsDSG beherrscht und sind keine Wettbewerbsunternehmen (vgl. § 2 Abs. 2 und Abs. 3 SächsDSG) oder sie nehmen „hoheitliche Aufgaben der öffentlichen Verwaltung wahr“ (§ 2 Abs. 1 Satz 2 SächsDSG). Dann sind sie sog. *Beliehene* und sind dann „insoweit öffentliche Stellen im Sinne dieses Gesetzes“, vgl. § 2 Abs. 1 Satz 2 SächsDSG. Sie sind dann auch Behörden. Zu den Stellen, die (als eigentlich Private) hoheitliche Aufgaben wahrnehmen, zählen z. B. der TÜV oder Schornsteinfeger. Soweit sie hoheitlich handeln, richtet sich die Datenverarbeitung nach dem Sächsischen Datenschutzgesetz.

Nicht selten ergibt sich aber auch die Fragestellung in Bezug auf die Datenverarbeitung an privaten Schulen. Das Sächsische Gesetz über Schulen in freier Trägerschaft unter-

scheidet zwischen der genehmigten Ersatzschule (§ 4 SächsFrTrSchulG) und der anerkannten Ersatzschule (§ 8 SächsFrTrSchulG). Die genehmigte Ersatzschule hat lediglich das Recht, Kinder und Jugendliche zur Erfüllung ihrer Schulpflicht aufzunehmen (§ 4 Abs. 3 SächsFrTrSchulG). Bietet die Ersatzschule Gewähr, dass sie dauernd die an entsprechende öffentliche Schulen beziehungsweise Schulen im Sinne des § 3 Abs. 2 SächsFrTrSchulG gestellten Anforderungen erfüllt, wird ihr die Eigenschaft einer staatlich anerkannten Ersatzschule verliehen (§ 8 Abs. 1 SächsFrTrSchulG). Mit der Anerkennung erhält die Ersatzschule dann das Recht, nach den für öffentliche Schulen bzw. Schulen im Sinne des § 3 Abs. 2 SächsFrTrSchulG geltenden Vorschriften Prüfungen abzuhalten und Zeugnisse zu erteilen (§ 8 Abs. 2 SächsFrTrSchulG). Die anerkannte Ersatzschule nimmt also hoheitliche Aufgaben wahr. Sie ist dann Beliehene im Sinne von § 2 Abs. 1 Satz 2 SächsDSG und die Datenverarbeitung richtet sich *soweit* (in Bezug auf die hoheitliche Aufgabenerfüllung) nach dem Sächsischen Datenschutzgesetz. „Soweit“ bedeutet dann, dass sich z. B. die Datenverarbeitung zu den Zeugnissen der Schüler nach dem Sächsischen Datenschutzgesetz, die Beschäftigtendatenverarbeitung der anerkannten Ersatzschule nach dem Bundesdatenschutzgesetz richtet. Bei nur *genehmigten* Ersatzschulen regelt sich die Datenverarbeitung ausschließlich nach dem Bundesdatenschutzgesetz.

1.6 Beendigung des Amtes als Datenschutzbeauftragter bei Fusion

Bei der Fusion zweier juristisch selbständiger Krankenkassen trat die Frage auf, was mit den Ämtern der Datenschutzbeauftragten der beiden Krankenkassen geschieht.

§ 144 Abs. 4 Satz 1 i. V. m. Abs. 3 SGB V legt fest, dass mit Bestimmung des Zeitpunktes durch die Aufsichtsbehörde, an dem die Vereinigung von Ortskrankenkassen wirksam wird, die bisherigen Krankenkassen geschlossen sind. Die neue Krankenkasse tritt im Wege der Gesamtrechtsnachfolge in die Rechte und Pflichten der bisherigen Krankenkassen ein. Die bisherigen Krankenkassen verlieren ihre Rechtsfähigkeit. Mit der Schließung enden die Ämter der Datenschutzbeauftragten. Die Datenschutzbeauftragten sind einer verantwortlichen Stelle zugeordnet (§ 4f Abs. 1 BDSG). Hört diese Stelle auf zu existieren, wird die Aufgabe gegenstandslos. Eine Regelung für ein Übergangs- oder Restmandat gibt es nicht.

Eines Widerrufs der Bestellung der Datenschutzbeauftragten (§ 4f BDSG i. V. m. §§ 1, 81 Abs. 4 SGB X und § 35 SGB I) bedarf es nicht, da durch den Verlust der Rechtsfähigkeit der bisherigen Krankenkassen die Ämter automatisch enden.

Eine Verpflichtung, aus den bisherigen Datenschutzbeauftragten bei einer Neubestellung auszuwählen, ergibt sich weder aus § 4f Abs. 1 Satz 5 BDSG noch aus § 4f

Abs. 3 Satz 3 und 4 BDSG. Die erste Regelung ermöglicht lediglich bei Vorliegen einer besonderen Behördenstruktur eine Zusammenlegung der Aufgaben mehrerer Datenschutzbeauftragten auf einen Datenschutzbeauftragten. Die zweite Regelung soll eine Benachteiligung des Datenschutzbeauftragten wegen der Erfüllung seiner Aufgaben verhindern. Ein Widerruf kann nur in entsprechender Anwendung von § 626 BGB erfolgen. Eine Benachteiligung bei Beendigung des Amtes aufgrund Wegfalls der Aufgaben liegt nicht vor. Ein Widerruf ist nicht erforderlich, so dass auch nicht zu prüfen ist, ob ein Grund nach § 626 BGB überhaupt vorliegt.

Vergleichbare Fälle sind vorstellbar bei der Fusion von Krankenhäusern, die über Datenschutzbeauftragte - nach einer Altfassung des Bundesdatenschutzgesetzes - verfügen, vgl. § 33 Abs. 8 Satz 4 SächsKHG.

Entsprechend verhält es sich bei nach dem Sächsischen Datenschutzgesetz bestellten Datenschutzbeauftragten, so z. B. bei der erfolgten Zusammenlegung von Landkreisverwaltungen. Mit der Bildung der neuen Rechtspersonen sind die alten Gebietskörperschaften erloschen. Die alte Landkreisverwaltung besteht so nicht mehr. Es gibt eine Gesamtrechtsnachfolge. Konkrete Beauftragten-Ämter bestehen aber nicht weiter, sondern erlöschen. Bei den zusammengelegten Verwaltungseinheiten sehe ich erst recht eine Notwendigkeit begründet, Datenschutzbeauftragte zu bestellen. Ich empfehle auch, die Möglichkeiten, die das Gesetz bietet, zu nutzen und einen Stellvertreter der Datenschutzbeauftragten nach § 11 Abs. 1 Satz 1 SächsDSG zu bestellen.

2 Parlament

2.1 Kleine Anfrage zu Betroffenen von Ordnungswidrigkeitenverfahren

Die Staatsregierung fragte, ob sie im Rahmen der Beantwortung parlamentarischer Kleiner Anfragen wie erwünscht Auskunft über eventuell festgestellte Ordnungswidrigkeiten von Betreibern bestimmter Anlagen, über staatsanwaltschaftliche Ermittlungen gegen diese sowie über die Höhe eventuell verhängter Bußgelder erteilen dürfe. Ich habe die Frage - im Anschluss an 4/2, 8/9.4.1 und 13/2.1 - wie folgt beantwortet:

Dem parlamentarischen Fragerecht von Abgeordneten des Sächsischen Landtages nach Art. 51 Abs. 1 SächsVerf können die Datenschutzrechte der Betroffenen als „Rechte Dritter“ nach Art. 51 Abs. 2 SächsVerf entgegenstehen. Der Abgeordnete soll mittels seines parlamentarischen Fragerechts kontrollieren können, ob und ggf. wie (recht- und zweckmäßig) die Exekutive handelt. Dieses Fragerecht stößt nach Art. 51 Abs. 2 SächsVerf an seine Grenzen, soweit das in Art. 33 SächsVerf garantierte Recht auf informationelle Selbstbestimmung des Dritten einer Beantwortung entgegensteht. Art. 51

SächsVerf stellt dem Parlament mithin kein Instrument zur (tieferen) Ausforschung Dritter außerhalb der öffentlichen Verwaltung, hier von Anlagenbetreibern, zur Verfügung.

Parlamentarisches Interpellationsrecht und das Recht auf informationelle Selbstbestimmung der jeweiligen Betroffenen müssen im Einzelfall im Wege der *Herstellung praktischer Konkordanz* einander so zugeordnet werden, dass beide Verfassungsrechtsgüter sich so weit wie möglich entfalten können. Dazu bietet sich zunächst der Versuch an, den Personenbezug (vgl. § 3 Abs. 1 SächsDSG) durch Zusammenführung (Aggregation) der Angaben aus eventuell mehreren Ordnungswidrigkeitenverfahren in einer bestimmten Region, etwa einem Landkreis, aufzuheben. Möglich erscheint dies allerdings nur, wenn es um jeweils mehr als drei Verfahren oder Bußgelder geht. Ist dies unmöglich, sollten Angaben zumindest pseudonymisiert, also konkrete Namen und andere identifizierende Merkmale durch Pseudonyme (z. B. „Jahr 2007: Landkreis AB, Betrieb XY, 2 Bußgeldverfahren, bestandskräftig, Bußgelder i. H. v. zusammen 2.500 €“) ersetzt werden. Diese Art der Beantwortung eröffnet dem Abgeordneten die Möglichkeit zu prüfen, ob und in welchem Umfang die Verwaltung gehandelt und ihre gesetzlichen Aufgaben erfüllt hat; zugleich wahrt sie die Datenschutzrechte der Betroffenen.

3 Europäische Union / Europäische Gemeinschaft

3.1 EU-Dienstleistungsrichtlinie

In Sachsen ist das SMWA federführend für die Umsetzung der EU-Dienstleistungsrichtlinie (*RL 2006/123/EG - ABl. L 376, S. 36 vom 27. Dezember 2006*) zuständig, die die freie grenzüberschreitende Erbringung von Dienstleistungen in einem europäischen Binnenmarkt regelt. Der Abbau von bürokratischen Hindernissen und eine an mutmaßlichen Bedürfnissen von Dienstleistungserbringern orientierte integrierte Verwaltungsorganisation soll mittels einheitlicher (behördlicher) Ansprechpartner und neuer elektronischer Kommunikationsinfrastrukturen online über das Internet sichergestellt werden, Art. 6 und 7, 8 Abs. 1 RL 2006/123/EG. Ausländische Dienstleister, Ärzte, Rechtsanwälte, Handwerker sollen ihre Dienstleistungen in Deutschland anbieten können und über den einheitlichen Ansprechpartner eine Möglichkeit haben, die bürokratischen Prozeduren zu bewältigen. In Sachsen ist dabei vorgesehen, behördliche Wege und Infrastrukturen nicht nur für grenzüberschreitende Vorgänge, sondern auch für die inländischen Abläufe einzurichten.

Das Staatsministerium habe ich weitergehend in den datenschutzrechtlichen Fragen beraten.

Das Richtlinienziel darf nicht zu Lasten datenschutzrechtlicher Grundsätze verfolgt werden. Dementsprechend ist zu fordern, dass eine personenbezogene Datenverarbeitung zweckgebunden zu erfolgen hat. Zu schaffende gesetzliche Vorschriften zur Umsetzung der Richtlinie - unter anderem ein Gesetz zur Einrichtung des einheitlichen Ansprechpartners - haben den Zweck der personenbezogenen Datenverarbeitung genau festzulegen und zu beschränken. Der Grundsatz der informationellen Gewaltenteilung bedingt, dass ein Informationsaustausch zwischen verschiedenen Behörden nicht ohne Weiteres stattfinden darf. Sollen aber schon Datenflüsse gebündelt oder konzentriert werden, wie es die Richtlinie 2006/123/EG vorsieht, so sind gleichwohl dem Trennungsgebot folgend informationelle Datenverbünde weitestgehend zu minimieren oder zu vermeiden. Dies ist auch in Sachsen gesetzlich und mit Verfahrensvorschriften sicherzustellen.

In Sachsen ist vorgesehen, dass eine Stelle, eine Landesdirektion, die Aufgaben des einheitlichen Ansprechpartners wahrnehmen soll. Aufgabe des einheitlichen Ansprechpartners nach der Richtlinie ist es, den zentralen Eingang von Anfragen und Anträgen zu bewältigen. Mit der Einrichtung des *einheitlichen Ansprechpartners* soll gerade nicht in bestehende Zuständigkeiten eingegriffen werden, Art. 6 Abs. 2 RL 2006/123/EG. Letztendlich soll der Vorgang von den zuständigen Behörden bearbeitet werden. Dem einheitlichen Ansprechpartner sollen koordinierende und überwachende Funktionen zukommen. Er soll die bei ihm eingehenden Anträge an die zuständige Stelle weiterleiten. Vor diesem Hintergrund muss aber eine doppelte Datenverarbeitung vermieden oder wenigstens minimiert werden. Die Verarbeitung personenbezogener Daten durch den einheitlichen Ansprechpartner ist auf das zur Aufgabenerfüllung erforderliche Maß zu beschränken. Dauer und Umfang der Datenverarbeitung des einheitlichen Ansprechpartners sind gesetzlich zu beschränken. Auch auf die Betroffenenrechte ist zu achten. Geregelt sein sollte somit auch, dass Anträge auf Löschung, Berichtigung, Auskunft und Akteneinsicht sowie Widerspruch gegen die Datenverarbeitung an den einheitlichen Ansprechpartner gerichtet werden können.

In Bezug auf Datensicherheitsanforderungen und die technische Umsetzung der RL 2006/123/EG gilt nichts anderes als für andere automatisierte Verfahren und Infrastrukturen auch. Ein *Datenschutz- und Datensicherheitskonzept* ist zu erstellen und gesetzlich erforderliche *Vorabkontrollen* sind durchzuführen. Bei vorgesehener elektronischer Kommunikation sind eine sichere Authentifizierung, elektronische Nachweisverfahren (z. B. bei der Einreichung von Belegen und Urkunden) und eine dauerhafte gerichtsfeste Erhaltung von Dokumenten und elektronischen Entscheidungen sicherzustellen. Fragen der gesicherten Übermittlung und Langzeitarchivierung digital signierter Dokumente aus dem EU-Ausland sind noch ungelöst.

Zum Ende des Berichtszeitraums lag mir noch keine Verfahrensbeschreibung zur Umsetzung der EU-Dienstleistungsrichtlinie vor. Zwischenzeitlich liegen mir Teilfachkonzepte zur rechtssicheren Kommunikation und zur Vorgangsbearbeitung und Verwaltung des Schriftguts durch die LD Leipzig als einheitlichem Ansprechpartner vor (vgl. u.).

Im Berichtszeitraum war ein Gesetz zum einheitlichen Ansprechpartner noch in der Beratung und noch nicht verabschiedet worden. Zwischenzeitlich liegt ein Gesetz über den einheitlichen Ansprechpartner im Freistaat Sachsen (SächsEAG), in dem die LD Leipzig als einheitlicher Ansprechpartner festgelegt wird, vor. Konkretisierte Regelungen zum Datenschutz sind in dem Gesetz nicht enthalten. Das Staatsministerium wird ermächtigt, eine Rechtsverordnung zu schaffen, in der die Datenverarbeitung des einheitlichen Ansprechpartners zu regeln ist.

Über das Verfahren und die Verordnung werde ich weiter berichten.

3.2 Binnenmarktinformationssystem IMI

In den Beitrittsländern der EU soll ein elektronisches Kommunikationssystem zwischen den Behörden der Mitgliedstaaten eingerichtet werden, um Informationen im Vollzug der Binnenmarktvorschriften zu übermitteln. Das Verfahren, das sich „IMI“ nennt, soll den Informationsfluss aus unterschiedlichen Verwaltungs- und Arbeitsabläufen und mit verschiedenen Sprachen verbessern helfen. Insbesondere soll auch durch eine verbesserte Behördenzuweisung und die Einrichtung zentraler Kopfstellen das Fehlen fester Ansprechpartner in den Mitgliedstaaten kompensiert werden. In einem ersten Schritt soll IMI Unterstützung für die gegenseitige Amtshilfe gemäß der überarbeiteten Berufsanerkennungsrichtlinie (2005/36/EG) leisten. Ab Dezember 2009 soll das Verfahren dann auch der Unterstützung der Verwaltungszusammenarbeit laut EU-Dienstleistungsrichtlinie (2006/123/EG) dienen. IMI ist ein Verfahren, das als automatisierte Unterstützung für Bereiche des Binnenmarktrechts angelegt worden ist, das aber auch auf andere Rechtsbereiche ausgedehnt werden soll.

Die Einführung von IMI wird auf Bund-Länder-Ebene mit Beteiligung des BMWi gegenüber der EU-Verwaltung koordiniert. In Sachsen ist das für die EU-Dienstleistungsrichtlinie auch zuständige SMWA federführend. Die EU sichert ein hohes Datenschutzniveau zu und dass angemessene technische und organisatorische Maßnahmen getroffen seien, gesteht aber den nationalen Datenschutzbehörden kein Kontrollrecht zu. Hinsichtlich der technisch-organisatorischen Maßnahmen wird den Mitgliedstaaten auch kein Einsichtsrecht in den Sicherheitsplan und die Details zugebilligt**.**

Auf der 75. DSK wurde seitens der Datenschutzbeauftragten in einem Beschluss die fehlende Rechtsgrundlage für die Einführung des EU-weiten Verfahrens kritisiert. In der Folge avisierten EU-Vertreter, dass nach einem positiven internen Beschluss voraussichtlich im Rahmen der Regelungen zur Dienstleistungsrichtlinie auch das Verfahren IMI als verbindliches Verfahren festgelegt werden soll. Dies konnte als Weiterentwicklung der Rechtsgrundlage im Sinne des Briefwechsels zwischen dem Europäischen Datenschutzbeauftragten (EDPS) und EU aus dem Sommer 2008 gewertet werden.

Darüber hinaus veröffentlichte die EU-Kommission gegen Ende meines Berichtszeitraums Datenschutz-Leitlinien (Empfehlung der Kommission von 3/2009 zu Datenschutzleitlinien für das Binnenmarktinformationssystem (IMI)).

Vor diesem Hintergrund habe ich einer Ausweitung des Pilotbetriebs auf weitere Bereiche - bis zur Schaffung einer sicheren Rechtsgrundlage - gegenüber dem Staatsministerium zugestimmt, gleichzeitig aber vereinbart, dass Daten mit hohem Schutzbedarf (z. B. Strafverfahrens- und Gesundheitsdaten) von sächsischen Behörden bis auf Weiteres nicht in das IMI-Verfahren eingepflegt oder von anderen Stellen abgerufen werden sollen.

4 Medien

In diesem Jahr nicht belegt.

5 Inneres

5.1 Personalwesen

5.1.1 Der Schutz von Beschäftigtendaten bei behördlichen Schreiben

Mehrfach ist meine Behörde angefragt worden, ob die Veröffentlichung von behördlichen Schriftsätzen durch die privaten Empfänger - insbesondere im Internet - zulässig sei und ob die Behörde bei der Frage, ob eine nicht-öffentliche Stelle ein Schriftstück der Behörde veröffentlichen könne, ein Mitspracherecht bzw. Fürsorgepflichten habe, da im Briefkopf und im Text personenbezogene Daten von Behördenmitarbeitern verarbeitet werden, u. a. die Unterschrift von Bediensteten, offenbart werden.

Auch die in Briefbögen gemachten Angaben zu Bearbeitern und deren Kontaktdaten, Vor- und Zunamen, E-Mail-Adressen, dienstliche Telefonnummern, Zimmernummern, Funktionsbezeichnungen und Dienstanschriften - die sog. Amtsträgerdaten (Urteil des OVG Koblenz vom 10. September 2007 (Az.: 2 A 10413/07.OVG)) - sind personenbezogene Daten im Sinne von § 3 Abs. 1 SächsDSG. Natürlich ist auch der unterschriebene Namenszug eine personenbezogene Angabe. Spezielle Regelungen zum Schutz von Beschäftigtendaten im öffentlichen Dienst bzw. von Beschäftigten öffentlicher Stellen enthält § 37 SächsDSG. § 37 Abs. 2 SächsDSG regelt aber lediglich die Veröffentlichung der Daten von Beschäftigten durch die öffentliche Stelle selbst. Die Übermittlung der dienstlichen Schreiben an die nicht-öffentlichen Empfänger erfolgt zur Aufgabenerfüllung und ist als Datenverarbeitung nach § 37 Abs. 1 i. V. m. § 16 SächsDSG - als Übermittlung an nicht-öffentliche Stellen - zulässig. Die Briefkopfangaben sind zunächst als Amtsträgerdaten für sich genommen regelmäßig keine schutzwürdigen Angaben, sondern bei der Übermittlung an die Empfänger erforderlich. Die Datenverarbeitung der Empfänger und nicht-öffentlichen Stellen wiederum kann sich, was die Veröffentlichung angeht, in Bezug auf den Inhalt allenfalls nach dem Bundesdatenschutzgesetz richten (vgl. § 27 Abs. 2 BDSG). Bei Rückfragen der Empfänger gegenüber der öffentlichen Stelle, was eine Veröffentlichung oder Weitergabe betrifft, sollte bei der Beantwortung beachtet werden, dass Daten mit Doppelbezug, d. h. Schriftsätze, in denen Angaben über Dritte, also nicht nur Informationen über den Empfänger selbst, auch oder nur vorkommen, in der Regel persönlichkeitsrechtliche Relevanz haben werden. Darüber hinaus ist auch zugunsten der Beschäftigten der öffentlichen Stellen anzuraten, abzusprechen, dass die Veröffentlichung von Unterschriftenzeichen (nachrangiger) Bediensteter unterbleibt. Schwärzungen bei einer Veröffentlichung wären hierbei vorstellbar. Ansonsten gelten zunächst keine Einschränkungen in Bezug auf behördliche Schreiben, es sei denn, es treten persönlichkeitsrechtsbelastende Nebenumstände hinzu, wie z. B. die Verbindung der Angaben in dem behördlichen Schreiben mit anderen belastenden Informationen.

So werden regelmäßig auch urheberrechtliche Regelungen eine Veröffentlichung nicht hindern, sind doch die schriftlichen Mitteilungen von Rechtsauffassungen, Bescheide, Vermerke und andere behördliche Schriftsätze gegenüber den Empfängern nicht vom Urheberrecht erfasst. Ausnahmen kann es aber geben, auch in ganzen Verwaltungsbereichen, so z. B. bei Architekturzeichnungen von Hochbauämtern, Skizzen und Vortragsunterlagen, denen wissenschaftlicher Rang zukommt bzw. Veröffentlichungswerken der Behörden selbst im Internet oder in anderen Medien.

5.1.2 Verwaltungsermittlungen - Teilarchivierung der Akten

Mit meinen Beiträgen 12/5.1.12 und 13/5.1.9 hatte ich auf ein nicht datenschutzgerechtes, Bedienstete belastendes Verfahren bei Verwaltungsermittlungen hingewiesen.

War noch ursprünglich zugesichert worden, dass eine Archivierung solange nicht erfolgt, wie Betroffene noch ihre Berichtigungs-, Auskunfts- und Einsichtsrechte geltend machen und die Akten benötigt werden, sind trotz der Anschreiben Betroffener und weiterer laufender in einem inhaltlichen Zusammenhang stehender Verfahren Akten im Berichtszeitraum 2008 teilweise auf Betreiben einer Abteilung archiviert worden. Betroffene wurden im Nachgang auf Nachfragen hin informiert. Eine andere Abteilung des SMI war hingegen (zutreffend) der Ansicht, dass die Akten noch benötigt werden und eine Archivierung nicht erfolgen könne. Von einer zuständigen Abteilung geführte Teile der Verwaltungsermittlungsakten befinden sich daher noch immer im Staatsministerium, während der andere Teil der Akten dem Hauptstaatsarchiv übergeben wurde. So war nach der Übergabe letzteres mit aufwendig zu bearbeitenden Beschwerden und Anfragen Betroffener belastet. Aus Grundrechtsträgersicht ist die Teilarchivierung zu bemängeln, waren doch gerade die Befugnis, personenbezogen zu ermitteln, und der Inhalt der Verwaltungsermittlungsakten streitig. Damit war zu erwarten gewesen, dass Betroffene Berichtigungen, weitere Auskünfte und Löschungen beanspruchen würden. Die Verfahrensweise ist umso unverständlicher, als dass auch weitere gesetzliche Verfahren, in denen auf die Akten Bezug genommen wird, noch nicht abgeschlossen gewesen sind. Gerade den Abschluss aller Verfahren hatte ich aber gefordert. Solange war die gesamte Akte auch noch zur Aufgabenerfüllung erforderlich, vgl. 13/5.1.9 - am Ende.

Durch die ungleichmäßige Verfahrensweise bei den Teilakten entstehen nunmehr durch das Fortschreiben der noch in Bearbeitung stehenden Teilakten am Ende unterschiedliche Akteninhalte der sich im Übrigen ganz oder zum Teil inhaltlich überschneidenden Aktenbände.

Eine Akteneinsichtnahme wird zwischenzeitlich den Betroffenen immerhin durch das Hauptstaatsarchiv gewährt. Damit ist es den Betroffenen besser möglich gewesen, Inhalt, Umfang und Tiefe der z. T. gegen sie gerichteten Datenverarbeitung abzuschätzen und Gegendarstellungen abzugeben als bei einer bloßen Auskunft.

5.1.3 Leistungsbewertungen nach § 18 TVöD - Dokumentation

Nach den Tarifverträgen im öffentlichen Dienst wurden in den Ländern - auch in Sachsen - (für die Länder ab 2007 und für die Kommunen bereits 2005) Leistungsbewertungen im öffentlichen Dienst festgelegt.

In Bezug auf die die Tarifbestimmung jeweils umsetzenden Dienstvereinbarungen zwischen Dienststelle und Personalrat stellt sich daher die Frage, wie die Datenverarbeitung zu gestalten ist, ob, was und wo diesbezügliche Unterlagen aufzubewahren sind.

Während die Tarifparteien in § 12 LeistungsTV-Bund die Aufnahme des Ergebnisses der individuellen Leistungsfeststellung in die Personalakte vereinbart haben, hatten die Tarifparteien der Länder und Kommunen keine Regelung getroffen. Zwischenzeitlich ist nach dem Tarifvertrag für den öffentlichen Dienst der Länder vom 12. Oktober 2006 in der Fassung des Änderungstarifvertrages vom 1. März 2009 die Vorschrift über die Leistungsbewertung für den Freistaat gestrichen. Die damit einhergehende Datenverarbeitung findet daher auf staatlicher Ebene in Sachsen nicht mehr weiter statt. Im Wesentlichen ist hingegen die Leistungsbewertung in den Kommunen aufrechterhalten geblieben.

§ 37 Abs. 1 SächsDSG erlaubt die Verarbeitung, also auch die Speicherung, von Beschäftigtendaten im öffentlichen Dienst, soweit dies zur Eingehung, Durchführung, Beendigung oder Abwicklung des Dienst- oder Arbeitsverhältnisses erforderlich ist oder ein Gesetz, Tarifvertrag oder eine Dienstvereinbarung dies vorsieht. Nach § 18 TVöD soll das Leistungsentgelt dazu beitragen, die öffentlichen „Dienstleistungen“ zu verbessern. Zugleich sollen Motivation, Eigenverantwortung und Führungskompetenz gestärkt werden. Damit soll es ein Mittel zur Optimierung von Personalentwicklung und Personalführung sein. Sinn und Zweck des Leistungsentgeltes ist somit nicht nur die Zahlung eines zusätzlichen Entgeltes.

Bereits die Zahlung an sich macht es aus haushaltsrechtlichen Gründen erforderlich, das Ergebnis der Leistungsbewertung in der Personalakte (Bezüge) aufzubewahren. Aber auch die Bedeutung des Leistungsentgeltes über die Zahlung hinaus macht die Dokumentation erforderlich. Die Leistung ist neben der Befähigung notwendiger Bestandteil einer Regelbeurteilung. Die Leistungsbewertung kann dazu einen Beitrag liefern. Das steht auch nicht im Widerspruch zur Niederschriftserklärung zu § 18 TVöD der Tarif-

parteien Kommunen, die die systematische Leistungsbewertung nicht als Regelbeurteilung sehen. Es verbietet sich danach nur, die Regelbeurteilung der Vergabe von Leistungsentgelten zugrunde zu legen. Die Leistungsbewertung sollte an die vorangegangenen Leistungsbewertungen anschließen. Nur so ist es möglich, für die Zukunft sinnvolle Anforderungen festzulegen, differenziert auf die speziellen Bedingungen der Stelle und des Mitarbeiters einzugehen. Auch das macht eine Aufbewahrung der Leistungsbewertungen in der Personalakte erforderlich.

Es ist aus datenschutzrechtlicher Sicht sowohl eine Aufbewahrung der Ergebnisse der Zielvereinbarungen und systematischen Leistungsbewertungen in Bezüge- oder Beurteilungsakten als auch aufgeteilt in beiden möglich. Im Einzelnen sollte dies, sofern eine Dienstvereinbarung existiert, in dieser konkret geregelt werden.

Ich sehe auch die zeitweise Aufbewahrung von Zielvereinbarungen, Dokumentationen geführter Gespräche hinsichtlich des Leistungsentgeltes (z. B. wegen Änderung der Bedingungen) sowie von Kopien der Leistungsbewertungen durch den für die Leistungsbewertung zuständigen Vorgesetzten als erforderlich an, auch wenn in der Personalakte selbst nur die Ergebnisse der Leistungsbewertungen aufbewahrt werden sollten. Um eine zweckmäßige und kontinuierliche Fortführung der leistungsbezogenen Vergütung zu gewährleisten, ist eine vorübergehende Aufbewahrung dieser Unterlagen begründet.

Eine solche Handhabung ist jedoch in einer Dienstvereinbarung zu regeln, um transparent zu machen, wo sich vorbereitende Unterlagen zum Leistungsentgelt befinden dürfen. In der Dienstvereinbarung ist auch zu regeln, wann die vorbereitenden Unterlagen vernichtet werden müssen, denn eine ständige Aufbewahrung ist nicht erforderlich. Ich habe in einer mir zur Prüfung vorgelegten Dienstvereinbarung eine 3-Jahresfrist noch für angemessen gehalten.

5.1.4 Rechtswidrige Verarbeitung von Nebentätigkeitsangaben bei einer Gemeinde

Bei der Kontrolle einer Gemeinde stellte ich fest, dass in den Personalakten der Angestellten Nebentätigkeitserklärungen für das Jahr 2006 enthalten waren. Eine Erforderlichkeit war nicht gegeben. Mit dem Inkrafttreten des TVöD (Bund und Kommunen) am 1. Oktober 2005 gibt es keinen Verweis mehr auf die beamtenrechtlichen Vorschriften für die Arbeitnehmer der Kommunen. Die Beschäftigten haben lediglich die Nebentätigkeit ihrem Arbeitgeber rechtzeitig vorher anzuzeigen (§ 3 Abs. 3 TVöD). Erklärungen zur Nebentätigkeit nach § 9 SächsNTVO sind ab dem Jahr 2006 nicht mehr für Arbeitnehmer erforderlich und daher zu löschen. Eine Ausnahme ist nur dann möglich,

wenn eine abweichende Vereinbarung im Arbeitsvertrag vereinbart wurde und keine Tarifbindung besteht (§ 4 Abs. 3 TVG).

5.1.5 Stasi-Überprüfungen

Beinahe zwanzig Jahre nach dem Zusammenbruch der DDR finden weiterhin Überprüfungen von Mandatsträgern und kommunalen Wahlbeamten - auch nach der Novellierung des Stasi-Unterlagengesetzes - statt (vgl. 13/5.1.3). Ein Wahlbeamter wurde, obwohl er bereits seit mehreren Jahren als solcher tätig war, im Jahr 2008 auf Stasi-Tätigkeit gemäß §§ 20 Abs. 1 Nr. 6b, 21 Abs. 1 Nr. 6b StUG überprüft. Er wandte sich an mich, da er über die Überprüfung nicht informiert gewesen sei. Die Gemeinde erklärte hingegen, der Betroffene sei informiert gewesen, da es bereits im Jahr 2004 einen Stadtratsbeschluss gegeben habe, nach dem eine Überprüfung stattfinden sollte. Die Überprüfung erfolgte zunächst aber nicht, weil man irrtümlich dachte, dass eine Zustimmung des Betroffenen hierfür erforderlich gewesen sei. Erst später erkannte die Verwaltung, dass eine Zustimmung nicht erforderlich war und holte die Überprüfung nunmehr nach.

Tatsächlich musste der Wahlbeamte nach den §§ 20 Abs. 1 Nr. 6b, 21 Abs. 1 Nr. 6b StUG nur vorher informiert werden. Allerdings hätte der Betroffene im vorliegenden Fall von der erst Jahre später veranlassten Überprüfung informiert werden müssen. Er musste nicht mehr damit rechnen, erst nach Jahren überprüft zu werden. Da er aber inzwischen auch von dem Ergebnis der Überprüfung informiert wurde und die Gemeinde lediglich eine falsche Rechtsauffassung vertreten hat, habe ich den Vorgang nicht weitergehend moniert.

Grundsätzlich gilt zusätzlich, dass Überprüfungen „nach Maßgabe der dafür geltenden Vorschriften“ durchzuführen sind. Gemeinden haben das Überprüfungsverfahren im Einzelnen in einer Satzung zu regeln. Auch auf Landesebene fehlen noch immer die gesetzlichen Regularien eines geordneten Verfahrens für den nach der Novellierung des Stasi-Unterlagengesetzes geringer gewordenen Kreis zu überprüfender Amtsträger (vgl. den Wortlaut der §§ 20 Abs. 1 und 21 Abs. 1 StUG - am Anfang).

5.1.6 Präsentation von Beschäftigtendaten im Internet

In 7/5.5.1 habe ich die Auffassung vertreten, dass ein Einstellen von Beschäftigtendaten, also von Namen, behördlichen Anschriften, Telefonnummern usw. in das Internet, auch bei Vorliegen einer Einwilligung grundsätzlich unzulässig sei. Allenfalls käme eine Veröffentlichung der Daten von Beschäftigten in herausgehobener Position (Bürgermeister, Dezernenten, Amtsleiter, Referatsleiter) in den Netzen (im behördeninternen Intranet ohne, im weltweit zugänglichen Internet nur mit Einwilligung) in Betracht.

Nach der Neufassung der Vorschrift zur Beschäftigtendatenverarbeitung im Sächsischen Datenschutzgesetz (SächsDSG 1991: § 31 Abs. 2, SächsDSG 2003: § 37 Abs. 2) ist nunmehr die Rechtslage eine andere. Eine entsprechende Veröffentlichung ist gemäß § 37 Abs. 2 Nr. 2 SächsDSG auch dann möglich, wenn dies für die Information der Allgemeinheit erforderlich ist. Unter Bezugnahme auf ein Urteil des OVG Koblenz vom 10. September 2007 (Az.: 2 A 10413/07.OVG) gehe ich nunmehr davon aus, dass Dienstherren sich für einen „personalisierten“ Behördenauftritt und auch zu einem entsprechenden Internetauftritt mit personenbezogenen Namens- und Kontaktangaben und dies auch ohne Einwilligung der betroffenen Bediensteten zu entscheiden befugt sind. Das gilt jedenfalls insoweit, als dass es sich um Beschäftigte handelt, die auch Außenkontakte haben und die Dienststelle nach außen vertreten können sollen. Nach der Rechtslage in Sachsen ist gemäß § 37 Abs. 2 Nr. 2 SächsDSG aber zu prüfen, ob einer Veröffentlichung im Einzelfall keine schutzwürdigen Interessen des Betroffenen entgegenstehen. Der Veröffentlichung und Weitergabe von Namen, Funktionen und Erreichbarkeit per E-Mail können u. a. Fürsorgepflichtgesichtspunkte bzw. Sicherheitsbelange entgegenstehen, so etwa bei Bediensteten, die aufgrund ihrer Funktion und Aufgaben als gefährdet gelten. Soweit Angaben zu Beschäftigten, *zu deren Aufgaben Außenkontakte zählen*, mit Kontaktdaten im Internet veröffentlicht werden sollen, ist also eine entsprechende Organisationsentscheidung im Rahmen der Ausübung eines pflichtgemäßen Ermessens bei Abwägung der Interessen zu treffen. Abbildungen Bediensteter können nur nach Einwilligung der Betroffenen veröffentlicht werden, § 22 KunstUrhG (vgl. ausführlich unter 13/5.5.1).

Maßgeblich für die Bestimmung des von der Veröffentlichung betroffenen Personenkreises ist die zugewiesene Funktion. Der Umstand, ob der Beschäftigte hingegen bereits Außenkontakte hat, ist jedenfalls nur eingeschränkt entscheidungserheblich. Käme es allein hierauf an, so würde dies die Absicht des Dienstherrn, den Behördenzugang durch eine Personalisierung zu erleichtern und damit Kontakte zu der Behörde zu verbessern, von vorneherein erschweren.

§§ 117 Abs. 3 Satz 1 und 121 Abs. 2 SächsBG, demzufolge Personalaktendaten zu schützen sind und Auskünfte an Dritte nur mit Einwilligung des Beamten erteilt werden dürfen, stehen einer Veröffentlichung nicht entgegen. Ohnehin betrifft die Vorschrift unmittelbar nur Beamte. Zudem regelt die Bestimmung die individuelle Weitergabe von Personalaktendaten (des Beamten) und erfasst nicht die Amtsträgerdaten, die ihn als Teil der Behördenorganisation mit Namen und dienstlichen Kontaktdaten betreffen.

Ich rege im Zusammenhang mit der Frage der Veröffentlichung von Bedienstetendaten an, gemessen an den Anforderungen an die Behörde, auch die Verwendung funktionsbezogener Angaben und E-Mail-Adressen oder Zentral-Postfachadressen in die Überle-

gungen zur Entscheidung, wie und was veröffentlicht werden soll, einzubeziehen (vgl. 12/5.1.11). Hierdurch werden zum einen gleichmäßige Informationsflüsse und ein registrierbarer E-Mail-Posteingang bei den Geschäftsabläufen erreicht, zum anderen kann bei Mitarbeiterwechseln die Kommunikation nahtlos weitergeführt werden. Diese Organisationsgesichtspunkte sollten bei allen Vorzügen eine noch bürgerfreundlichere Außendarstellung der Behörden zu erreichen, nicht in den Hintergrund treten. Bei Funktions-E-Mail-Adressen wird letztendlich auch vermieden, dass bei einer unvorhergesehenen Abwesenheit eines Beschäftigten der entsprechende E-Mail-Posteingang eingesehen werden kann. Dies wäre anderenfalls bei erlaubter privater Nutzung der personenbezogenen E-Mail-Adresse ein Verstoß gegen das Fernmeldegeheimnis (vgl. 13/5.1.6).

5.1.7 Anpassung des Sächsischen Beamtengesetzes und Ausblick

Im Zuge der Föderalismusreform sind mit dem bundesrechtlichen Beamtenstatusgesetz (BeamtStG) rechtliche Grundlagen für alle Beamten in Deutschland geschaffen worden. Eine Regelung betrifft das Personalaktenrecht. So regelt § 50 BeamtStG den materiellrechtlichen Personalaktenbegriff. Insofern konnte § 117 Abs. 1 SächsBG angepasst werden und verweist auf die Vertraulichkeit der Personalakte nach § 50 Satz 2 BeamtStG. § 117 Abs. 1 Satz 1 SächsBG regelt, dass die in Dateien gespeicherten Personalaktendaten zur Personalakte gehören. Das ist inhaltlich nichts Neues. Soweit eine digitale Personalakte in Sachsen angestrebt wird, wäre im Sächsischen Beamtengesetz dennoch eine ausdrückliche Befugnis hierfür zu schaffen. Im Übrigen rate ich bei einer zukünftigen weitergehenden Novellierung des Sächsischen Beamtengesetzes die abschließende Nennung der Dateien, in denen Daten des Beamten verarbeitet werden, in einem *in der Grundakte zu führenden Dateiverzeichnis* gesetzlich vorzuschreiben, aus Gründen der Rechtsklarheit einen Zugriff der Innenrevision auf Personalakten zu normieren und das Arbeitnehmerrecht dem beamtengesetzlichen Personalaktenrecht per gesetzlicher Verweisung im Sächsischen Datenschutzgesetz weitgehend anzugleichen.

5.1.8 Ressortübergreifende Personalvermittlungsplattform II

In meinem 13. Tätigkeitsbericht hatte ich bereits über das Vorhaben der Staatsregierung berichtet, eine ressortübergreifende Personalvermittlungsplattform einzurichten. Ich hatte im Einklang mit § 4 Abs. 1 SächsDSG eine gesetzliche Regelung, nicht lediglich eine Verwaltungsvorschrift, gefordert, 13/5.1.2.

Zwischenzeitlich ist eine gesetzliche Regelung in Kraft getreten, das *Gesetz über die Verarbeitung personenbezogener Daten in der Personalvermittlungsplattform (Sächsisches Personalvermittlungsplattformgesetz - SächsPVPG)*.

Vereinzelt erhalte ich deswegen Nachfragen. Gegen das Gesetz in der jetzigen Fassung habe ich aber keine Bedenken erhoben.

Das Personalvermittlungsplattformgesetz enthält einen Katalog der zu verarbeitenden Daten des Beschäftigten in § 2 Abs. 2. Die Verarbeitung der gesetzlich vorgesehenen Angaben ist vertretbar. Mit Einwilligung des Beschäftigten sollen darüber hinaus weitere personenbezogene Daten gespeichert werden können, die für eine ressortübergreifende Vermittlung *förderlich* sind. Hierbei kann es sich nur um einschlägige Informationen handeln, wie weitergehende Ausbildungsnachweise, ggf. Sprachkenntnisse usw. Beim Vollzug der Bestimmung ist datensparsam zu verfahren, § 9 Abs. 1 Satz 2 SächsDSG. Ob die Angaben verarbeitet werden können, entscheidet nicht der Bedienstete, sondern die Dienststelle im Sinne einer gleichmäßigen Datenverarbeitung nach Erforderlichkeitsgesichtspunkten. Nicht notwendige Angaben und eingereichte Dokumente sind ggf. an den Bediensteten zurückzugeben.

5.2 Personalvertretung

5.2.1 Datenschutzorganisatorische Anforderungen bei Löschungen / Kein ordnungsgemäßer Auftrag gemäß § 7 SächsDSG

Ein Personalratsmitglied bat einen Bekannten, der über einen Brennofen verfügt, für ihn einige Unterlagen des Personalrates, die nicht mehr benötigt wurden, zu verbrennen. Dabei handelte es sich zum Teil um geheimhaltungsbedürftige Unterlagen aus Personalratssitzungen, Schreiben des Dienstherrn und weitere Schriftstücke, in denen personenbezogene Daten enthalten waren. Der Bekannte übernahm die Unterlagen, um diese zu verbrennen. Durch Zufall wurden diese Unterlagen jedoch noch unverbrannt aufgefunden. Davon wurde ich informiert. Ich hatte nun zu prüfen, ob hier ein Datenschutzverstoß vorlag.

Das Sächsische Datenschutzgesetz gilt auch für den Personalrat als Teil der Behörde bzw. eigenständige funktionale öffentliche Stelle. Die Bitte an einen Bekannten, Unterlagen zu verbrennen, Daten zu löschen, war die Bitte um eine Gefälligkeit, da kein Rechtsbindungswille auf beiden Seiten vorhanden war. Demzufolge konnte es sich auch nicht um einen Auftrag im Sinne von § 7 SächsDSG handeln. Es gab keinen Auftraggeber oder Auftragnehmer, ohnehin - wie nach dem Gesetz erforderlich - keinen schriftlichen Vertrag, in dem Gegenstand und Umfang der Datenverarbeitung sowie die zu treffenden Maßnahmen geregelt waren. Der Personalrat hätte aber einen Auftrag gemäß § 7 SächsDSG erteilen müssen, sofern er die Unterlagen nicht selbst zu vernichten beabsichtigte. Mit der Weitergabe der Daten an einen Dritten, einen Unbefugten (da dem Bekannten kein Auftrag gemäß § 7 SächsDSG erteilt wurde) wurden bereits Personalratsgeheimnisse verletzt. Im Übrigen wäre eine Person, nur weil diese über einen Brenn-

ofen verfügt, nicht allgemein geeignet, um personenbezogene Daten zu löschen. Gemäß § 7 Abs. 2 SächsDSG ist der Auftragnehmer unter besonderer Berücksichtigung der Eignung der von diesem getroffenen personellen, technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. Ist eine ordnungsgemäße Löschung von Daten vorgesehen, so hätte der Personalrat als Stelle ein Fachunternehmen beauftragen oder die Dienststelle selbst (unter Beteiligung des Personalrats) um die Löschung bitten müssen, wollte er sich die erforderliche Technik zur Datenlöschung nicht selbst anschaffen.

5.3 Einwohnermeldewesen

5.3.1 Erhebung von Meldedaten durch die GEZ

Eine sächsische Gemeinde wurde von einem Gebührenbeauftragten der GEZ gebeten, eine Liste mit allen Einwohnern im Alter zwischen 16 und 28 Jahren (da bei diesen die Anmeldedichte sehr niedrig sei), gelistet nach Straße, Hausnummer, Name, Vorname und Geburtsdatum an ihn zu übermitteln. Da sie jedoch (zu Recht) Zweifel an der Rechtmäßigkeit einer entsprechenden Datenübermittlung hatte, wandte sie sich an das zuständige LRA, dieses an das zuständige RP (jetzt Landesdirektion) und letzteres schließlich an das SMI.

Das SMI ging in einem ersten Antwortentwurf, der mir freundlicherweise vorab zur Stellungnahme übersandt wurde, von der grundsätzlichen Zulässigkeit einer derartigen Übermittlung aus. Nach einem umfangreichen Schriftwechsel, in den auch die SK einbezogen wurde, konnte ich das SMI davon überzeugen, dass eine gesetzmäßige Datenverarbeitung mit einer listenweisen Übermittlung von Einwohnerdaten seitens der Melderegisterbehörde nicht auf das Sächsische Meldegesetz gestützt werden konnte.

Die Erhebung von Meldedaten durch die GEZ ist im Rundfunkgebührenstaatsvertrag geregelt. Eine Erhebung bei Meldebehörden ist gemäß § 4 Abs. 6 Satz 1 RGebStV bei Personen, bei denen *tatsächliche Anhaltspunkte* vorliegen, dass sie ein Rundfunkgerät zum Empfang bereithalten und dies nicht oder nicht umfassend angezeigt haben, zulässig. Dies war vorliegend jedoch nicht der Fall, vielmehr lag lediglich eine bloße Vermutung in Bezug auf eine Gesamtgruppe *nicht namentlich bekannter Einwohner* anhand nicht substantiiert dargetaner statistischer Erfahrungswerte vor.

Gemäß § 4 Abs. 6 Satz 2 RGebStV bleiben weiterhin *besondere* melderechtliche Regelungen des Landesrechts, die eine Übermittlung von Daten an Landesrundfunkanstalten oder die von ihnen beauftragte Stelle zulassen, unberührt. Das Sächsische Meldegesetz enthält lediglich eine derartige besondere Regelung: Die regelmäßige Datenübermitt-

lung nach § 30a SächsMG. Danach kann eine Datenübermittlung „im Falle der Anmeldung, Abmeldung oder des Todes“ erfolgen. Auch dies war vorliegend nicht der Fall.

Wie auch das SMI letztlich einsah, wäre im vorliegenden Fall die Erteilung der gewünschten Gruppenauskunft rechtswidrig gewesen (siehe auch Rech, DuD 2009, 231). Diese Auffassung teilte sie den drei sächsischen Landesdirektionen in einem Schreiben im Herbst 2008 mit. Ich gehe daher davon aus, dass die GEZ keine Gruppenauskünfte von sächsischen Meldeämtern erhält.

5.3.2 Bundesverwaltungsgerichtsentscheidung vom 3. Juni 2006 (Az. 6 C 05/05)

In meinem letzten Tätigkeitsbericht hatte ich auf die Möglichkeit hingewiesen, der Übermittlung der Meldedaten an Private im Wege der einfachen Melderegisterauskunft zu widersprechen, wenn die Daten vom Empfänger erkennbar zu Zwecken der Direktwerbung verwendet werden sollen, 13/5.3.5.

Bei meinen Kontrollen im letzten Berichtszeitraum stellte ich fest, dass die Möglichkeit, den Widerspruch auszuüben, von einzelnen Gemeinden nicht gewährt wurde, da die Melderegistersoftware die Berücksichtigung des Widerspruchs nicht vorsehe.

Demgegenüber hatte das SMI Hinweise gegeben, wie der Widerspruch im System berücksichtigt werden kann. Auch sind die Melderegisterbehörden pflichtig, bei den Softwareverfahrenherstellern eine an die Rechtslage angepasste Software zu beauftragen.

Im Fall der Ausübung des Widerspruchs mit dem vorgenannten Inhalt ist gleichfalls ein Widerspruch gegen eine automatisierte Auskunftserteilung im Wege des automatisierten Abrufs bei der einfachen Melderegisterauskunft einzutragen, § 32 Abs. 4 Satz 4 SächsMG, da beim automatisierten Abruf eine Prüfung der Meldebehörde nicht vorgenommen werden kann.

5.3.3 Kommunales Kernmelderegister

Gegen Ende des Berichtszeitraums besuchte meine Behörde das neu eingerichtete Kommunale Kernmelderegister bei der SAKD in Bischofswerda. Zu diesem Zeitpunkt war das zentrale Melderegister zu 97 % mit den Teil-Datensätzen der gemeindlichen Meldebehörden befüllt worden. In der Praxis wurde über vielfältige Zuordnungsprobleme bei Meldedatenänderungen bzw. dem Abgleich zwischen gemeindlichen Meldedaten und dem KKM berichtet. Eine regelmäßige Datenübermittlung nach § 4a SAKDG konnte zum Zeitpunkt meines Besuchs, obwohl gesetzlich vorgesehen, nicht

festgestellt werden. Die Datenabrufe von nach der neuen Sächsischen Meldeverordnung berechtigten Stellen konnten bei der SAKD im Übrigen anhand von Protokolldaten datenschutzgerecht nachvollzogen werden. Zum Zeitpunkt meiner Kontrolle waren erst wenige Abrufverfahren eingerichtet und die überschaubaren Abrufe befanden sich zum Teil noch im Test.

Zwischenzeitlich sind immer mehr Abrufverfahren für empfangende Stellen - auch nach § 39 SächsMeldVO - eingerichtet worden. Nach der Verordnung sind keine besonderen Voraussetzungen an die Einrichtung der Abrufverfahren nach § 39 geknüpft. Abrufverfahren sind rechtlich mit einer Gesamtdatenübermittlung der abrufbaren Daten gleichzusetzen. Datenschutzorganisatorisch halte ich diese Öffnung des KKM für bedenklich, werden auf diese Weise die Melderegisterdaten, ohne dass die SAKD als Meldebehörde Entscheidungen zu den Übermittlungen zu treffen in der Lage ist, potentiell für hunderte Behörden und ggf. *Nutzerkonten* in sächsischen Behörden zugänglich. Bereits in meinem letzten Tätigkeitsbericht hatte ich die Verordnung in diesem Punkt bemängelt, 13/5.3.2. Mit der Bestimmung, dass meine Behörde nach § 39 Abs. 2 Satz 2 SächsMeldVO von der Einrichtung der Abrufverfahren zu unterrichten ist, versucht der Verordnungsgeber offenbar die datenschutzorganisatorischen Risiken zu kaschieren. Die Unterrichtungspflicht hilft datenschutzorganisatorisch nicht, da meine Behörde die Einrichtung der Abrufverfahren nicht mitzuentscheiden berechtigt ist.

Das KKM und den Vollzug werde ich erneut kontrollieren.

5.4 Personenstandswesen

5.4.1 Ausleihe gegen Abgabe des Personalausweises

Ein Besucher einer staatlichen Einrichtung hatte Bedenken geäußert, ob die zeitweise Abgabe des Personalausweises bei der Ausleihe eines Audioguides dem Datenschutz entspreche.

Anfragen dieser Art erhalte ich von besorgten Bürgern häufig.

Bei einer unentgeltlichen Ausleihe kommt es zwischen Entleiher und Verleiher zu einem Leihvertrag. Wird auch nur ein geringes Entgelt für das zur Verfügung gestellte Gerät verlangt, wird ein Mietvertrag zwischen Mieter und Vermieter abgeschlossen. In beiden Fällen ist der Verleiher als auch der Vermieter aus Geschäftszwecken daran interessiert, das von ihm zur Verfügung gestellte Gerät in ordnungsgemäßem Zustand zurück zu erhalten. Für den Verleiher oder Vermieter ist es daher erforderlich zu wissen, wem er sein Gerät überlässt. Daher ist eine Erhebung der Personalausweisdaten und auch eine Überprüfung mittels Personalausweis zulässig.

Die vorübergehende Aufbewahrung des Personalausweises ist ebenso ein Erheben von Personalausweisdaten und somit erlaubt.

Alternativ könnte der Verleiher oder Vermieter die Personaldaten auch schriftlich aufnehmen und bis zur Feststellung der ordnungsgemäßen Rückgabe aufbewahren. Jedoch hätte das den Nachteil, dass eine Speicherung erfolgen würde. Der Datenträger müsste unter Beachtung der datenschutzrechtlichen Vorschriften nach Wegfall der Erforderlichkeit gelöscht werden.

Davon abgesehen, dass eine Speicherung aufwändiger ist, geht sie auch weiter als nur das Erheben.

Im Übrigen steht es im Ermessen des Entleihers oder Mieters das Angebot zum Vertragsabschluss abzulehnen, wenn er seine Personalausweisdaten nicht offenbaren will. Ist er jedoch bereit, den Vertrag mit dem Verleiher oder Vermieter abzuschließen, willigt er auch in die Erhebung seiner Daten ein. Dass auf eine schriftliche Einwilligung bei dem aktiven Übergeben und nur zeitweisen Überlassen des Ausweisdokuments verzichtet wird (vgl. aber § 4 Abs. 3 SächsDSG), ist üblich und - so meine ich - eigentlich sozialadäquat. Hilfreich ist es jedoch, das Verfahren so transparent zu gestalten, dass dem Besucher mögliche Ängste einer missbräuchlichen Verwendung seines Personalausweises genommen werden.

5.5 Kommunale Selbstverwaltung

5.5.1 Kommunale Videoüberwachungen

Die zunehmende Videoüberwachung öffentlich zugänglicher Flächen durch Gemeinden (z. B. von Markt- und Rathausvorplätzen, Schulen, Abfallcontainern) bildete einen meiner Tätigkeitsschwerpunkte im Berichtszeitraum. Mit dieser Zunahme an Überwachung des öffentlichen Raums wird die Verhaltensfreiheit und mitunter auch die Privatheit der redlichen Passanten und sonstigen Betroffenen - darunter auch häufig Arbeitnehmer der Gemeinden - vielfach über Gebühr eingeschränkt. Jede Videoüberwachung und ggf. auch -aufzeichnung greift in Grundrechte, zumindest in das Recht auf informationelle Selbstbestimmung (Art. 33 SächsVerf), mitunter auch in die allgemeine Handlungsfreiheit, ein. Jeder hat jedoch ein Recht darauf, sich grundsätzlich unbeobachtet von der öffentlichen Gewalt im öffentlichen Raum, den Straßen und Plätzen seiner Gemeinde, bewegen zu können. Ich rate deshalb allen Gemeinden, genau zu prüfen, ob die Voraussetzungen einer Videoüberwachung und ggf. -aufzeichnung sowie die sonstigen Voraussetzungen von § 33 SächsDSG erfüllt sind. Andernfalls werde ich im Einzelfall von meinem Recht zur förmlichen Beanstandung nach § 29 SächsDSG Gebrauch machen.

Nur beispielhaft seien folgende drei aus über 60 Fällen, mit denen ich im Berichtszeitraum befasst war, genannt: In einem Fall wurde der Rathausvorplatz sowie eine angrenzende Straßenkreuzung überwacht und die Bilder für 72 Stunden gespeichert, da es zuvor zahlenmäßig nicht näher belegte Schmierereien auf der Fahrbahn sowie illegale Plakatierungen an einer ehemaligen Kaufhalle gegeben habe. In einem anderen Fall wurden in einem Pilotprojekt die Standorte von Wertstoffcontainern überwacht und die Bilder für 72 Stunden gespeichert, um über die Kfz-Kennzeichen der zur Anlieferung genutzten Fahrzeuge die Verursacher von Verschmutzungen besser identifizieren zu können. In einem dritten Fall wurden an einer grenznah gelegenen aufwändig sanierten Erholungs- und Freizeitanlage Kameraattrappen angebracht, um von Sachbeschädigungen, Diebstählen und Vandalismus abschrecken zu können; allerdings hatte es zuvor dort konkrete Vorkommnisse nicht gegeben.

Waren diese Maßnahmen rechtmäßig? Nach § 33 Abs. 1 SächsDSG dürfen Gemeinden öffentlich zugängliche Räume mit Videotechnik nur beobachten, soweit dies zur Aufgabenerfüllung, insbesondere zur Gewährleistung der öffentlichen Sicherheit und Ordnung, oder zur Wahrnehmung des Hausrechts *erforderlich* ist und *schutzwürdige Interessen Betroffener nicht überwiegen*. Nach § 33 Abs. 2 SächsDSG dürfen die erhobenen Daten nur gespeichert und weiterverarbeitet werden, wenn die Speicherung und weitere Verarbeitung zum Erreichen des verfolgten Zwecks erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen des Betroffenen überwiegen. Inhalt und Reichweite der gesetzlichen Befugnis zur Videoüberwachung und -aufzeichnung bestimmen sich somit insbesondere nach dem Erforderlichkeitsprinzip sowie einer Abwägung mit den schutzwürdigen Interessen der Betroffenen (Passanten, Besucher, Mitarbeiter).

Erforderlich ist eine Videoüberwachung nur, wenn die Gemeinde ihre Aufgabe ohne die Videoüberwachung nicht, nicht rechtzeitig oder nicht vollständig erfüllen könnte. Die Videoüberwachung und -aufzeichnung sind letzte Mittel („ultima ratio“). Sie dürfen nur stattfinden, wenn andere, „konventionelle“ Mittel, die die Grundrechte der Betroffenen nicht berühren oder in diese weniger tief eingreifen (z. B. verstärkte Beleuchtung der Fläche, Bestreifung durch Polizei oder Sicherheitsdienst, Gefährderansprachen), sich bereits als ungeeignet herausgestellt haben. Vor jeder Videoüberwachung müssen also nachweislich andere „konventionelle“ Maßnahmen zur Abwehr der Gefahren oder zur Verbesserung der Ahndung von Ordnungswidrigkeiten oder Straftaten ergriffen worden sein. Die Videoüberwachung und -aufzeichnung darf nicht von vornherein als das vermeintlich leichteste Mittel zur Erreichung des Zwecks herangezogen werden.

Doch selbst wenn zuvor herkömmliche Maßnahmen erfolglos ergriffen worden sind, ist Videoüberwachung nur zulässig, wenn sie sich nach einer Abwägung mit den schutz-

würdigen Interessen der Betroffenen als angemessen erweist (Übermaßverbot). Dazu ist jeder einzelne Kamerastandort nach Art, Umfang und Intensität des Eingriffs in die Grundrechte der Betroffenen zu dem Zweck der Maßnahme - namentlich den vorzubeugenden illegalen Handlungen nach Art, Häufigkeit und Schadenshöhe - ins Verhältnis zu setzen. Zu berücksichtigen ist, dass es sich im Fall der präventiven Überwachung um Maßnahmen handelt, die im Vorfeld einer konkreten Gefahr getroffen werden. Die Betroffenen sind überwiegend nicht aufgrund bestimmter Anhaltspunkte verdächtig, Rechtsgüter zu gefährden. Insoweit wird mit einer Videoüberwachung der Grundsatz durchbrochen, dass der Einzelne nur dann „polizeipflichtig“ gemacht werden kann, wenn er hierfür einen hinreichenden Anlass gegeben hat. Videoüberwachung ist deshalb nur dann angemessen, wenn die Begehung von Straftaten oder schwerwiegenden Ordnungswidrigkeiten in nennenswertem Umfang verhindert werden soll. Hierfür ist der Nachweis, dass an dem konkreten Ort bereits rechtswidrige Handlungen von einigem Gewicht sowie in nicht unerheblichem Umfang begangen worden sind, zu führen. Allein die Annahme, dass irgendwann irgendjemand z. B. die öffentliche Anlage beschädigen oder zerstören werde, vermag eine *Erforderlichkeit* der Videoüberwachung nicht zu begründen. Auch der bloße Hinweis auf künftige hohe Schäden vermag eine Videoüberwachung nicht zu rechtfertigen.

Diese Grundsätze gelten in gleicher Weise für Videokameraattrappen, da diese ebenso wie „echte“ Kameras in das Recht auf informationelle Selbstbestimmung eingreifen. Attrappen erzeugen den gleichen Anpassungsdruck auf die Betroffenen wie „echte“ Kameras. Das Bundesverfassungsgericht erkennt in ständiger Rechtsprechung, dass dieses Grundrecht auch vor einem „*Einschüchterungseffekt*“ schützt, der entsteht und zu Beeinträchtigungen bei der Ausübung anderer Grundrechte führt, „wenn für den Einzelnen nicht mehr erkennbar ist, wer, was, wann und bei welcher Gelegenheit über ihn weiß“. Die Freiheit des Einzelnen, aus eigener Selbstbestimmung zu planen und zu entscheiden, kann dadurch wesentlich gehemmt werden. Ein von der Grundrechtsausübung abschreckender Effekt fremden Geheimwissens müsse nicht nur im Interesse der betroffenen Einzelnen vermieden werden. Auch das Gemeinwohl werde hierdurch beeinträchtigt, weil Selbstbestimmung eine „elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger gegründeten freiheitlich demokratischen Gemeinwesens ist“. Das bedeutet: Auch wenn in Wirklichkeit keine Daten verarbeitet werden, genügt der Anschein der Datenverarbeitung, weil die Auswirkungen der Maßnahme auf den Betroffenen die gleichen wie bei einer „echten“ Datenverarbeitung sind.

Schließlich ist die Tatsache der Videoüberwachung und die verantwortliche Stelle durch geeignete Maßnahmen erkennbar zu machen (§ 33 Abs. 3 SächsDSG). Vor dem Betre-

ten des überwachten Bereichs muss durch deutlich sichtbare Schilder je nach den Umständen des Einzelfalls - in Touristenregionen oder im Grenzgebiet mehrsprachig - sichergestellt sein, dass die Betroffenen von dieser Maßnahme Kenntnis erhalten und sich darauf einstellen können. Schließlich ist ein Verfahrensverzeichnis nach § 10 SächsDSG zu führen und, falls kein Datenschutzbeauftragter bestellt worden ist, mir zuzuleiten.

In dem oben genannten ersten Fall ist die Videoüberwachung nach meiner Beanstandung eingestellt worden. In dem zweitgenannten Fall hat sich die Gemeinde - auch unter Berücksichtigung des hohen Personalaufwands - entschlossen, das Pilotprojekt nicht weiter zu verfolgen.

Lediglich in dem drittgenannten Fall werde ich weiter auf ein rechtskonformes Verhalten der Gemeinde hinwirken müssen.

Eine erste Prüfung der Zulässigkeit einer beabsichtigten Videoüberwachung mag durch folgende, an § 33 SächsDSG orientierte, Checkliste erleichtert werden:

1. Welche öffentlich zugänglichen Räume sollen zu welchen Zwecken videoüberwacht werden?

2. Kann ausreichend belegt werden, dass eine Videoüberwachung erforderlich ist, m. a. W.: dass die Kommune ihre Aufgabe anders nicht, nicht rechtzeitig oder nicht vollständig erfüllen kann?

3. Welche „konventionellen“ Maßnahmen zur Erreichung des Zwecks wurden zuvor ergriffen?

4. Gibt es Anhaltspunkte für schutzwürdige Interessen Betroffener und überwiegen diese ggf. den in der Überwachung liegenden Eingriff?

5. Ist über die Überwachung hinaus eine Speicherung der erhobenen Daten zum Erreichen des verfolgten Zwecks erforderlich?

6. Gibt es Anhaltspunkte für schutzwürdige Interessen Betroffener und überwiegen diese ggf. den in der Speicherung liegenden Eingriff?

7. Wie wird sichergestellt, dass die gespeicherten Daten für keine anderen Zwecke als die Abwehr von Gefahren für die öffentliche Sicherheit sowie zur Verfolgung von Straftaten oder Ordnungswidrigkeiten verarbeitet werden?

8. Welche Personen haben Zugang zu den gespeicherten Daten und welche Maßnahmen wurden zur Gewährleistung des Datenschutzes insbesondere nach § 9 Abs. 2 SächsDSG ergriffen?

9. Sind die technischen Voraussetzungen für eine datenschutzgerechte Videoüberwachung und ggf. -speicherung erfüllt (vgl. http://www.bfdi.bund.de/cln_029/nn_533554/SharedDocs/Publikationen/Arbeitshilfen/Schutzprofil,templateId=raw,property=publicationFile.pdf/Schutzprofil.pdf)?

10. Ist ein Verzeichnis nach § 10 Abs. 1 SächsDSG erstellt worden?

11. Ist das Verzeichnis dem Sächsischen Datenschutzbeauftragten oder dem Datenschutzbeauftragten nach § 11 SächsDSG zugeleitet worden?

12. Werden evtl. besonders heikle Daten nach § 4 Abs. 2 SächsDSG oder Beschäftigtendaten nach § 37 SächsDSG verarbeitet? Sind ggf. die erforderlichen Vorabkontrollen (§ 10 Abs. 4 SächsDSG) erfolgt und hat die erforderliche Beteiligung des Personalrats (§ 80 Abs. 3 Nr. 16 SächsPersVG) stattgefunden?

13. Wie lange sollen die Aufzeichnungen gespeichert bleiben bzw. wann sollen sie gelöscht werden?

14. Wie würde die Videoüberwachung und die verantwortliche Stelle erkennbar gemacht (§ 33 Abs. 3 SächsDSG)?

15. Nach welchen Zeiträumen soll die Videoüberwachung und ggf. auch -speicherung evaluiert werden?“

5.5.2 Niederschriften von Gemeinderatssitzungen im Internet

Neben der Frage nach der Zulässigkeit von Tonbandaufzeichnungen von Gemeinderatssitzungen, zu der ich mich zu verschiedenen Anlässen geäußert habe (vgl. TB 3, 4, 10, 12), erhalte ich zunehmend, auch von Gemeinderäten, Nachfragen zur Zulässigkeit der Veröffentlichung von Niederschriften von Gemeinderatssitzungen im Internet, wie sie durch verschiedene Gemeinden vorgenommen werden. Auch hierzu habe ich mich bereits geäußert (12/5.5.9).

Für die Verwendung der Niederschriften der öffentlichen Sitzungen des Gemeinderates ist § 40 Abs. 2 Satz 5 SächsGemO zu beachten, der bestimmt, den Einwohnern die Einsichtnahme in die Niederschriften über die öffentlichen Sitzungen zu gestatten. Eine höhere Transparenz und Bürgerfreundlichkeit des Gemeinderates durch eine Veröffentlichung der Niederschriften von öffentlichen Sitzungen anzustreben, ist zwar grundsätz-

lich zu begrüßen. Die Niederschriften sind jedoch amtliche Dokumente der Gemeinde, deren Inhalt und Form den Regelungen des § 40 SächsGemO unterliegen. Hinsichtlich der Verarbeitung personenbezogener Daten ist das Sächsische Datenschutzgesetz und die Geheimhaltungsvorschriften in Spezialgesetzen wie beispielsweise im Sozial- und Steuerbereich zu beachten.

Im Gegensatz zu dem in § 40 Abs. 2 Satz 5 SächsGemO vorgesehenen Maß der Kontrolle durch den Bürger - den Einwohner! - durch Einsichtnahme in die Niederschrift der öffentlichen Gemeinderatssitzung wird hier die Öffentlichkeit weltweit zugänglich im Internet hergestellt. Dabei ist zu beachten, dass sich durch eine automatisierte Auswertung Anwesenheitsprofile einzelner Gemeinderatsmitglieder durch das in § 40 Abs. 1 SächsGemO geregelte namentliche Festhalten der Anwesenheit und (unter Angabe des Grundes) der Abwesenheit erstellen lassen. Damit ist das informationelle Selbstbestimmungsrecht der Gemeinderatsmitglieder betroffen. Selbst wenn § 40 Abs. 2 Satz 5 SächsGemO eine Veröffentlichung der Niederschrift im Internet zuließe, wäre unabhängig davon und unter Beachtung der sonstigen gesetzlichen Regelungen zum Schutz personenbezogener Daten eine derartige Veröffentlichung nur mit Einwilligung aller Mitglieder des Gemeinderates möglich. Darüber hinaus erweist sich eine Veröffentlichung über das Internet in der Praxis auch bei datenschutzbewussten Gemeinden als nicht einfach. Sie realisieren, dass Persönlichkeitsrechte weiterer Personen, von Bürgern und Sachverständigen betroffen sein können, insbesondere dann, wenn der Gemeinderat eine Fragestunde oder eine Anhörung nach § 44 Abs. 3, 4 SächsGemO beschließt. Das führt zum Teil zu der inkonsequenten Tendenz, im Internet veröffentlichte Fassungen der Niederschriften vorher noch einmal zu überarbeiten, um sie „internetfähig“ zu machen.

Der Gesetzgeber hat dem Wortlaut nach in § 40 Abs. 2 Satz 5 SächsGemO geregelt, dass den *Einwohnern* (und nur diesen) eine Einsichtnahme in die Niederschriften der öffentlichen Sitzungen zu gewähren ist. Eine weltweite Veröffentlichung über das Internet ist damit nicht intendiert gewesen.

Während verschiedene Kommentatoren der Gemeindeordnung (u. a. Menke/Arens Gemeindeordnung für den Freistaat Sachsen, 4. Aufl. - § 40 Rdnr. 3) meine Auffassung teilen, sieht die oberste Kommunalaufsichtsbehörde bisher keinen Anlass, gegen eine Veröffentlichung von Niederschriften von öffentlichen Gemeinderatssitzungen über das Internet aufsichtlich vorzugehen. Um den Gemeinden die erforderliche Rechtssicherheit in der Auslegung der Gemeindeordnung und dem Schutz personenbezogener Daten zu verschaffen, halte ich eine solche Äußerung für geboten. Oder der Gesetzgeber schafft Klarheit.

5.5.3 Akteneinsichtnahmeverfahren bei Kommunen

Immer wieder werde ich von Gemeinden um Auskunft zur Verfahrensweise zum Schutz personenbezogener Daten Betroffener oder Dritter bei Akteneinsichtsbegehren gebeten. Häufig handelt es sich um Einsichtnahmeersuchen bei denen die Behörden unsicher sind, ob und inwieweit eine von einem Anzeigeerstatter gewünschte und bei Anzeigeerstattung evtl. zugesicherte Vertraulichkeit gegenüber einer von einem Verwaltungsverfahren betroffenen Person oder ihres Rechtsvertreters zu beachten ist.

Gegenüber dem Sächsischen Datenschutzgesetz speziellere Rechtsgrundlage für die begehrte Akteneinsicht im Verwaltungsverfahren ist § 29 VwVfG (auch andere besondere Einsichtnahmevorschriften gehen der auffanggesetzlichen Vorschrift in § 18 SächsDSG vor). Eine Behörde ist nach § 29 Abs. 2 VwVfG zur Gestattung der Akteneinsicht nicht verpflichtet, soweit die Vorgänge ihrem Wesen nach, namentlich wegen der berechtigten Interessen der Beteiligten oder Dritter geheim gehalten werden müssen. Dabei ist anerkannt, dass die Bekanntgabe des Namens von Behördeninformanten auch im Wege der Akteneinsicht unterbleiben muss, wenn dieser die Behörde nicht bewusst wahrheitswidrig oder in sonst unbilliger Weise über Rechtsverstöße unterrichtet hat (Schoenemann DVBl. 1988, 523; vgl. auch 9/10.2.10). Schutzwürdig sind grundsätzlich auch vertrauliche Auskünfte, die aufgrund des Vertrauens darauf, dass sie vertraulich bleiben, gegeben wurden (vgl. Kopp VwVfG, 6. Aufl. § 29 Rdnr. 26). Ein überwiegendes Interesse des Informanten steht einer unbeschränkten Einsichtnahme des Betroffenen auch dann entgegen, wenn zu befürchten ist, dass der Einsichtsbegehrende in unerlaubter Weise - etwa tätlich - gegen den Informanten vorgeht (vgl. Obermayer VwVfG, 3. Aufl. § 29 Rdnr. 44).

Auch nach § 18 Abs. 5 Nr. 3 SächsDSG muss eine Auskunftserteilung unterbleiben, wenn berechtigte Interessen eines Dritten überwiegen und deswegen das Interesse des Betroffenen an der Auskunftserteilung zurücktreten muss. Die vorzunehmende Abwägung durch die Behörde ist dem Wortlaut nach schon im Gesetz verankert. Das berechtigte Interesse umfasst auch ein wirtschaftliches oder ideelles. Dem Gesetzeszweck nach hat die Behörde eine bestmögliche Auskunft bzw. Einsichtnahme zu gewährleisten. Soweit eine Akteneinsichtnahme in Vorgänge, bei denen die Interessen Dritter überwiegen, gewährt werden soll, wären die personenbezogenen Daten, die den Dritten erkennen lassen, unkenntlich zu machen. Entscheidungen über Akteneinsichtnahmen nach Verwaltungsverfahrensgesetz oder dem Sächsischen Datenschutzgesetz sind immer Einzelentscheidungen, die als Verwaltungsakt gegenüber dem Antragsteller ergehen. Zu grundsätzlichen Fragen der Auskunft und der Akteneinsicht vgl. auch 12/5.14.2 und 13/10.2.18.

5.5.4 Beschlussvorlagen für den Gemeinderat und Verpflichtung der Gemeinderäte auf das Datengeheimnis

Regelmäßige Nachfragen erhalte ich von Gemeinden wegen des Schutzes personenbezogener Daten in Beschlussvorlagen für nicht-öffentliche und öffentliche Sitzungen des Gemeinderats und seiner Ausschüsse.

Nach § 36 Abs. 3 Satz 1 SächsGemO beruft der Bürgermeister den Gemeinderat schriftlich ein und teilt rechtzeitig die Verhandlungsgegenstände unter Beifügung der Beratungsunterlagen mit, soweit nicht das öffentliche Wohl oder berechtigte Interessen Einzelner entgegenstehen. Der gesetzliche Vorbehalt für die berechtigten Interessen Einzelner trägt dem Grundrecht auf informationelle Selbstbestimmung Rechnung.

Wesentlich für die Entscheidung, ob personenbezogene Daten durch den Bürgermeister in Beratungsunterlagen (bei nicht vorher eingeholter schriftlicher Einwilligung der Betroffenen) weitergegeben werden können, ist, dass diese für die Entscheidungsfindung tatsächlich erforderlich sind. Die Zulässigkeit kann nur anhand des konkreten Einzelfalls beurteilt werden. Grundsätzlich gilt das Prinzip der Datensparsamkeit.

Beispielsweise kann sich eine stufenweise Vorgehensweise dahingehend anbieten, dass bei einer Vorlage, die sich auf personenbezogene Daten mehrerer Betroffener bezieht - z. B. eine zusammenfassende Anlage mit pseudonymisierten, aber noch personenbezogenen Angaben der Betroffenen zur Beschlussvorlage zunächst - in eine nicht-öffentliche Sitzung des zuständigen Ausschusses gegeben wird. Erst bei konkreten Nachfragen von Gemeinderäten wären einzelne Namen der Betroffenen in nicht-öffentlicher Sitzung zu nennen. Soweit in nicht-öffentlicher Sitzung Vorlagen mit zu schützenden personenbezogenen Daten von Betroffenen ausgereicht werden sollen, empfiehlt es sich, diese aus Datenschutzgründen nach Sitzungsende wieder einzuziehen. Darüber hinaus empfiehlt es sich, die Sitzungsteilnehmer vor Sitzungsbeginn auf ihre Verschwiegenheitspflicht gemäß § 19 Abs. 2 i. V. m. § 35 Abs. 1 SächsGemO hinzuweisen und in diesem Zusammenhang - soweit noch nicht geschehen - auf eine Verpflichtung der Gemeinderäte auf das Datengeheimnis nach § 6 SächsDSG hinzuwirken. Die allgemeine Amtsverschwiegenheit oder Verschwiegenheitspflichten nach den kommunalrechtlichen Vorschriften, die sich primär auf unbefugte Weitergaben richten - während das Datengeheimnis jegliche unbefugte Verarbeitung erfasst - sind nämlich aliud-Vorschriften und daher nicht spezieller, wie z. B. die Verpflichtung von Bediensteten auf das Meldegeheimnis nach § 9 SächsMG. Bei der Verpflichtung der Mandatsträger in kommunalen Vertretungskörperschaften werde ich dennoch bisher nicht von der obersten Kommunalaufsichtsbehörde unterstützt. Dabei ist die Verpflichtung auf das Datengeheimnis als individuelle Konkretisierung des öffentlich-rechtlichen Mandatsträgerver-

hältnisses zur Begründung der *individuellen* Pflicht zum rechtmäßigen Umgang mit personenbezogenen Daten in allen sächsischen Kommunen erforderlich (vgl. auch 13/5.5.3 - am Ende).

5.5.5 Öffentlich-rechtliches Forderungsmanagement im Auftrag von Gemeinden und anderer öffentlich-rechtlicher Stellen

In zurückliegenden Berichtszeiträumen hatte ich mich bereits zur Beauftragung von Privatunternehmen durch sächsische öffentliche Stellen, insbesondere Gemeinden, zur Beitreibung privatrechtlicher und öffentlich-rechtlicher Forderungen und zur Vorbereitung von Vollstreckungsmaßnahmen geäußert, 6/5.5.6 und 7/5.5.9. Im letzten Berichtszeitraum war die Thematik erneut aktuell geworden. Die Lage öffentlicher zu sanierender Haushalte, mit z. T. nicht unerheblichen noch nicht eingebrachten Außenständen führte erneut zu entsprechenden Anfragen, ob derartige Auftragsvergaben datenschutzrechtlich zulässig seien.

In der Vergangenheit vertrat ich eine restriktive Auffassung, was die Auftragsvergabe an private Inkassounternehmen betraf. Schon gestützt auf § 30 VwVfG, wonach die Beteiligten in einem Verwaltungsverfahren grundsätzlich Anspruch darauf haben, dass ihre Geheimnisse, insbesondere die zum persönlichen Lebensbereich gehörenden Geheimnisse sowie die Betriebs- und Geschäftsgeheimnisse, von der Behörde nicht unbefugt offenbart werden, sah ich die Rechtmäßigkeit derartiger Beauftragungen in Frage gestellt.

Nach § 87 SächsGemO sind Gemeinden auf der anderen Seite auch grundsätzlich befugt, die Kassengeschäfte ganz oder zum Teil von Stellen außerhalb der Gemeindeverwaltung besorgen zu lassen, wenn die ordnungsgemäße und sichere Erledigung und die Prüfung nach den für die Gemeinde geltenden Vorschriften gewährleistet sind. Nach dem Inkrafttreten der letzten Änderungen des Sächsischen Datenschutzgesetzes am 1. Januar 2007 gilt es zudem, die anderslautenden Bestimmungen zur Auftragsdatenverarbeitung zu untersuchen. Nach alledem ergibt sich ein differenzierteres Bild. Danach kann sich durchaus eine Befugnis für eine entsprechende Offenbarung von Daten aus Verwaltungsverfahren aus § 7 SächsDSG in Verbindung mit einem entsprechenden Auftrag ergeben.

Nach wie vor vertrete ich allerdings die Auffassung, dass Vollstreckungen nach dem Sächsischen Verwaltungsvollstreckungsgesetz zum Kernbereich hoheitsrechtlicher Verwaltung gehören und nicht auf private Inkassobüros übertragen werden können. Repression ist ausschließlich staatliche Aufgabe; sie kann ohne klare gesetzliche Vorschrift nicht auf Private übertragen werden. Ferner sind die Grenzen im Sozialleis-

tungsbereich gemäß § 80 SGB X zu beachten. Auch bei dem Steuergeheimnis nach § 30 AO unterliegenden Angaben ergibt sich aus Art. 108 GG und §§ 2, 17 Abs. 3 FVG, dass die Verarbeitung entsprechender Daten als integraler Bestandteil hoheitlicher Aufgabenerfüllung anzusehen ist und daher nur von öffentlichen Stellen erfolgen kann.

Im Übrigen ist zu beachten, dass sich die Befugnis eines als Auftragnehmer tätigen Inkassounternehmens, Daten zu verarbeiten, von denen des Auftraggebers ableitet. Der Auftragnehmer hat also nicht mehr Möglichkeiten zur Datenverarbeitung als die ihn beauftragende Kommune. Das bedeutet insbesondere, dass eine Verwendung von bereits vorliegenden Adress- oder gar Bonitätsinformationen unzulässig ist. Vielmehr kann sich das Inkassounternehmen nur aus öffentlichen Registern, wie beispielsweise Melderegistern, Informationen beschaffen. Selbstverständlich dürfen die Daten aus der öffentlich-rechtlichen Auftragsdatenverarbeitung auch nicht zur Validierung des Datenbestandes des Inkassounternehmens verwendet werden. Den technisch-organisatorischen Maßnahmen des Auftragnehmers gemäß § 9 SächsDSG, eine unüberwindbare Trennung von Datenbeständen und Organisationseinheiten sicherzustellen, ist seitens des Auftraggebers besondere Aufmerksamkeit zu widmen, sind doch die Geschäftsabläufe auch seriöser Inkassounternehmen beim Forderungsmanagement auch deshalb so erfolgreich, da Datenbestände optimiert verknüpft werden.

Rechtlich ist darüber hinaus zu beachten, dass bei einer Datenverarbeitung im Auftrag die Auftragnehmer keine eigenen Entscheidungsbefugnisse haben dürfen. Anderenfalls würde es sich rechtlich nicht mehr nur um eine Auftragsdatenverarbeitung, sondern um eine Funktionsübertragung und damit um Übermittlungen gemäß § 16 SächsDSG handeln, die wegen des Fehlens einer Erforderlichkeit regelmäßig unzulässig wären. Der Auftragnehmer kann daher beispielsweise nicht selbständig Ratenzahlungen gemäß § 34 KomHVO mit dem Schuldner vereinbaren. Dies kann nur entweder jeweils nach Rücksprache mit dem Auftragnehmer oder durch die Vorgabe eines sog. *Entscheidungsbaumes*, bei dem alle möglichen Entscheidungen durch bestimmte Entscheidungsregeln vorweggenommen sind, erfolgen, was in der Praxis eine nicht unerhebliche Schwierigkeit darstellt.

Nach alledem relativieren sich die Vorteile einer Auftragsvergabe an private Inkassounternehmen durchaus. Sie ist aber nach den Regeln der Auftragsdatenverarbeitung nach § 7 SächsDSG durchaus zulässig. Auch unterliegen privatrechtliche Forderungen der kommunalen Gebietskörperschaften hinsichtlich ihres Einzugs durch Dritte nicht den strengen Restriktionen wie bei öffentlich-rechtlichen Geldforderungen. Bei der Entscheidungsfindung sollten zuvor aber - zumindest auf kommunaler Ebene - auch die rechtlichen Möglichkeiten einer Zusammenarbeit, z. B. durch Zweckverbände geprüft werden. Hier sehe ich noch nicht häufig genutzte Gestaltungsspielräume. Kommunale

Zweckverbände sind als öffentliche Stellen datenschutzrechtlich befugt, weitergehende Aufgaben (und Datenverarbeitung) zu übernehmen als ein Auftragnehmer, der nach den Regeln der Auftragsdatenverarbeitung gesetzlich auf unterstützende Hilfsdienstleistungen beschränkt ist.

Letztendlich vertrete ich weiterhin die Meinung, dass die sächsischen Kommunalbehörden in der Lage sind, öffentlich-rechtliche Forderungen selbst zu vollstrecken oder durch eine leistungsstarke und sachkundige Vollstreckungsbehörde vollstrecken zu lassen, vgl. 6/5.5.6 und 7/5.5.9 und auch die Ausführungen von Härig, Sachsenlandkurier 2008, 345 ff.

5.5.6 Informationelle Gewaltenteilung in der Gemeinde - Geschäftsabläufe

Ich erhielt eine Anfrage einer Gemeindeverwaltung, ob die an die Meldebehörde gerichtete Post vom Sekretariat der Gemeindeverwaltung zur Registrierung geöffnet werden darf und der Postausgang der Meldebehörde über das Sekretariat erfolgen dürfe. Einsicht in die Post - so die Gemeinde - werde nur dem Bürgermeister und einer Sachbearbeiterin gewährt. Anfragen dieser Art, wie die Geschäftsabläufe datenschutzgerecht zu gestalten sind, erhalte ich häufig.

Meldedaten unterliegen dem Meldegeheimnis, § 9 SächsMG. Für die Daten besteht also ein besonders geregeltes, gesetzlich zu beachtendes Geheimnis. Die Daten sind abgeschottet von anderen Organisationseinheiten der Gemeinde aufzubewahren.

Als besonders sensibel sind die Daten zu betrachten, zu denen Auskunftssperren bestehen. Meldebehörden sind befugt, personenbezogene Daten zu verarbeiten, soweit das ein Gesetz oder eine andere Rechtsvorschrift erlaubt oder der Betroffene eingewilligt hat. Es ist daher Aufgabe der Meldebehörde, Meldedaten zu verarbeiten (§ 4 Abs. 1 SächsMG). Zwar ist die Gemeinde Meldebehörde. Wegen des Datengeheimnisses bleibt es aber Aufgabe der konkret hierauf verpflichteten Amtsträger, Meldedaten zu verarbeiten. Der Bürgermeister oder seine Sekretärin gehören nicht dazu.

Aber bereits unabhängig davon ist eine informationelle Gewaltenteilung auch innerhalb der Gemeinde zu praktizieren. In einer Entscheidung von 1987 hat das Bundesverfassungsgericht auf die Pflicht, dass die verschiedenen Stellen innerhalb der Gemeinde ihre Daten voreinander schützen müssen, hingewiesen (Beschluss vom 18. Dezember 1987, 1 BvR 962/87). Das gilt auch für Untereinheiten innerhalb der Gemeindeverwaltung als Bündelungsbehörde. Die funktionalen Stellen in der Gemeinde sind so zu organisieren, dass der informationelle Austausch zwischen den Organisationseinheiten möglichst gering bleibt. Selbst Vorgesetzte haben nicht die unbesehene Befugnis in alles Einblick zu nehmen. Das gilt ganz besonders für die Meldedaten. Vorgesetzte sind

nur befugt soweit teilzuhaben, wie das zur Wahrung ihrer Vorgesetztenfunktion notwendig ist. Das kann jedenfalls nicht bedeuten, dass sie grundsätzlich die gesamte einem besonderen gesetzlichen Schutz anheimfallende Post, die an das Meldeamt gerichtet ist, sichten. Anfragen an die Meldebehörde sind grundsätzlich durch die Meldebehörde zu beantworten. Ebenso ist der Postausgang nicht in Bezug auf seinen Inhalt grundsätzlich durch andere Bedienstete einzusehen.

Für vergleichbare Bereiche, wie z. B. die Standesämter der Gemeinden, gilt Entsprechendes.

5.6 Baurecht; Wohnungswesen

In diesem Jahr nicht belegt.

5.7 Statistikwesen

5.7.1 Schülerregister-Vorhaben der Kultusministerkonferenz

Seit meinem letzten Bericht zu den Bestrebungen der Kultusministerkonferenz, landesweite und zusätzlich sogar ein bundesweites (pseudonymisiertes) Schüler- und Lehrerregister zu schaffen (13/5.7.1) hat die KMK im Juli 2008 ein überarbeitetes - nicht mehr als zwei DIN A4-Seiten umfassendes - „Konzept für die Nutzung der schulstatistischen Einzeldaten“ vorgelegt. Dieses ist von allen Landesdatenschutzbeauftragten mit Ausnahme Thüringens in einer gemeinsamen - nicht ganz so knapp gehaltenen – Stellungnahme abgelehnt worden. Die KMK ist daraufhin bisher nicht mehr an die Landesdatenschutzbeauftragten mit neuen Vorstellungen herangetreten.

Für Sachsen bin ich weiterhin zuversichtlich, dass das SMK sich, auch angesichts der Spitzenplätze Sachsens bei der letzten PISA-Untersuchung, nicht von der Erkenntnis abbringen lassen wird, dass für die Bildungspolitik wirklich nützliche Erkenntnisse nur aus unvergleichlich genaueren und reichhaltigeren und damit zugleich natürlich nur für eine äußerst beschränkte Stichprobe erhobenen Daten gewonnen werden können: Im Rahmen von Forschungsvorhaben, in denen es um die konkrete Gestaltung des Bildungswesens geht, statt um riesige Register. So lässt das SMWK für die Jahre 2008 bis 2011 durch das Max-Planck-Institut für Bildungsforschung (Berlin) „Entwicklungsverläufe an Haupt- und Realschulen in Baden-Württemberg und Mittelschulen in Sachsen“ untersuchen, und außerdem werden unter Beteiligung des Zentrums für Neurowissenschaften und Lernen der Universität Ulm 1.400 Kinder im Alter zwischen drei und zwölf Jahren, wie man der Presse im Oktober 2009 hat entnehmen können, im Lernalltag genau beobachtet, um herauszufinden, wie ein „optimaler Bildungstag“ aussehen kann (Forschungsvorhaben „FOKUS Kind“).

Angesichts der Forderungen nach unabhängiger statt durch die Kultusbürokratie beeinflusster Bildungsforschung, wie bei den Vorbildern Finnland und Kanada, (Schmoll FAZ 8. Dezember 2007, ähnlich Wolfgang Nowak SPIEGEL 24. November 2008) und der Auffassung der Bildungsforschung, dass es darauf ankommt, einzelne Unterrichtsformen und deren Erfolg zu untersuchen, (Schmoll FAZ 21. Oktober 2008) sowie der bei der KMK festzustellenden Scheu, die Erkenntnismöglichkeiten, die die PISA-Untersuchungen bieten, ländervergleichend auszuschöpfen (Tenorth FAZ 16. Dezember 2008) oder des dort festzustellenden Widerstandes gegen Leistungsvergleiche unter den Bundesländern (FAZ 9. Dezember 2008) ist die *Nützlichkeit* des bisher von der KMK-Mehrheit verfolgten Vorhabens einer Totalerhebung auch bei großem Wohlwollen nicht zu erkennen.

5.7.2 Fünfjährige Stichprobenzugehörigkeit bei der Dienstleistungsstatistik

Jemand, der zur Auskunftserteilung für die Dienstleistungsstatistik (nach dem Dienstleistungsstatistikgesetz des Bundes, DlStatG vom 19. Dezember 2000, BGBl. S. 1765; vgl. zur Dienstleistungsstatistik auch 12/5.7.8) herangezogen worden war, beschwerte sich, weil dies nunmehr schon im dritten Jahr in Folge geschehen war. Er meinte, dies sei deswegen verfassungswidrig, weil es zu einem „lückenlosen Datensatz“ für die drei Jahr führe, auf den der Staat kein Recht habe, zumal die von ihm zu erteilenden Auskünfte weitgehend dem entsprächen, wozu man sich auch in der Einkommenssteuererklärung gegenüber dem Finanzamt äußern müsse. Auch leuchtete ihm die vom StaLA (vorsorglich) gegebene Begründung dafür, dass er weiterhin in die zur Auskunft herangezogene Stichprobe falle („ausgewählter Berichtskreis“ in der Sprache der Statistiker), nicht ein, weil die Behörde doch methodisch und daher auch rechtlich richtig jeweils eine neue zufällige Stichprobe ziehen müsse.

Wie sich ergeben hat, ist das Verfahren des StaLA bei der Auswahl der auskunftspflichtigen Erhebungseinheiten für die Durchführung der Dienstleistungsstatistik des betreffenden Jahres, nämlich Beibehaltung des bereits ausgewählten Berichtskreises unter Erweiterung lediglich um eine Ergänzungsstichprobe, datenschutzrechtlich nicht zu beanstanden gewesen:

Der für die Dienstleistungsstatistik in § 1 Abs. 2 DlStatG vorgegebenen Beschränkung auf eine (bundesweit betrachtet 15%ige) Stichprobenerhebung läuft es nicht zuwider, wenn es zu einer mehrjährigen, hier fünfjährigen, Mehrfachverwendung der ordnungsgemäß gezogenen Stichprobe kommt: Das gilt jedenfalls dann, wenn die Stichprobe wie im vorliegenden Fall ergänzt wird durch jährliche (naturgemäß ebenfalls 15%ige) Ergänzungsstichprobe aus den seit der Ziehung der Erst-Stichprobe zu verzeichnenden Neuzugängen zur sog. Grundgesamtheit, also der Gesamtzahl der unter das betreffende

Statistikgesetz fallenden Dienstleistungsunternehmen. Denn auf diese Weise wird gewährleistet, dass die Stichprobe weiterhin repräsentativ und die Datenerhebung somit in dieser Hinsicht unverändert *geeignet* (und deswegen nicht wegen mangelnder Geeignetheit rechtswidrig) ist.

Die nach Auskunft des StaLA für den Dienstleistungsbereich erfolgende fünfjährige Verwendung einer Stichprobe dient insbesondere dem Ziel, Entwicklungen, also wirtschaftliche Veränderungen, über einen längeren Zeitraum hinweg ohne Beeinflussung durch einen eventuellen Stichprobenfehler - der bei der Neuziehung einer Stichprobe eben nicht vollständig ausgeschlossen ist - beobachten zu können, also ohne Beeinflussung durch strukturelle Abweichungen zwischen alter und neuer Stichprobe.

Datenschutzrechtliche Einwände hiergegen, einschließlich solcher verfassungsrechtlicher Art, sind nicht zu erkennen. Der Umstand, dass die betreffenden Daten nicht nur eine einmalige Momentaufnahme, sondern am Ende ein Entwicklungsbild über fünf Jahre darstellen, ist von der gesetzlichen Ermächtigung noch gedeckt und nähert sich noch nicht einem von der Verfassung verbotenen (eben umfassenden) Persönlichkeitsprofil. Der fünfjährige Fortbestand einer Stichprobe ist auch keine Besonderheit nur der Dienstleistungsstatistik.

Von der Wahrung des Statistikgeheimnisses gerade auch gegenüber dem Finanzamt kann jeder nach den jahrzehntelangen Erfahrungen mit der tatsächlichen Einhaltung des Statistikgeheimnisses als sicher ausgehen.

5.7.3 „Sprechende“ Nummern-Angaben auf Erhebungsbögen

Bei einem zum Mikrozensus herangezogenen Petenten hatte es Misstrauen erweckt, dass die von ihm ausgefüllt abzugebenden Unterlagen mit einer *Auswahlbezirks-Nummer* und einer *laufenden Nummer des Haushaltes im Auswahlbezirk* gekennzeichnet waren.

Dieses Misstrauen war gut nachvollziehbar, der Sachverhalt recht verwickelt, aber nach genauer Prüfung, zu der auch eine Rücksprache des StaLA mit Fachleuten des Statistischen Bundesamtes gehört hat, hat sich die festgestellte Praxis als zulässig erwiesen:

(1) Die beiden genannten Nummern, also die „Auswahlbezirks-Nummer“ und die „laufende Nummer des Haushalts im Auswahlbezirk“, sind, nachdem zunächst die Inhalte der Erhebungsbögen auf maschinell verwertbaren Datenträger eingegeben worden und die Bögen selbst vernichtet worden sind, Bestandteil sowohl einer sog. *Organisationsdatei* als auch Bestandteil der *Erhebungsdaten-Datei* (mit den sog. *Interviewdaten-*

sätzen). In der Organisationsdatei sind der Verbindung von „Auswahlbezirks-Nummer“ und „laufender Nummer des Haushalts im Auswahlbezirk“ die Hilfsmerkmale „Name“ und „Anschrift“ zugeordnet.

(2) Damit ist die Kombination von Auswahlbezirks-Nummer und laufender Nummer des Haushalts im Auswahlbezirk - als „Pseudonym“ im datenschutzrechtlichen Sinne - Verbindungsglied, und zwar das einzige Verbindungsglied, zwischen den Hilfsmerkmalen, nämlich „Name“ und „Anschrift“, und den zu den betreffenden Hilfsmerkmalen jeweils gehörenden eigentlichen Erhebungsdaten.

(3) Die *Auswahlbezirke* sind die sog. *Klumpen*, die bei der Ziehung der Stichprobe aus einer (bloßen) Anschriften-Datei ausgewählt werden (vgl. dazu ausführlich 9/5.7.1); die dafür vergebene Nummer ist im ganzen Erhebungsgebiet, also der Bundesrepublik Deutschland, einmalig. Die dazugehörige *Haushaltsnummer* vergibt der Erhebungsbeauftragte. (Mindestens sechs bis höchstens 13 Haushalte; wegen der Möglichkeit, dass nach einem Wegzug innerhalb des Vier-Jahres-Turnus der Wohnungsnachfolger die Befragungsbeteiligung „erbt“, kann die Zahl steigen.)

(4) Damit kann das StaLA aus der Auswahlbezirksnummer durchaus erkennen, aus welchem engeren Wohngebiet der Vordruck stammt. Denn mithilfe der bei der Behörde vorhandenen Auswahlbezirks-Nummern-Liste kann die jeweilige Anschrift bzw. der jeweilige Anschriften-Bereich zu der Auswahlbezirks-Nummer festgestellt werden.

(5) Das StaLA verfremdet vor der Lieferung der Datensätze an das Statistische Bundesamt (das hat jeweils spätestens sechs Wochen nach Quartalsende zu erfolgen) die zum Datensatz gehörende Auswahlbezirks-Nummer in einer für das Statistische Bundesamt nicht zurückverfolgbaren Weise.

(6) Nach Abschluss der vierjährigen Befragungsperiode wird der sich auf den betreffenden Haushalt beziehende Teil der Organisationseinheit, also der Datensatz, in dem den Nummern die Hilfsmerkmale des betreffenden Haushaltes (Name, Anschrift) zugeordnet werden, gelöscht.

Zusätzlich wird in den vier zusammengehörenden sich auf ein und denselben Haushalt beziehenden Erhebungsmerkmal-Dateien die Auswahlbezirks-Nummer und die Haushaltsnummer im Auswahlbezirk, also das diesen (vierteiligen) Gesamt-Datensatz kennzeichnende Pseudonym, programmgesteuert in nicht rückverfolgbarer Weise durch ein neues Pseudonym ersetzt.

(7) Damit wird genau § 12 BStatG eingehalten, genauer gesagt § 12 Abs. 1 Satz 2 und Abs. 2 Satz 1 und 2 BStatG. Diese Vorschrift lautet folgendermaßen:

Hilfsmerkmale sind, […soweit bestimmte Rechtsvorschriften nichts anderes bestimmen …] zu löschen, sobald bei den Statistischen Ämtern die Überprüfung der Erhebungs- und Hilfsmerkmale auf ihre Schlüssigkeit und Vollständigkeit abgeschlossen ist. Sie sind von dem Erhebungsmerkmal zum frühestmöglichen Zeitpunkt zu trennen und gesondert aufzubewahren.
Bei periodischen Erhebungen für Zwecke der Bundesstatistik dürfen die zur Bestimmung des Kreises der zu Befragenden erforderlichen Hilfsmerkmale, soweit sie für nachfolgende Erhebungen benötigt werden, gesondert aufbewahrt werden. Nach Beendigung des Zeitraumes der wiederkehrenden Erhebung sind sie zu löschen.

Die Verwendung der den Personenbezug als pseudonymes Bindeglied zwischen Hilfs- und Erhebungsmerkmalen schaffenden (und überdies auch unabhängig davon aufgrund der festen Zuordnung von Auswahlbezirks-Nummern und Anschriftenbereichen für das StaLA als Ganzes das Herstellen eines Personenbezuges ermöglichenden) Auswahlbezirksnummer, kombiniert mit der dazugehörigen Haushaltsnummer, ist von § 12 BStatG bis zu dem Zeitpunkt des § 12 Abs. 2 Satz 2 BStatG gedeckt: *Vor* diesem Zeitpunkt ist sie erforderlich, um die bei der gebotenen getrennten Aufbewahrung von Hilfs- und Erhebungsmerkmalen im Bedarfsfalle nötige Verbindung herzustellen, ferner auch dafür, den Zusammenhang der vier zueinander gehörenden Befragungsergebnisse (§ 12 Abs. 2 Satz 1 BStatG) zu gewährleisten.

Nach Ausscheiden der betreffenden Erhebungseinheit (Haushalt) aus der Befragung entfällt durch die nicht rückverfolgbare Ersetzung von Auswahlbezirks- und Haushaltsnummer durch ein anderes Pseudonym jede einen Personenbezug noch ermöglichende Wirkung des dann noch vorhandenen Pseudonyms: Dieses hat dann nurmehr die Funktion eines Kennzeichens, das die Unterscheidung der betreffenden Datensätze von anderen Datensätzen ermöglicht.

Die Tatsache, dass die beiden Nummern nicht im Mikrozensusgesetz erwähnt sind, begründet keine Rechtswidrigkeit ihrer Verwendung. Das folgt aus § 9 Abs. 2 BStatG, wonach laufende Nummern und Ordnungsnummern zur Durchführung von Bundesstatistiken einer Bestimmung in der eine einzelne Bundesstatistik (hier: Mikrozensus) anordnenden Rechtsvorschrift nur insoweit bedürfen, als sie Angaben über persönliche oder sachliche Verhältnisse enthalten, die über die Erhebungs- und Hilfsmerkmale hinausgehen - was ja bei der Auswahlbezirks-Nummer und der laufenden Nummer des Haushaltes im Auswahlbezirk nicht der Fall ist, da diese ja nur die Anschrift und damit ein Hilfsmerkmal enthalten.

5.7.4 Statistikrechtliche Grenzen einer zugunsten der Beantwortung parlamentarischer Anfragen stattfindenden Verarbeitung personenbezogener Daten

Mit der Kleinen Anfrage 4/12825 hat nach der Wahl neuer Kreistage im Juni 2008 ein Abgeordneter Anfang Juli 2008 von der Staatsregierung Angaben zur sozialen Zusammensetzung der zehn neugewählten Kreistage bekommen wollen. Je Kreistag hat er wissen wollen, wie viele Kreistagsmitglieder jeweils

- kommunale Wahlbeamte
- sonstige Beamte oder Angestellte im öffentlichen Dienst
- selbständige Unternehmer oder Gewerbetreibende
- freiberuflich Tätige
- unselbständig beschäftigte außerhalb des öffentlichen Dienstes oder aber
- sonstige wie z. B. Studenten, Rentner oder Arbeitsuchende

seien. Mit Schreiben vom 4. September 2008 hat der Sächsische Staatsminister des Innern diese Kleine Anfrage durch Vorlage einer entsprechenden Tabelle beantwortet und im Hinblick auf die ersichtlich unvollständigen Angaben eines LRA angegeben, dass sie das Ergebnis einer anonymen Befragung der Kreisratsmitglieder in der konstituierenden Sitzung des Kreistages am 27. August 2008 gewesen seien.

Weil in dem betreffenden einen LRA - lobenswerterweise! - datenschutzrechtliche Bedenken bestanden hatten, hatte man eine solche Befragung mittels anonymer Ankreuz-Möglichkeit ohne Auskunftspflicht, also auf erklärtermaßen freiwilliger Grundlage, durchgeführt, nur 27 von 98 Kreisräten hatten sich beteiligt, und das LRA hatte den „Unmut“ des RP (jetzt Landesdirektion) zu spüren bekommen, welches das Datenverlangen des SMI an das LRA weitergegeben hatte.

Höchstverständlich, dass nunmehr die Datenschutzbeauftragte des LRA von mir wissen wollte, was in diesem Falle die rechtmäßige Verhaltensweise gewesen war oder gewesen wäre.

Nach Prüfung der Angelegenheit habe ich der SK und außerdem dem SMI als in der Angelegenheit tätig gewordener Stelle wie auch wegen dessen Zuständigkeit für Statistikrecht Folgendes geschrieben:

Zu dem Zweck, dem SMI die Beantwortung der Kleinen Anfrage LT-DS-Nr.: 4/12825 zu ermöglichen, sind offensichtlich in allen (neuen) Landkreisen bis auf den Landkreis X durch die LRA personenbezogene Daten von Kreistags-Mitgliedern erhoben worden, die unabhängig von dieser Anfrage den für die Durchführung des Kommunalwahl-

gesetzes und die Verwaltung der Kreistags-Mandate zuständigen Stellen nicht zur Verfügung gestanden haben.

Die Antwort der Staatsregierung auf die o. g. Kleine Anfrage lässt darauf schließen, dass außer im Falle des Landkreises X die betreffende Datenerhebung nicht anonym durchgeführt worden ist.

Diesen Sachverhalt habe ich wie folgt bewertet:

(1) Die Pflicht der Staatsregierung, gemäß Art. 51 Abs. 1 Satz 1 SächsVerf parlamentarische Anfragen *nach bestem Wissen zu beantworten*, begründet, für sich genommen, noch keine Rechtsgrundlage für die Erhebung personenbezogener Daten. Mit anderen Worten: Die Staatsregierung darf *nur* mitteilen, was sie ohnehin schon weiß, d. h. was an personenbezogenen Daten bei ihr oder bei den ihrer Aufsicht unterstehenden Stellen der Exekutive aus dem normalen Verwaltungsvollzug vorhanden ist. Aus dem Verwaltungsvollzug vorhanden gewesen sind im vorliegenden Falle die Angaben nach § 16 Abs. 1 und 2 KomWO, nämlich aus der Durchführung des Kommunalwahlgesetzes.

Diese Daten durften datenschutzrechtlich gesehen auf der Rechtsgrundlage des § 7 Abs. 1 SächsStatG durch die Wahlbehörde des LRA zur Erstellung einer Statistik gemäß den in der Frage enthaltenen Merkmalen genutzt werden. Denn aus der genannten verfassungsrechtlichen Pflicht der Staatsregierung folgte die Aufgabe des für die Kommunalaufsicht zuständigen SMI und daraus die Aufgabe des unterhalb dessen die Kommunalaufsicht ausübenden RP als dem LRA übergeordneter Behörde, die entsprechenden Angaben zu sammeln, sofern sie bei der Stelle, von der sie möglicherweise beschafft werden konnten, also eben dem LRA als Kommunalwahlbehörde, aus der Durchführung des Kommunalwahlgesetzes vorhanden waren.

Für die Durchführung derartiger *Statistiken im Verwaltungsvollzug* nach § 7 Abs. 1 SächStatG bedarf es keiner zusätzlichen Rechtsgrundlage, insbesondere keiner kommunalen Statistiksatzung und auch keiner kommunalen Statistikstelle. Diese letzteren Anforderungen bestehen nur im Hinblick auf Primärstatistiken, nicht im Hinblick auf die statistische Nutzung von Daten, die zu nichtstatistischen Zwecken im Verwaltungsvollzug angefallen sind, eben die sogenannten Statistiken im Verwaltungsvollzug.

Die LRA haben also die Angaben, welche für die gewählten Kreisräte nach § 16 Abs. 1 und 2 Satz 1 KomWO erhoben worden sind, für die Beantwortung der Kleinen Anfrage nutzen dürfen. Die auf dieser Grundlage vorliegenden Daten haben sich jedoch nicht den in der Kleinen Anfrage genannten Merkmalen eindeutig zuordnen lassen; so konnte ein Arzt im Sinne von § 16 Abs. 2 Satz 1 KomWO im Sinne der Anfrage Beamter und Angestellter im öffentlichen Dienst, Selbständiger, unselbständig Beschäftigter außer-

halb des öffentlichen Dienstes oder aber auch Arbeitsuchender sein. Die von den LRA über das RP weitergegebenen Daten hätten also nur unter Offenlegung der fehlenden genauen Zuordnungsmöglichkeit beantwortet werden können, die hinsichtlich einiger Berufsbezeichnungen bestanden hat.

(2) Eine Erhebung von Daten - bei den Betroffenen, also den Kreistagsmitgliedern - genau zu dem Zweck der Weitergabe von Daten zwecks Beantwortung der Kleinen Anfrage durch die Staatsregierung hätte bzw. hat keine Rechtsgrundlage gehabt. Das ergibt sich aus Folgendem:

Eine eigene Rechtsgrundlage dafür, etwa im Bereich des Kommunalrechtes und insbesondere des Kommunalwahlrechtes, existiert nicht.

Grundsätzlich in Frage gekommen wäre eine statistikrechtliche Grundlage: Dazu hätte es jedoch, weil es sich um eine Primärstatistik gehandelt hätte, einer Statistiksatzung des Landkreises und der Durchführung durch eine gesonderte Statistikstelle des LRA bedurft.

Eine Pflicht des Landkreises gegenüber dem Freistaat, zu dem Zwecke, diesem die Beantwortung parlamentarischer Anfragen zu ermöglichen, eigens eine Primärstatistik durchzuführen, besteht nicht. Nämlich genauso wenig, wie die Staatsregierung etwa die Pflicht hat, sich die Beantwortung parlamentarischer Anfragen dadurch zu ermöglichen, dass sie einen Regierungsentwurf für ein Landesgesetz über die Durchführung einer diesbezüglichen Landesstatistik vorlegt. Auch kann man § 11 Abs. 1 SächsStatG entnehmen, dass keine Pflicht der Staatsregierung besteht, zugunsten der Beantwortung parlamentarischer Anfragen Landesstatistiken ohne besondere gesetzliche Grundlage anzuordnen - was im Übrigen ohnehin gemäß § 11 Abs. 3 SächsStatG nur ohne Auskunftspflicht und mit einer Stichprobengröße von höchstens 0,5 vom Hundert erlaubt ist.

(3) Schließlich ist auch eine Erhebung auf freiwilliger Grundlage rechtswidrig gewesen: Der Sache nach hat es sich um die Durchführung einer (amtlichen) Statistik gehandelt, nicht um Verwaltungsvollzug und damit die Regelung von Einzelfällen. Daher ist auf diesen Vorgang das Sächsische Statistikgesetz anzuwenden. Dieses gehört, zusammen mit dem Bundesstatistikgesetz, zu denjenigen Statistikgesetzen in Deutschland, die auch für die Erhebung und Weiterverarbeitung personenbezogener Daten zu Statistikzwecken auf freiwilliger Grundlage, also für die Durchführung von Statistiken ohne Auskunftspflicht, eine besondere Rechtsvorschrift zur Voraussetzung machen (§ 11 Abs. 1 SächsStatG).

(4) Unabhängig davon gibt die Antwort der Staatsregierung auf die genannte Kleine Anfrage 4/12825 zusätzlich Anlass zu folgendem Hinweis: Nach einer in der Anwendung des Statistikrechtes unumstrittenen Faustregel verletzt die Angabe von Tabellenfeldwerten, die kleiner als 3 sind, das Statistikgeheimnis, d. h. stellen sie eine Übermittlung personenbezogener Daten dar, sofern, wie hier, unter den Empfängern der betreffenden Zahlenangabe mit Zusatzwissen hinsichtlich der in der Tabelle implizit vorkommenden Personen (Erhebungseinheiten) zu rechnen ist. Die Tabellenfeldwerte 0, 1 und 2 müssen demnach, soweit keine Befugnis zur Übermittlung personenbezogener Daten besteht - was für die Staatsregierung im vorliegenden Falle auch nicht der Fall gewesen ist - durch ein (zu erläuterndes) Stellvertreterkennzeichen, etwa ein „Stern“-Zeichen ersetzt werden.

Aufgrund dessen habe ich die Staatsregierung gebeten, in derartigen Fällen künftig bei Datenanforderungen an der Aufsicht des Freistaates unterstehende Stellen diese ausdrücklich darauf hinzuweisen, dass eine Erhebung (und Weiterverarbeitung) personenbezogener Daten ausschließlich zu dem Zwecke, der Staatsregierung die Beantwortung der parlamentarischen Anfrage zu ermöglichen, nicht zulässig ist, sondern die Daten ausschließlich im Wege der Statistik im Verwaltungsvollzug nach § 7 Abs. 1 SächsStatG gewonnen werden dürfen.

Abschließend habe ich die Adressaten wie üblich gebeten, es mich wissen zu lassen, wenn sie Einwände gegen meine Rechtsauffassung haben sollten. Solche Einwände sind mir gegenüber nicht vorgebracht worden. Dasselbe gilt auch für den Präsidenten des Sächsischen Landtages und damit die Landtagsverwaltung, die ich in der gleichen Weise über die Beschränkungen der Antwortmöglichkeiten der Staatsregierung, die sich aus dem Vorstehenden ergeben, unterrichtet habe.

5.7.5 Bürgerbefragungen ohne Rechtsgrundlage

Die Bürgermeister von Aue, Lößnitz, Schneeberg und Bad Schlema wollten unter Umgehung der Anforderungen an Bürgerentscheide *Bürgerbefragungen* zur Einstellung zu einem Zusammenschluss der vier Gemeinden zur Stadt „Silberstadt“ durchführen. Man hat auch über eine Rechtsgrundlage nachgedacht und das Vorhaben anders als in dem in 4/5.7.6 dargestellten Fall nicht als Statistik auf der Grundlage des Statistikrechtes durchführen wollen, sondern, wie es hieß, „in Anlehnung an §§ 8 und 9 SächsGemO“ zur Vermeidung der Manipulation des Ergebnisses durch Mehrfachbeantwortungen durch ein und dieselbe Person auf auszuteilenden Fragebögen Namen und Anschrift des Befragten erheben wollen, wofür man sich im Hinblick auf § 4 Abs. 1 Nr. 2 SächsDSG die *Einwilligung* als Rechtsgrundlage hatte einfallen lassen. Dabei hat man „in Anlehnung an § 8 Abs. 1 Satz 2 SächsGemO“ auch die 16- und 17-Jährigen einbeziehen wollen.

Keine zwei Wochen vor der geplanten Ausgabe der Fragebögen hat einer der beteiligten Bürgermeister mir diese übersandt und um „kurzfristige Beantwortung sowie gegebenenfalls weiterführende rechtliche und tatsächliche Hinweise“ gebeten. Er hat sich, so wird man vermuten können, in dieser in der Bevölkerung in der Sache nicht unumstrittenen Frage kurz noch vorsorglich hinsichtlich der Verfahrensweise datenschutzrechtlich absichern wollen.

Umgehend habe ich den Bürgermeister auf meine Ausführungen in 4/5.7.6 zur Frage der Zulässigkeit derartiger Bürgerbefragungen einschließlich der Frage der Einbeziehung der 16- und 17-jährigen Jugendlichen der Gemeinde hingewiesen und deutlich gemacht, dass sich an dem von mir damals eingenommenen Rechtsstandpunkt nichts geändert hat: Die in der Gemeindeordnung geregelten Formen der Beteiligung der Einwohnerschaft an derartigen Entscheidungen, nämlich der Bürgerentscheid nach § 24 SächsGemO und im vorliegenden Falle zusätzlich das Anhörungsverfahren nach § 8 Abs. 1 und 4 SächsGemO sind *abschließende Regelungen* für die Erhebung personenbezogener Daten. Dabei habe ich dem Bürgermeister angeboten, falls er Einwände oder ergänzende Fragen zum Verhältnis zwischen konsultativen Volksbefragungen und verfassungsrechtlichem Demokratieprinzip habe, das von mir seinerzeit erörtert worden ist, sich wieder an mich zu wenden. Von dieser Möglichkeit hat er auch Gebrauch gemacht, was mir Gelegenheit gegeben hat, die von mir damals angestellten Überlegungen noch einmal zu erläutern und dabei auch das Verhältnis zwischen Statistik und derartigen Befragungen zu präzisieren:

Die konsultative Volksbefragung ist selbstverständlich der ‚Kompetenz’ des Entscheidungsträgers Parlament oder Gemeinderat oder (sonstige) Exekutive abträglich. Auf den ersten Blick scheint das unter Demokratie-Gesichtspunkten überhaupt nicht schlimm, ja sogar gut zu sein. Allerdings ist diese Abträglichkeit eine lediglich faktische und keine rechtliche. Denn eine Volks- oder Einwohnerbefragung der Art, wie sie hier geplant gewesen ist, also gerade außerhalb der von der Rechtsordnung zur Verfügung gestellten Abstimmungsverfahren (Bürgerentscheid, Volksentscheid), ist eine rechtlich unverbindliche - eben eine lediglich „konsultative“. Das Problem liegt nun darin, dass dem nach dem Grundprinzip der Demokratie obersten Entscheidungsträger, nämlich dem Volk bzw. der Gemeinde-Einwohnerschaft, in Gestalt einer amtlichen Befragung eine Willensäußerung abverlangt werden soll, die eben rechtlich im Verhältnis zu dem demgegenüber nach dem Grundprinzip der Demokratie schwächeren Entscheidungsträger, nämlich der gewählten Vertretung (sei sie nun als Parlament oder als Exekutivorgan einzuordnen), nicht maßgeblich sein, sondern gegenüber der Entscheidung dieses letzteren Entscheidungsträgers gegenüber nachrangig, ja genaugenommen unmaßgeblich sein soll.

Aus diesem - in der Tat nicht ganz auf der Hand liegenden - Gedankengang folgt, dass eben doch gerade das Demokratie-Prinzip und nicht, wie es vordergründig in der Tat ausschließlich der Fall zu sein scheint, das Repräsentativ-Prinzip berührt, ja verletzt ist. Letzteres ist deswegen nicht verletzt, weil ja de iure die gewählten Entscheidungsträger, nicht das Volk selbst, entscheiden sollen.

Es handelt sich dabei logisch gewissermaßen um einen Widerspruch und praktisch-politisch um einen Gewissenskonflikt - beides sollte die Rechtsordnung nach Möglichkeit vermeiden.

Der Präsident des Bundesverfassungsgerichts, Prof. Hans-Jürgen Papier, hat es in einem Interview auf die Frage, ob der Entwurf eines Verfassungsvertrages für die EU ohne eine Verfassungsänderung in Deutschland zum Gegenstand einer konsultativen Volksbefragung gemacht werden könne, schlicht so formuliert: Konsultative Volksbefragungen seien verfassungsrechtlich problematisch, weil sie zwar ‚formal-juristisch' keine verbindlichen Folgen zeitigten, wohl aber mittelbar politisch vergleichbare Wirkungen hätten (FAZ 8. Juni 2004, S. 5).

Der Bürgermeister hatte aber nicht nur verfassungsrechtlich im Hinblick auf das Problem der konsultativen Volksbefragungen argumentiert, sondern auch aus dem zweiten Teil des Abschnittes 5.7.6 meines 4. TB gefolgert, dass die unverbindliche Bevölkerungsbefragung amtlich auch in Gestalt einer *amtlichen Statistik* durchgeführt werden könne. Damit hatte er insofern recht gehabt, als ich seinerzeit in dem Dresdner Fall die Unzulässigkeit einer solchen Statistik(Satzung) rein statistikrechtlich begründet habe. Die Frage, ob nicht die Demokratieprinzip-Widrigkeit einer bloß unverbindlichen Willensbekundung des Souveräns die rechtliche Wirkung haben muss, dass eine ins Gewand einer Kommunalstatistik gekleidete Meinungsbefragung unzulässig ist, hat seinerzeit nicht beantwortet werden müssen. Ich bin nun zu der Auffassung gekommen, dass auch diese Frage mit „ja" beantwortet werden muss: Unverändert bin ich der Auffassung, dass auch die mit statistischen Methoden und zu - lediglich - statistischen Zwecken durchgeführte Erhebung bloßer Meinungen (Einstellungen, Überzeugungen, Werthaltungen, Zukunftseinschätzungen) oder sonstiger subjektiver Gegebenheiten im Rechtssinne Statistiken sind (dass das Haben und vor allem das Bekunden einer Meinung ein personenbezogenes Datum ist, lässt sich unschwer § 3 Abs. 9 BDSG entnehmen). Aber das verfassungsrechtliche Demokratieprinzip steht einer Auslegung des Sächsischen Statistikgesetzes (bzw. überhaupt der Statistikgesetze) entgegen, die darauf hinausliefe, es als Grundlage für eine amtliche Statistik - und damit als Ermächtigungsgrundlage für eine Verarbeitung personenbezogener Daten zu diesem Zweck - zu verstehen, in der (wohlgemerkt:) amtlich, durch eine Behörde als Träger

öffentlicher Gewalt, die Meinung der Einzelnen in einer von den in der Rechtsordnung bestimmten Entscheidungsträgern zu entscheidenden Frage erhoben wird.

Erklärtermaßen kaum in der Überzeugung, sich an geltendes Recht gehalten zu haben, als vielmehr im Hinblick auf „die Autorität des Sächsischen Datenschutzbeauftragten" als etwas *Faktisches mit normativer Kraft* haben die Bürgermeister ihr ursprüngliches Vorhaben dann aufgegeben. Stattdessen haben sie, *mangelnden Schutz vor dem Datenschutz* beklagend, die Angelegenheit mit den einheimischen Gewerbevereinen und auch mit der örtlichen Presse besprochen. Diese hat dann eine Befragung mit den von den Bürgermeistern entwickelten Inhalten durchgeführt, und getrennt davon haben gemeinsam verschiedene Vereine eine inhaltlich gleiche Befragung auf den Weg gebracht - was beides an meine Behörde gerichtete empörte Anfragen von Einwohnern ausgelöst hat. Dazu habe ich dem betreffenden Bürgermeister erläutert, dass der Sächsische Datenschutzbeauftragte kraft seiner Zuständigkeit nach § 2 SächsDSG, also was die Zuständigkeit für die Verarbeitung personenbezogener Daten durch öffentliche Stellen betrifft, nur insoweit zuständig ist, als Träger öffentlicher Gewalt, also im konkreten Fall die vier Bürgermeister, mittelbar die Verarbeitung personenbezogener Daten veranlasst haben, indem sie, wie es in der „Freien Presse" hieß, alle Leser aufgefordert haben, sich an der Leserumfrage der Zeitung zu beteiligen. Ein solcher „Aufruf" seitens der Bürgermeister hat diese Aktion zu einer halbamtlichen gemacht. Das hätte nicht sein dürfen. Anregungen, die die Bürgermeister mündlich Vereinen zum Datensammeln gemacht haben, habe ich als noch hinnehmbar beurteilt. Es hätte jedoch nicht der Fall sein dürfen, was angeblich jedoch geschehen ist, dass nämlich die durchführenden Vereine dadurch in den Geruch gekommen sind, bloße Strohmänner der Stadtverwaltung gewesen zu sein, dass sie bei der Frage nach einem Ansprechpartner im Hinblick auf die Befragung auf den jeweiligen Bürgermeister verwiesen haben. Ich habe den Bürgermeister aufgerufen, gegenüber den Vereinen deutlich klarzustellen, dass derartige missverständliche, die Kommune nach dem Erscheinungsbild in die Befragungsaktion hineinziehenden Äußerungen in Zukunft zu unterbleiben haben. Desgleichen waren die Stadtverwaltungen verpflichtet, es zu unterlassen, Auskünfte über die Sammelstellen für die abzugebenden Fragebögen zu erteilen, damit gewährleistet war, dass es sich auch dem äußeren Erscheinungsbild nach um eine Aktion ausschließlich der Vereine handelte. (Gegen die Weiterleitung falsch eingeworfener verschlossener Umschläge an einen Postzustellbetrieb habe ich keine Einwände erhoben.)

Selbstverständlich ist es den Bürgermeistern und Gemeinderäten unbenommen gewesen, kommunalpolitisch die Ergebnisse nichtamtlicher Befragungen zur Kenntnis zu nehmen und bei ihren Entscheidungen zu berücksichtigen. Es hat sich um Befragungen gehandelt, die bedauernswerterweise nicht mit ausschließlich privatem Erscheinungs-

bild durchgeführt worden, aber doch im Wesentlichen als rein private Umfragen anzusehen gewesen sind.

5.7.6 Keine Übermittlung von Einzelangaben aus der Todesursachenstatistik durch das Statistische Landesamt an die Gesundheitsämter

In den Gesundheitsämtern und auf deren Anregung im SMS hat es Bestrebungen gegeben, mit einer im Rahmen oder zumindest im Zusammenhang mit der Novellierung des Sächsischen Bestattungsgesetzes einzuführenden Rechtsvorschrift zu ermöglichen, dass das StaLA Einzelangaben aus der Todesursachenstatistik an die Gesundheitsämter übermittelt.

Ich habe geltend gemacht, dass eine solche Regelung gegen höherrangiges Recht verstieße und mit dieser Meinung am Ende beim SMS auch Gehör gefunden.

(1) Der *Sachverhalt*, nämlich die Gegebenheiten und die den genannten Bestrebungen zugrundeliegenden Überlegungen, waren einigermaßen kompliziert:

(1.1) Der Vordruck für den *vertraulichen Teil der Todesbescheinigung* wird vom Arzt mehr oder weniger vollständig ausgefüllt. Dabei machen die Ärzte vielfach Angaben über verschiedene ihnen bekannt gewordene Krankheiten, die der Tote gehabt hat (unter den Überschriften „Todesursache, Klinischer Befund“ und „Nähere Angaben zur Todesursache und zu Begleiterkrankungen [Epikrise]“), vielfach wird aber zur *Todesursache* unter I Buchst. c die eigentliche Ursache, also das sog. *Grundleiden*, nicht oder doch nicht richtig angegeben.

(1.2) Vor Übersendung an das Gesundheitsamt (abweichend von § 14 Abs. 3 Satz 5 SächsBestG, aber in Übereinstimmung mit § 6 Abs. 1 Satz 2 BevStatG, und damit wohl rechtmäßig - aber nicht etwa auf eine entsprechende Regelung der Dienstanweisung für Standesbeamte zu stützen) überprüft, auf der dazu wohl heranzuziehenden Grundlage des § 14 Abs. 4 Satz 1 SächsBestG, das Gesundheitsamt („zu statistischen Zwecken“ wohl auch der betreffenden Bundesstatistik, also konkret auch des StaLA) den Inhalt der Todesbescheinigung - Entsprechendes gilt für den Obduktionsschein - *auf Vollständigkeit und Richtigkeit der von dem Arzt vorgenommenen Eintragungen*. Diese Überprüfung führt gegebenenfalls zu Änderungen, also Berichtigungen oder Ergänzungen, unter Umständen auch aufgrund Rücksprache mit dem Arzt. Die Überprüfung wird von den Gesundheitsämtern in unterschiedlicher Qualität (manchmal nur von Schreibkräften, manchmal von medizinisch ausgebildeten Kräften) durchgeführt, die überprüften Todesbescheinigungen bzw. Obduktionsberichte werden sodann an das StaLA weitergegeben. Dies erfolgt monatlich.

Eine Übermittlung „auf automatisiert verarbeiteten Datenträgern oder durch Datenübertragung“ ist gemäß § 6 Abs. 1 Satz 3 BevStatG zulässig.

(1.3) Im StaLA werden die eingegangenen Daten vor allem hinsichtlich des Merkmals „Grundleiden“ als der eigentlichen *Todesursache* im Sinne von § 2 Abs. 1 Nr. 3 Buchstabe d BevStatG, und damit des hauptsächlichen statistischen Auswertungsmerkmals, überprüft. Dabei wird aufgrund von Vorgaben der Weltgesundheitsorganisation (WHO), die in einem Handbuch niedergelegt sind und auch mittels Hilfsprogrammen angewandt werden können, die eigentliche Todesursache, also das *Grundleiden*, festgestellt, und zwar anhand dieser genannten Regeln abgeleitet aus den verschiedenen vom Arzt gemachten Angaben zu Krankheiten, ggf. unter Korrektur der vom Arzt zum *Grundleiden* gemachten Angaben. Diese Aufgabe wird von sog. Signierern erfüllt.
(In diesem Stadium wären, weil es sich noch um die Erhebungsphase der Durchführung einer Statistik handelt, Rückfragen zu Einzelfällen beim Gesundheitsamt datenschutz- bzw. statistikrechtlich unbedenklich.)

Das Regelwerk der WHO hat die Funktion, auf der Grundlage medizinischen Wissens für eine weltweit einheitliche Todesursachenbeurteilung zu sorgen.

Die Änderungsquote, also der Anteil der Fälle mit Vervollständigung oder Berichtigung hinsichtlich des Merkmals „Grundleiden“, also des Erhebungsmerkmals (eigentliche) „Todesursache“ im Sinne von § 2 Abs. 1 Nr. 3 Buchstabe d BevStatG, liegt ganz grob geschätzt zwischen einem Drittel und zwei Dritteln.

(1.4) In den Fällen, in denen zusätzlich zum (einfachen) Leichenschauschein (Totenschein) ein Obduktionsschein ausgefüllt wird (§ 15 Abs. 5 SächsBestG), dessen Überprüfung durch das Gesundheitsamt (im Bestattungsgesetz) nicht vorgesehen ist, wird dieser, anscheinend aufgrund einer Subsumtion unter den Begriff *Leichenschauschein (Totenschein)* in § 2 Abs. 2 Satz 3 BevStatG, vom Gesundheitsamt an das StaLA übermittelt. Dies betrifft etwa fünf bis sechs Prozent aller Todesfälle, und dabei kann der zeitliche Abstand zur Übermittlung des (einfachen) Totenscheines in Einzelfällen mehrere Monate betragen.

(1.5) Die Todesursachenstatistik wird jährlich durchgeführt, und das StaLA veröffentlicht auf der Grundlage dieser Jahresstatistik einen Todesursachen-Bericht.

(1.6) Die von Praktikern aus einzelnen Gesundheitsämtern nun für wünschenswert gehaltene Daten-Rückübermittlung vom StaLA an die Gesundheitsämter bestünde aus Datensätzen, die aus folgenden Merkmalen bestünden:

- Als Hilfsmerkmal ein Identifikator, der aus einer Zahlenkombination bestünde, die schon im Gesundheitsamt jeweils für jeden einzelnen Todesfall eineindeutig erzeugt wird,
- das *Grundleiden* durch Angabe der Kennung nach dem ICD,
- die Angabe, ob ein Obduktionsbefund vorliegt,
- die „äußere Todesursache“, also die Angabe über nicht-natürliche Todesursachen wie Unfall, Fremdeinwirkung einschließlich medizinischer Behandlung oder Selbsttötung.

(1.7) Das Interesse der Gesundheitsämter bestünde darin, für den eigenen räumlichen Zuständigkeitsbereich eine Statistik über die Todesursachen führen zu können. Dabei wird angegeben (so im Bezugsschreiben), dass durch die Übermittlung unter Hinzufügung des Identifikators die Erkenntnis kleinräumiger Todesursachenverteilungen, also heruntergebrochen auf Teile des örtlichen Zuständigkeitsbereiches des Gesundheitsamtes, möglich gemacht werde.

Diese Überlegung ist schlüssig nur für Erkenntnisse unterhalb der räumlichen Einheit „Wohngemeinde“ (§ 2 Abs. 1 Nr. 3 Buchstabe a BevStatG), also nur für Großstädte (mit anderen Worten: Beim StaLA geht zwar die genaue Anschrift des Verstorbenen ein, das Datum wird jedoch gar nicht in dieser Genauigkeit erfasst, sondern eben lediglich die Wohngemeinde).

(1.8) Was die genannten drei Erhebungsmerkmale betrifft, so ist das als zweites genannte Merkmal (Obduktionsbefund vorliegend oder nicht) wenig aussagekräftig; immerhin weiß das Gesundheitsamt zu jedem Todesfall, ob ein Obduktionsbefund vorliegt oder nicht.

Falsche Angaben zur „äußeren“, also zur nicht-natürlichen Todesursache, also etwa falsche Einschätzung hinsichtlich Unfall, Fremdeinwirkung oder Selbstmord, sind nur bei extrem unsorgfältiger Arbeitsweise des Arztes und des Gesundheitsamtes anzunehmen; genauere Ermittlungsergebnisse der Strafverfolgungsbehörden, die viel später anfallen können, gehen, soweit erkennbar, nicht in die Statistik ein, eine diesbezügliche Übermittlung an das StaLA bzw. Erhebung durch das StaLA ist im Gesetz nicht vorgesehen.

(2) Meine rechtliche Bewertung ist folgende gewesen:

(2.1) Eine entsprechende landesrechtliche Vorschrift dürfte schon gegen § 16 Abs. 1 Satz 1 BStatG verstoßen: Es handelt sich um die Durchführung einer Bundesstatistik. Für Bundesstatistiken ist ausschließlich der Bundesgesetzgeber zur Gesetzgebung zuständig (Art. 73 Nr. 11 GG). Deswegen dürfte der Vorbehalt abweichender Regelungen durch besondere Rechtsvorschrift in § 16 Abs. 1 Satz 1 BStatG sich ausschließlich auf

bundesrechtliche Vorschriften beziehen (davon geht wohl auch die Kommentierung von Dorer/Mainusch/Tubies, Rdnr. 19 bis 21 zu § 16 BStatG aus).

(2.2) Darüber hinaus ist es nach dem Volkszählungsurteil des BVerfG (E 65, 1 ff., 51 unten, 61, 66) höchst zweifelhaft, ob es zulässig ist, dass Einzelangaben (personenbezogene Daten), wie es hier der Fall wäre, von Statistikbehörden an andere Behörden übermittelt werden dürfen. Dabei spielt es keine Rolle, dass die Daten zum größeren Teil vom Gesundheitsamt selbst zum StaLA gekommen sind; das Gesundheitsamt ist ja gerade deswegen an solchen Daten interessiert, weil es sie nicht selbst in dieser Qualität (und damit mit diesem Inhalt) hat.

Bei dieser verfassungsrechtlichen Beurteilung ist zu berücksichtigen, dass ein wirklich schwerwiegendes, bedeutende verfassungsrechtliche Güter betreffendes Interesse an der in Rede stehenden Übermittlung vom StaLA an die Gesundheitsämter nicht erkennbar ist:

Wegen der mir genannten allgemeinen Presseanfragen (aus Anlass des Todesursachen-Berichtes des StaLA fragt die Presse, wie denn die entsprechenden Zahlenwerte für den eigenen Landkreis sind) kann die Presse auch an das StaLA verwiesen werden, dies kann die Anfrage sehr schnell beantworten, wie gezeigt sogar gemeindebezogen. Bei aktuellen Katastrophen-Fällen oder Katastrophen-Verdachts-Fällen wird das öffentliche Interesse wohl wesentlich dringender sein, als dass es mit einem Rücklauf nach etwa zwei Monaten vom StaLA befriedigt werden könnte; in solchen Fällen dürften konkrete Todesfalluntersuchungen stattfinden, vermutlich auch aufgrund von Anordnungen von Strafverfolgungsbehörden. Bei der Suche nach nicht ganz offensichtlich statistischen Zusammenhängen, die auf bestimmte Ursachenzusammenhänge hinweisen, etwa erhöhte Leukämieraten in der Nachbarschaft bestimmter technischer Anlagen, kommt es nach allen Erfahrungen darauf an, dass gründliche wissenschaftliche Untersuchungen durchgeführt werden, die viele Monate oder gar Jahre benötigen und genauere Feststellungen zu den Erkrankungen treffen müssen, als es im Rahmen von Leichenschau und Todesursachenstatistik geschieht - auch insoweit besteht kein dringendes Interesse des örtlichen Gesundheitsamtes an dem Rücklauf von Einzelangaben aus der amtlichen Todesursachenstatistik.

Aus alledem ist gefolgt, dass von der Schaffung einer entsprechenden gesetzlichen Regelung aus rechtlichen Gründen unbedingt Abstand zu nehmen gewesen ist. Auch abgesehen davon wäre es nicht im Interesse der amtlichen Statistik gewesen, wenn Ausnahmen vom Statistikgeheimnis ohne verfassungsrechtlich schwerwiegendste Gründe vorgesehen worden wären.

Das hat die Beteiligten vielleicht nicht überzeugt, aber eben doch von ihrem Vorhaben Abstand nehmen lassen.

Siehe auch unten 13.2.

5.8 Archivwesen

5.8.1 Auch ein Landes-Datenschutzbeauftragter ist an Zuständigkeitsregeln gebunden

Der Datenschutzbeauftragte taugt nicht als Helfer in allen personenbezogene Daten betreffenden Fragen. Dies musste ich einer Petentin verständlich machen, die durch Einschaltung meiner Dienststelle das Geburtsdatum und den Geburtsort ehemaliger Insassen eines im Jahr 1983 aufgelösten Kinderheimes in Erfahrung bringen wollte, um diese für ein von ihr geplantes Ehemaligen-Treffen anschreiben zu können. Die Petentin selbst war zuvor, so hatte es den Anschein, mit ihrer Anfrage bei verschiedenen Behörden, an die sie sich gewandt hatte, nicht weitergekommen.

Die erbetene Mithilfe bei der Personensuche habe ich ablehnen müssen, da ich für derlei Datenbeschaffungs-Aufgaben nicht zuständig bin:

Der Sächsische Datenschutzbeauftragte kann die öffentlichen Stellen im Freistaat Sachsen in Datenschutzfragen beraten (§ 30 Abs. 4 SächsDSG) und er hat sie zu kontrollieren, also dafür zu sorgen, dass sie nur auf gesetzlicher Grundlage Informationen über Menschen sammeln, nutzen und insbesondere auch übermitteln (§ 27 Abs. 1 SächsDSG). Im Hinblick darauf kann sich jedermann an mich wenden, wenn er der Ansicht ist, bei der Verarbeitung seiner personenbezogenen Daten durch eine Behörde oder sonstige öffentliche Stellen in seinem Recht auf informationelle Selbstbestimmung verletzt worden zu sein (§ 24 Abs. 1 Satz 1 SächsDSG). In ähnlich gelagerten Fällen, bei denen es aber um den Anfrager selbst ging, habe ich bereits helfen können. Ein derartiger Eingriff in das Recht auf informationelle Selbstbestimmung lag jedoch nicht vor, insbesondere wurden der Petentin ja nicht sie selbst betreffende Daten vorenthalten, war also ihr datenschutzrechtlicher Auskunftsanspruch nicht berührt, natürlich auch nicht in der archivrechtlichen Gestalt des § 6 Abs. 3 SächsArchivG.

Dementsprechend wäre es mir lediglich möglich gewesen, mich an sächsische Stellen, die vielleicht Auskünfte unter Berufung auf datenschutzrechtliche Gründe verweigert hatten, zu wenden und aufzuklären zu versuchen, inwieweit datenschutzrechtliche Gründe der Erteilung der erbetenen Auskünfte entgegenstehen. Die von der Petentin jedoch in allererster Linie erbetene aktive Mithilfe bei der Suche nach Daten über die betreffenden Personen durfte und konnte ich deswegen gar nicht leisten: Nachfor-

schungen nach dem Verbleib von Datenbeständen sind nicht meine Aufgabe. Es war auch keine Rechtsgrundlage ersichtlich, die es mir erlaubt hätte, bei den in Frage kommenden Behörden selbst die erbetenen Auskünfte, das heißt Geburtsdatum und Geburtsort der gesuchten Personen, zu erfragen, da das Erfragen dieser Daten für meine Kontrolle nicht erforderlich gewesen wäre, schließlich wäre ich aber insbesondere auch nicht befugt gewesen, die entsprechenden Auskünfte an die Petentin weiterzuleiten.

Auch der Datenschutzbeauftragte, als Behörde, ist aus gutem rechtsstaatlichem Grund an die bestehenden Zuständigkeitsregeln und die daraus folgenden datenschutzrechtlichen Beschränkungen gebunden.

5.9 Polizei

5.9.1 Keine Amtshilfe der Polizei für freie Mitarbeiter der Gebühreneinzugszentrale (GEZ)

Zwei freie Mitarbeiter der GEZ riefen die Polizei in eine Gartensparte, um dort die Personalien des Pächters eines Kleingartens feststellen zu lassen. Sie gaben sich gegenüber den Polizeibeamten wahrheitswidrig als Beschäftigte des MDR aus und behaupteten, dass Ansprüche auf Rundfunkgebühren gegen den Pächter bestünden. Die Polizeibeamten waren irrtümlich der Ansicht, die Personalien des Pächters zum Schutz privater Rechte erheben zu können und stellten im Beisein der Mitarbeiter der GEZ dessen Personalien fest.

Tatsächlich haben die freien Mitarbeiter der GEZ weder Anspruch auf Amtshilfe noch auf Vollzugshilfe von Seiten der Polizei, da sie nicht Mitarbeiter einer Behörde und auch nicht vertretungsberechtigt für eine der öffentlich-rechtlichen Rundfunkanstalten sind. Sie arbeiten vielmehr selbständig auf erfolgsorientierter Provisionsbasis. Dennoch ist das geschilderte Vorgehen von Mitarbeitern der GEZ kein Einzelfall. Sie missbrauchen die Polizei immer wieder als Ermittlungshelfer für privatrechtliche Zwecke.

Aufgrund meines Tätigwerdens wertete die zuständige Polizeidirektion den Sachverhalt mit den Polizeibeamten aus und erließ eine diesbezügliche Handlungsanweisung für ihre Bediensteten. Diese Handlungsanweisung stellt klar, dass entsprechenden Anfragen von Mitarbeitern der GEZ auf Unterstützung bei der Personalienfeststellung oder Ähnlichem durch die Polizei nicht zu entsprechen ist und diesbezügliche Auskünfte aus polizeilichen Informationssystemen ebenfalls nicht gestattet sind.

Die in der Handlungsanweisung enthaltenen Vorgaben halte ich für geeignet, den Polizeibeamten vor Augen zu führen, dass die freien Mitarbeiter der GEZ bei Identitätsfeststellungen nicht von der Polizei unterstützt werden können. Um etwaige Unsicherheiten

in der rechtlichen Beurteilung von Unterstützungsersuchen durch Mitarbeiter der GEZ bei der Polizei auszuräumen, hat das SMI die Handlungsanweisung auf meine Bitte hin allen sächsischen Polizeidirektionen übersandt.

5.9.2 Fehlende gesetzliche Regelung des PASS-Verbundverfahrens

Das polizeiliche Auskunftssystem Sachsen (PASS) dient den einzelnen sächsischen Stellen des Polizeivollzugsdienstes zur landesweiten Erfassung, Speicherung und Auswertung polizeilich relevanter Informationen zu Straftaten, die im Freistaat Sachsen bearbeitet werden, oder deren Ereignisort sich auf dem Gebiet des Freistaates Sachsen befindet. Im Zusammenhang mit der Überprüfung der mir vom SMI vorgelegten Neufassung der Errichtungsanordnung zum PASS bin ich zu dem Ergebnis gelangt, dass es sich bei diesem Verfahren um ein Verbundverfahren handelt, für welches es zurzeit in Sachsen keine ausreichende Rechtsgrundlage gibt.

Davon ausgehend, dass es sich bei den durch Dienstbezirke und unterschiedliche Aufgaben voneinander abgrenzbaren Dienststellen des Polizeivollzugsdienstes (Landespolizeipräsidium, Landeskriminalamt, Präsidium der Bereitschaftspolizei, Polizeidirektionen) um datenschutzrechtlich eigenständige Stellen handelt, kann das PASS nur ein automatisiertes Abrufverfahren oder Verbundverfahren sein. Ein *automatisiertes Abrufverfahren* (§ 48 Abs. 1 SächsPolG i. V. m. § 8 SächsDSG) setzt voraus, dass eine für die Rechtmäßigkeit der Dateneingabe und -speicherung verantwortliche Stelle die Daten zum Abruf für andere Stellen bereithält. Die abrufenden Stellen haben - außer der Abrufmöglichkeit - keine weiteren Datenverarbeitungsbefugnisse, d. h. sie dürfen weder Daten eingeben, löschen noch sonst verarbeiten. Nach dem mir vorliegenden Entwurf der Errichtungsanordnung zum PASS soll die praktische Anwendung des PASS in Sachsen aber anders aussehen. Danach sollen die einzelnen Dienststellen des Polizeivollzugsdienstes (z. B. die Polizeidirektionen) zuständig und verantwortlich für die Speicherung (Einstellung), Löschung und sonstige Verarbeitung der Daten im PASS sein. Polizeidienststellen sollen somit nicht nur abrufende, sondern auch eingebende und für die Datenverarbeitung verantwortliche Stellen sein. Das Verfahren ist deshalb aus meiner Sicht kein Abrufverfahren, sondern ein *Verbundverfahren*. Verbundverfahren sind gemeinsame oder verbundene automatisierte Verfahren, in oder aus denen mehrere öffentliche Stellen personenbezogene Daten verarbeiten. Es unterscheidet sich insoweit von einem automatisierten Abrufverfahren, als nicht nur eine, sondern verschiedene Stellen für die Datenverarbeitung verantwortlich sind. Personenbezogene Daten werden auf vielfältige Weise von verschiedenen verantwortlichen Stellen verarbeitet. Ein solches Verfahren birgt ein größeres Gefahrenpotential für das Recht auf informationelle Selbstbestimmung der Betroffenen, als ein automatisiertes Abrufverfahren, weil die verschiedenen Daten einstellenden Stellen keinen Einfluss darauf haben, wann und wie

viele Daten zu welchen Zwecken zur Kenntnis und in die Verfügungsgewalt von abrufenden Dritten gelangen. Außerdem ist für die von der Datenverarbeitung Betroffenen - wenn überhaupt - nur schwer erkennbar, welche Stelle die datenschutzrechtliche Verantwortung für die Datenverarbeitung trägt.

Da es für die Einrichtung einer polizeilichen landesweiten Verbunddatei zum jetzigen Zeitpunkt keine Rechtsgrundlage in Sachsen gibt, habe ich beim SMI angeregt, eine solche in das Sächsische Polizeigesetz aufzunehmen und zu regeln, unter welchen Voraussetzungen, welche Daten zu welchem Zweck von welcher Stelle verarbeitet werden dürfen und welche Stellen die datenschutzrechtliche Verantwortung gegenüber den betroffenen Personen tragen.

Das SMI hält die Schaffung einer speziellen Rechtsgrundlage zwar nicht für zwingend erforderlich, steht jedoch einer klarstellenden Ergänzung des Sächsischen Polizeigesetzes nicht vollständig ablehnend gegenüber. Es betrachtet den gesamten Polizeivollzugsdienst mit allen einzelnen Dienststellen als eine Stelle und hält davon abgesehen den Betrieb vom PASS auf der Grundlage des § 43 SächsPolG für zulässig.

Dagegen ist einzuwenden, dass es sich bei dem § 43 SächsPolG um eine allgemeine, materielle Erlaubnisnorm für den Polizeivollzugsdienst handelt, die allgemein die Verarbeitung personenbezogener Daten in Akten oder Dateien erlaubt und die materiellen Zulässigkeitsvoraussetzungen für die Speicherung, Veränderung und Nutzung personenbezogener Daten durch den Polizeivollzugsdienst in Akten und Dateien bestimmt. Sie entspricht den Vorschriften, aus denen sich die (materiellen) Zulässigkeitsvoraussetzungen für die Datenerhebung, -übermittlung, -löschung, etc. ergeben, wie z. B. §§ 37, 43, 44 SächsPolG bzw. § 14 SächsDSG. Die in diesen Vorschriften genannten Voraussetzungen nennen allgemein - unabhängig von der Art des Datenverarbeitungsverfahrens - die (materiellen) Zulässigkeitsvoraussetzungen für die Zulässigkeit der Verarbeitung personenbezogener Daten und gelten insoweit selbstverständlich auch für die Verarbeitung der Daten im PASS. Darüber hinaus ist aber für besondere Formen von Datenverarbeitungsverfahren der Polizei (z. B. automatisierte Abrufverfahren oder Verbundverfahren) eine spezielle Rechtsgrundlage erforderlich. Eine solche spezielle Rechtsgrundlage wurde dementsprechend auch in § 48 SächsPolG für den Einsatz von automatisierten Abrufverfahren vom Gesetzgeber geschaffen. Geschuldet ist dies dem Umstand, dass automatisierte Abrufverfahren und Verbundverfahren besondere Gefahren für das Recht auf informationelle Selbstbestimmung in sich bergen. Diese speziellen Formen der automatisierten Datenverarbeitung dürfen deshalb nur aufgrund einer speziellen Rechtsgrundlage eingesetzt werden.

Von einer Beanstandung der Errichtungsanordnung, bzw. deren praktischer Umsetzung habe ich abgesehen, weil das PASS für die Polizei als Hilfsmittel zur Aufgabenerfüllung unentbehrlich und materiell nicht zu beanstanden ist. Ich empfehle aber weiterhin dringend, das Sächsische Polizeigesetz um eine Norm zu Verbundverfahren zu ergänzen.

5.9.3 Übermittlung von Daten potentiell gefährlicher Blutspender an eine Blutbank

Eine Staatsanwaltschaft unterbreitete mir folgenden interessanten Fall: Eine 26-jährige Frau habe sich im Frühjahr 2008 selbst getötet. Durch die Sektion sei eine HIV-Infektion festgestellt worden. Die Verstorbene sei Blutspenderin gewesen und habe häufig wechselnde Sexualpartner gehabt. Anfang Dezember 2007 habe sie letztmalig Blut gespendet und danach ausweislich ihres Notizbuchs sexuelle Kontakte zu mindestens elf Männern gehabt. Acht davon seien der Polizei namentlich bekannt. Die gespendeten Blutdosen seien bisher - mit jedoch nicht ganz zuverlässigen Tests - negativ getestet worden. Der Leiter einer örtlichen Blutbank, über deren Tisch ca. 70 % der im Stadtgebiet gewonnenen Blutdosen ginge, wolle nun wissen, ob und ggf. welche der der Polizei bekannten acht Sexualpartner ebenfalls Blutspender waren. Die Polizei habe bereits die Blutbank sowie die ihr namentlich bekannten acht Männer über das HIV-positive Ergebnis des Bluttests der Verstorbenen in Kenntnis gesetzt. Die Polizei frage nun an, ob sie die Namen der acht Männer an die Blutbank zwecks Abgleich übermitteln dürfe.

Ich habe der Staatsanwaltschaft mitgeteilt, dass dies aus folgenden Gründen nur mit der Einwilligung der Betroffenen in Betracht kommt:

Die Übermittlung polizeilicher Daten an öffentliche Stellen, hier die Blutbank, bemisst sich nach § 14 SächsDSG, da das Sächsische Polizeigesetz keine bereichsspezifische Übermittlungsvorschrift enthält. Danach ist die Übermittlung zulässig, wenn sie zur Erfüllung der Aufgaben u. a. der übermittelnden Stelle erforderlich ist und die Voraussetzungen vorliegen, die eine Nutzung nach § 13 Abs. 1 bis 4 SächsDSG zuließen. Nach § 13 Abs. 2 Nr. 1 SächsDSG ist eine zweckändernde Nutzung dann zulässig, wenn die Voraussetzungen vorliegen, unter denen nach § 12 Abs. 4 SächsDSG eine Erhebung bei Dritten zulässig wäre. Nach § 12 Abs. 4 Nr. 7 SächsDSG ist die Erhebung personenbezogener Daten bei Dritten zulässig, wenn „es zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte einer anderen Person erforderlich ist“. Die zur Übermittlungsbefugnis führende Paragraphenkette lautet also § 14 Abs. 1, § 13 Abs. 2 Nr. 1, § 12 Abs. 4 Nr. 7 SächsDSG.

Diese Voraussetzungen waren allesamt erfüllt. Nach § 1 Abs. 1 Satz 1 SächsPolG hätte die Polizei unzweifelhaft u. a. die Aufgabe, Gefahren für Leib oder Leben eines, wenngleich momentan noch namentlich unbekannten, Blutspendeempfängers abzuwehren. Die zweckändernde Nutzung der polizeibekannten Daten nach § 13 Abs. 2 Nr. 1 SächsDSG war möglich, da die Voraussetzungen einer Datenerhebung bei Dritten nach § 12 Abs. 4 Nr. 7 SächsDSG gegeben sind. Ein milderes Mittel zur Erreichung des angestrebten Zwecks war nicht ersichtlich. Allerdings kam es wegen der ärztlichen Schweigepflicht nicht in Betracht, einen Polizeibediensteten selbst in die Blutspenderdatei der Blutbank einsehen und den Abgleich selbst durchführen zu lassen. Denn schon das bloße Datum, dass jemand Blutspender ist - dies würde offenbar -, unterliegt der ärztlichen Schweigepflicht und darf durch die Blutbank nicht unbefugt der Polizei offenbart werden.

Allerdings bestimmt § 4 Abs. 2 SächsDSG, der 2003 aufgrund der EG-Datenschutzrichtlinie in das Sächsische Datenschutzgesetz eingefügt wurde, dass die Verarbeitung u. a. von „Daten über Gesundheit und Sexualleben“, hier Namen, Vornamen und Geburtsdatum der Betroffenen, nur zulässig ist, wenn aus Gründen eines wichtigen öffentlichen Interesses eine besondere Rechtsvorschrift dies ausdrücklich vorsieht oder zwingend voraussetzt (§ 4 Abs. 2 Nr. 1 SächsDSG) oder der Betroffene eingewilligt hat (§ 4 Abs. 2 Nr. 2 und 3 SächsDSG). Da eine bereichsspezifische Übermittlungsvorschrift nicht ersichtlich war, kam hier ausschließlich die Einwilligung der Betroffenen als Rechtsgrundlage einer Übermittlung in Betracht. Sollten auf dieser Grundlage die Daten der acht Männer an die Blutbank übermittelt werden, hätte diese außerdem streng auf die Zweckbindung der ihr übermittelten Daten zu achten. Sie dürften nur zur Aussonderung eventuell vorhandener Blutspenden verarbeitet werden und müssen danach unverzüglich und nachweislich gelöscht werden. Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Stelle, hier die zuständige Polizeidienststelle, § 14 Abs. 2 Satz 1 SächsDSG.

Die Polizei ist meinem Rat gefolgt. Sie hat die Personen, die im Zeitraum der HIV-Infektion der später Verstorbenen mit dieser Sexualkontakt hatten, angeschrieben und um Mitteilung gebeten, ob sie mit der Weitergabe ihrer Personalien an die Blutbank einverstanden seien. Ein Betroffener hat dem ohne Angabe von Gründen nicht zugestimmt, zwei Betroffene haben mit der Begründung, keine Blutspender zu sein, nicht zugestimmt, die übrigen Betroffenen haben eingewilligt. Mein Hinweis auf die strikte Zweckbeschränkung wurde ebenfalls beachtet.

5.9.4 Polizeiliche Ermittlungen und apothekerliche Schweigepflicht

Die Sächsische Apothekerkammer teilte mir mit, dass ein Apothekenleiter durch eine örtliche Polizeidienststelle aufgefordert worden sei, im Rahmen eines Ermittlungsverfahrens den Namen eines Kunden der Apotheke (Patienten) zu nennen.

Die Apothekerkammer hielt dies mit der apothekerlichen Schweigepflicht für unvereinbar und deshalb für unzulässig. Ich habe zu dieser Problematik bereits in 3/5.9.7 sowie in 8/5.9.3 Stellung genommen. Damit übereinstimmend bin ich im vorliegenden Fall der Ansicht der Apothekerkammer mit folgender Begründung beigetreten:

Die apothekerliche Schweigepflicht ergibt sich aus § 4 der Berufsordnung der Sächsischen Landesapothekerkammer (BO) vom 23. April 1997. Danach hat der Apotheker „über alle seinen Beruf berührenden Vorkommnisse, die ihm innerhalb und außerhalb seiner Tätigkeit bekannt werden, zu schweigen“. Nach § 4 Abs. 3 BO darf er „unbeschadet der gesetzlichen Aussage- und Anzeigepflichten die der Verschwiegenheit unterliegenden Tatsachen nur mitteilen, soweit der Betroffene ihn von der Schweigepflicht entbunden hat oder die Offenbarung zum Schutz eines höherrangigen Rechtsguts erforderlich ist“.

Die apothekerliche Schweigepflicht wird strafrechtlich durch § 203 Abs. 1 StGB abgesichert. Danach kann sich der Apotheker wegen „Verletzung von Privatgeheimnissen“ strafbar machen, wenn er „unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis, … offenbart“. „Geheimnis“ in diesem Sinne ist insbesondere schon der bloße Umstand, dass sich jemand in apothekerliche Behandlung begeben hat oder der Name des Patienten.

In der Rechtsprechung ist anerkannt, dass das Strafverfolgungsinteresse des Staates die Verletzung dieser apothekerlichen Schweigepflicht grundsätzlich nicht rechtfertigt (OLG Bremen, Medizinrecht 1984, 112).

Dies kann wie folgt begründet werden: Die apothekerliche Schweigepflicht ist Ausdruck eines Grundrechts, namentlich des „Rechts auf informationelle Selbstbestimmung“ aus Art. 2 Abs. 1 i. V. m. Art. 11 Abs. 1 GG, Art. 33 SächsVerf. Demgegenüber wiegt das Rechtsgut „Strafverfolgungsinteresse des Staates“, ein zweifellos wichtiger Bestandteil unserer Rechtsordnung, leichter.

Eine Durchbrechung der apothekerlichen Schweigepflicht dürfte nur bei außerordentlich schweren, mit einer nachhaltigen Störung des Rechtsfriedens verbundenen Verbrechen zulässig sein (z. B. bei terroristischen Gewaltakten). Eine Offenbarung des Patientengeheimnisses wäre im Übrigen zur Gefahrenabwehr in den seltenen Fällen des § 34 StGB

(rechtfertigender Notstand) zulässig, allerdings auch dort erst nach einer Abwägung der widerstreitenden Interessen, wobei der Schutz des bedrohten Rechtsgutes die Integrität des (Grund)Rechts auf informationelle Selbstbestimmung wesentlich überwiegen müsste.

Etwas anderes - eine Offenbarungspflicht nämlich - würde gelten, wenn ein Apotheker „von dem Vorhaben oder der Ausführung“ eines Mordes oder Totschlags „zu einer Zeit, zu der die Ausführung oder der Erfolg noch abgewendet werden kann, glaubhaft erfährt“. Dann müsste der Apotheker dieses Vorhaben der gefährdeten Person oder der Polizei mitteilen. Unterließe er das, könnte er sich nach § 138 StGB wegen „Nichtanzeige geplanter Straftaten“ strafbar machen. Denn in dieser Konstellation ist das „Recht auf informationelle Selbstbestimmung“ nicht gegen das Strafverfolgungsinteresse des Staates abzuwägen, sondern gegen das schwerer wiegende und noch nicht verletzte, sondern zu schützende Grundrecht auf Leben.

Deshalb hätte im vorliegenden Fall der Apothekenleiter der Polizei nur Daten des Patienten mitteilen dürfen, wenn dieser zuvor in die Offenbarung seiner Daten an die Polizei nachweislich (schriftlich) eingewilligt hätte. Dies habe ich der Apothekerkammer mitgeteilt.

5.10 Verfassungsschutz

5.10.1 Rechte des sicherheitsüberprüften Betroffenen im Hinblick auf die zu ihm geführten Sicherheits- und Sicherheitsüberprüfungsakten

Sicherheitsüberprüfungen nach dem Sächsischen Sicherheitsüberprüfungsgesetz können, da eine Vielzahl auch privater oder gar intimer Daten zu einem partiell vollständigen Persönlichkeitsbild zusammengeführt werden, tief in die Datenschutzrechte des Betroffenen eingreifen. Sie geschehen formal auf der Grundlage der Einwilligung des Betroffenen; wird diese nicht erteilt, kann der Betroffene allerdings nicht für eine sicherheits- und damit im Einzelfall eventuell auch aufstiegsrelevante Tätigkeit in Betracht kommen. Sicherheitsüberprüfungen sind daher auch ein gutes Beispiel dafür, dass im Dienst- oder Arbeitsrecht kaum von einer wirklich freien Einwilligung (vgl. § 4 SächsDSG) ausgegangen werden kann.

Sicherheitsüberprüfungen öffentlicher Bediensteter oder von Mitarbeitern privater Unternehmen finden ihre abstrakte Rechtfertigung darin, vorhandene Sicherheitsrisiken zu einem bestimmten Zeitpunkt zu erkennen und Personen, bei denen ein solches Risiko nicht ausgeschlossen werden kann, von sicherheitsrelevanten Tätigkeiten (z. B. Zugang zu Verschlusssachen, Tätigkeit in Rüstungsunternehmen) fernzuhalten. Diese abstrakte Rechtfertigung entfällt allerdings, wenn diese Personen keiner sicherheitsrelevanten

Tätigkeit mehr nachgehen, z. B. weil sie versetzt worden sind. In diesem Fall sollte der Bedienstete wissen können, wie die ihn betreffenden Sicherheitsüberprüfungsdaten weiter verarbeitet werden und insbesondere, wie lange sie noch wo gespeichert werden.

Der Betroffene sollte deshalb

1. gegenüber der „zuständigen Stelle“ im Sinne des Sächsischen Sicherheitsüberprüfungsgesetzes (= Beschäftigungsbehörde) im Wege der Auskunft nach § 24 SächsSÜG um Auskunft ersuchen zu den Fragen

   - ob ein und ggf. welcher Vernichtungstermin für die „*Unterlagen* über die Sicherheitsüberprüfung“ nach § 20 Abs. 2 SächsSÜG vorgesehen ist (im Regelfall sind dies fünf Jahre, gezählt ab dem tatsächlichen Ausscheiden; ein Antrag auf früheres Löschen kann nicht schaden) und ob die Unterlagen vor einer Löschung dem zuständigen Archiv angeboten werden, § 20 Abs. 4 SächsSÜG,
   - ob ein und ggf. welcher Löschungstermin für die in *Dateien* gespeicherten personenbezogenen Daten zu seiner Person gemäß § 23 Abs. 2 Nr. 1 SächsSÜG vorgesehen ist.

2. gegenüber der „mitwirkenden Behörde“ (= LfV Sachsen) um Auskunft ersuchen über

   - den für die *Unterlagen* vorgesehenen Vernichtungstermin nach §§ 20 Abs. 3 Satz 1, 23 Abs. 2 Satz 1 Nr. 1 SächsSÜG; zugleich kann er der weiteren Speicherung widersprechen, d. h. eine etwa dahingehend erteilte Einwilligung widerrufen,
   - den nach § 23 Abs. 2 Satz 1 Nr. 2 SächsSÜG für die in *Dateien* gespeicherten personenbezogenen Daten vorgesehenen Löschungstermin sowie bei evtl. gegebenen Erkenntnissen nach § 21 Abs. 2 Nr. 3 SächsSÜG über die Löschung nach § 23 Abs. 2 Satz 1 Nr. 2 Buchst. c SächsSÜG.

Zugleich sollte sich der Betroffene zur Kontrolle die absehbaren Termine auch selbst zur „Wiedervorlage“ merken.

5.11 Landessystemkonzept/Landesnetz

In diesem Jahr nicht belegt.

5.12 Ausländerwesen

5.12.1 Fragen der Ausländerbehörde zum Verhältnis zwischen Rechtsanwalt und Mandant

Im Rahmen der Prüfung eines Visumantrages zum Ehegattennachzug legte die zuständige Ausländerbehörde dem hier lebenden Ehepartner einen 22-seitigen Fragebogen „Entscheidungshilfe in den Fällen des Ehegattenachzugs“ vor, mit dessen Hilfe das Vorliegen einer Scheinehe als Versagungsgrund einer Aufenthaltserlaubnis nach § 27 Abs. 1a Nr. 1 AufenthG ermittelt werden sollte. Dem im Ausland lebenden Ehepartner wurde der gleiche Fragebogen von der zuständigen Auslandsvertretung zur Beantwortung vorgelegt. Aufgrund von insgesamt sieben Fragen, welche das Verhältnis der Ehepartner zu ihrem Rechtsanwalt betrafen, wandte sich dieser mit der Bitte um Prüfung an mich. Die Ausländerbehörde wollte etwa wissen, weshalb sich die Ehepartner durch einen Rechtsanwalt vertreten ließen, von wem dieser ggf. empfohlen wurde und wer dessen Kosten begleiche.

Auch wenn die Betroffenen nicht zur Beantwortung dieser Fragen verpflichtet waren, sind solche Fragestellungen, die das Verhältnis des Verfahrensbeteiligten zu seinem Rechtsanwalt betreffen, grundsätzlich rechtswidrig. Denn mit der Auswahl und Bestellung einer anwaltlichen Vertretung üben die Verfahrensbeteiligten lediglich ihr gesetzliches Recht (§ 14 VwVfG, § 3 Abs. 3 BRAO) auf ein rechtsstaatliches Verfahren aus. Daher verbietet es sich aus eben dieser Rechtsausübung nachteilige Schlussfolgerungen zu ziehen. Die mit der Beantwortung der Fragen verbundene Datenerhebung war somit zur Aufgabenerfüllung nicht erforderlich und daher unzulässig, § 12 Abs. 1 SächsDSG. Zudem liegt die Zuziehung eines Rechtsanwalts grundsätzlich auch im objektiven Interesse der Behörde, da sie in der Regel das Verwaltungsverfahren erleichtert und ein rechtsstaatliches Verfahren garantiert.

Im Rahmen der Kontrolle teilte die Ausländerbehörde mir mit, dass es keinen behördeneinheitlichen Fragebogen zum Ehegattennachzug gebe. Keiner der gebräuchlichen Fragebögen enthalte Fragen zum Verhältnis der Verfahrensbeteiligten zu ihrem Rechtsanwalt. Lediglich eine Sachbearbeiterin, die inzwischen die Ausländerbehörde verlassen habe, habe einzig in dem zugrunde liegenden Fall Fragen zum Mandatsverhältnis gestellt. Meine Rechtsauffassung würde vorbehaltlos geteilt. Es habe sich um einen Einzelfall gehandelt. Die Bediensteten seien nochmals auf die Unzulässigkeit derartiger Fragen hingewiesen worden.

Ich habe danach auf eine förmliche Beanstandung verzichtet und es bei einer Rüge belassen. Außerdem habe ich die Ausländerbehörde aufgefordert, die unzulässig erho-

benen und gespeicherten Daten gemäß § 21 Abs. 5 SächsDSG zu sperren. Eine Löschung der Daten kommt nach § 20 Abs. 2 SächsDSG derzeit noch nicht in Betracht.

5.12.2 Akteneinsicht in Ausländerakten

Das Recht auf Akteneinsicht der Beteiligten im ausländerrechtlichen Verfahren hat mich auch in diesem Berichtszeitraum wieder beschäftigt, wie nachfolgendes Beispiel zeigt.

Die zuständige Ausländerbehörde hatte mehrere Seiten der Hauptakte unter dem Hinweis auf „personenbezogene Daten Dritter“ aus dieser entfernt und in eine Nebenakte aufgenommen, welche dem Beteiligten im Rahmen seiner Akteneinsichtnahme nicht zugänglich war. Die entnommenen Seiten enthielten personenbezogene Daten der Ehefrau des Beteiligten, namentlich Auskünfte aus dem amtlichen Melderegister im Wesentlichen über deren aktuelle und frühere Wohnanschrift. Die Ausländerbehörde begründete die insoweit teilweise versagte Akteneinsicht mir gegenüber damit, dass diese Melderegisterauskünfte Daten enthielten, die über die Daten einer einfachen Meldeauskunft hinausgingen. Sie ging offenbar aufgrund dessen von einem überwiegenden Geheimhaltungsinteresse der Ehefrau aus, welche dem Recht auf Akteneinsicht des Ehemanns entgegenstünde.

Dieser Ansicht konnte ich mich nicht anschließen. Zutreffend beinhalteten die Seiten zwar personenbezogene Daten (etwa frühere Anschriften), die eine einfache Melderegisterauskunft nach § 32 SächsMG nicht enthalten würde. Das Sächsische Meldegesetz gibt jedoch nicht den Beurteilungsmaßstab vor, an dem der Ausnahmetatbestand der berechtigten Interessen Dritter zu prüfen wäre, welcher eine Versagung der Akteneinsicht nach § 29 Abs. 2 VwVfG oder § 18 Abs. 5 Nr. 3 SächsDSG rechtfertigen könnte. Im Unterschied zum Melderegisterauskunftsverfahren gilt es im Rahmen der Akteneinsichtsvorschriften grundsätzlich die Rechtsposition des Akteneinsichtersuchenden als Verfahrensbeteiligten zu berücksichtigen. Die Akteneinsicht dient dem Beteiligten zur Ausübung seiner Rechte und muss daher bei der vorzunehmenden Abwägung zwischen dem Geheimhaltungsinteresse des Dritten und dem Informationsinteresse des Verfahrensbeteiligten besondere Berücksichtigung finden. Im Hinblick auf die in diesem Fall konkret in den entnommenen Aktenseiten enthaltenen Daten der Ehefrau und deren persönliches Verhältnis zum Akteneinsichtersuchenden (Ehemann) berücksichtigend, vermochte ich insofern aber bereits ein besonderes Geheimhaltungsinteresse nicht zu erkennen, auch wenn im Zeitpunkt der erfolgten Akteneinsicht davon auszugehen war, dass die Eheleute getrennt lebten. Überdies verfing auch der Hinweis auf die einfache Melderauskunft in der Sache nicht. Denn bereits mit der erweiterten Melderegisterauskunft nach § 32a SächsMG, für die lediglich ein berechtigtes Interesse glaub-

haft gemacht werden muss, wird u. a. auch Auskunft über frühere Anschriften des Betroffenen erteilt.

Ich habe die Ausländerbehörde auf die insoweit rechtswidrige Versagung der Akteneinsicht hingewiesen und sie aufgefordert, diese Seiten wieder in die Hauptakte aufzunehmen und die ausgeübte Praxis hinsichtlich der Gewährung der Akteneinsicht kritisch zu überdenken. Dem kam die Behörde anstandslos nach.

5.13 Wahlrecht

In diesem Jahr nicht belegt.

5.14 Sonstiges

5.14.1 Verfahren der Zuverlässigkeitsüberprüfung nach dem Luftsicherheitsgesetz (LuftSiG)

Im Berichtszeitraum war ich erneut (vgl. 13./5.14.1) mit mehreren Fragen der Zuverlässigkeitsüberprüfung nach dem Luftsicherheitsgesetz befasst.

Sport- und Berufspiloten, Flughafenpersonal und alle anderen, die aus beruflichen Gründen Zutritt zu Sicherheitsbereichen in Flughäfen erhalten sollen, werden regelmäßig auf ihre Zuverlässigkeit hin überprüft. Rechtsgrundlage sind das Luftsicherheitsgesetz und die Luftsicherheits-Zuverlässigkeitsüberprüfungsverordnung (LuftSiZÜV).

Zuverlässigkeitsüberprüfungen nach § 7 LuftSiG werden in Sachsen zentral durch die Landesdirektion Dresden durchgeführt. Die Neuansiedlung eines großen Frachtunternehmens am Flughafen Halle/Leipzig sowie der Neubau der Start- und Landebahn am Flughafen Dresden ließ - so wurde uns im vorangegangenen Berichtszeitraum durch das Regierungspräsidium Dresden erläutert - viele Überprüfungsanträge erwarten. Um diese in angemessener Zeit bearbeiten zu können und um Mehrfacherfassungen zu vermeiden, sollten die Antragsdaten durch die Betreibergesellschaften der Flughäfen erhoben und an die LD Dresden übermittelt werden. Ich habe deutlich gemacht, dass die Betreibergesellschaften durch das Luftsicherheitsgesetz nicht ermächtigt worden sind, personenbezogene Daten der Antragsteller zum Zweck der Zuverlässigkeitsüberprüfung zu erheben. In Betracht käme lediglich, dass die Betreibergesellschaften die Daten der Antragsteller als Auftragnehmer der LD nach § 7 SächsDSG erheben und übermitteln. Die LD bliebe für die Einhaltung der datenschutzrechtlichen Vorschriften verantwortlich und hätte die Betreibergesellschaften 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 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 (Arbeitnehmerdaten).

Die LD Dresden hat schließlich von der Möglichkeit einer Datenerfassung durch die Betreibergesellschaften der Flughäfen Abstand genommen.

Die LD Dresden als zentrale sächsische Luftsicherheitsbehörde darf des Weiteren bei Polizei und Verfassungsschutz Daten zu den Betroffenen erheben. Da die Zuverlässigkeitsüberprüfungen erst nach fünf Jahren wiederholt werden, ist in § 7 Abs. 9 LuftSiG ab dem 11. Januar 2007 neuerdings im Zusammenhang mit der geänderten Beurteilung der Sicherheitslage im Luftraum eine Nachberichtspflicht der Verfassungsschutzbehörden der Länder vorgeschrieben. Danach muss der Verfassungsschutz Erkenntnisse, die er innerhalb der fünf Jahre erlangt, der Luftsicherheitsbehörde nachmelden. Problem aus Sicht des Datenschutzes: Zu diesem Zweck muss der Verfassungsschutz nunmehr - anders als früher - die Daten der zuverlässigkeitsüberprüften Personen mit seinen aktuellen Daten verknüpfen. Dies geschieht durch die Aufnahme dieser Personen in das bundesweite „Nachrichtendienstliche Informationssystem“ NADIS, in das alle Verfassungsschutzbehörden von Bund und Ländern Daten eingeben und abrufen. Eine vergleichbare Situation besteht für den Bereich der Sicherheitsüberprüfungen. Bereits in den vergangenen Jahren erfolgten fast ca. 60% der Eintragungen im NADIS aufgrund von Sicherheitsüberprüfungen. Dieser Prozentsatz wird sich durch die zusätzlichen Zuverlässigkeitsüberprüfungen erhöhen.

Ich habe das LfV gebeten, besonderes Augenmerk auf die Zweckbestimmung, auf eine Protokollierung der Zugriffe sowie auf die Speicherdauer und Löschung dieser Daten zu legen.

5.14.2 Verwendung von Auskünften des LKA Sachsen durch ein kommunales Ordnungsamt

Der Datenschutzbeauftragte einer sächsischen Stadt fragte, ob die Informationen, die das LKA Sachsen unter ausdrücklichem Hinweis auf ihre „Gerichtsverwertbarkeit“ dem Ordnungsamt seiner Stadt über einen bestimmten Anmelder einer Veranstaltung sowie sein Umfeld, also Dritte, übermittelt hatte, so auch in die Begründung der Verbotsverfügung hätten übernommen werden dürfen. Dabei bezogen sich seine Bedenken wohl darauf, dass der Anmelder und Adressat der Verbotsverfügung (Anmelder) hierdurch

Informationen zu den dritten Personen aus seinem Umfeld erhalten konnte, die er möglicherweise vorher nicht hatte.

Ich habe wie folgt geantwortet:

Die Übermittlung durch das LKA an das Ordnungsamt bemaß sich mangels einer bereichsspezifischen Vorschrift für die Übermittlung personenbezogener Daten durch die Polizei an eine andere öffentliche Stelle ausschließlich nach § 14 SächsDSG. Diese Voraussetzungen lagen hier vor. Die Informationen des LKA waren für das städtische Ordnungsamt zur substantiierten Begründung der Verbotsverfügung erforderlich, d. h. zwingend notwendig; die Voraussetzungen einer zulässigen zweckändernden Verarbeitung lagen vor. Verbotsverfügungen müssen insbesondere so substantiiert abgefasst sein, dass der Anmelder notfalls gerichtlich dagegen vorgehen kann; dies ist eine sich aus dem Rechtsstaatsprinzip ergebende Forderung.

Die Feststellung des LKA, dass die aufgeführten Erkenntnisse gerichtsverwertbar seien, betraf ausschließlich Gründe der Geheimhaltung. Darüber zu entscheiden oblag ausschließlich dem LKA.

Aus Sicht des Datenschutzes geht es in solchen Fällen darum, zu verhindern, dass das Recht auf informationelle Selbstbestimmung der dritten Personen aus dem Umfeld des Anmelders so weit wie möglich gewahrt wird. Der Anmelder darf nicht durch die Verbotsverfügung Kenntnis von personenbezogenen Daten Dritter erhalten, die er zuvor nicht hatte. Dagegen können die zur Person des Anmelders übermittelten Erkenntnisse (selbstverständlich) in der an ihn gerichteten Verbotsverfügung verarbeitet werden. Insofern handelte es sich quasi um eine Auskunft über die zu seiner Person gespeicherten Daten, die grundrechtlich nicht nur unproblematisch, sondern sogar begrüßenswert ist.

Differenziert muss dagegen die Verwendung von Daten zu Dritten, mit denen der Anmelder in einem sachlichen oder persönlichen Zusammenhang steht, beurteilt werden. Im vorliegenden Fall hatte der Anmelder immer wieder Handys dritter Personen genutzt. Diesen Umstand hatte das LKA jeweils mit Nennung des Namens der Dritten dargelegt. Diese Daten wiesen einen deutlichen Bezug auch zur Person des Anmelders auf und dürfen m. E. unproblematisch in der Verbotsverfügung genannt werden. Anders dagegen die darüber hinausgehenden Angaben zu eigenständigen Aktivitäten dieser Dritten, die keinen Bezug auch zur Person des Anmelders aufwiesen, z. B. die Information, dass einer der Dritten „über das genannte Telefon … sämtliche Aktivitäten der Organisation in seinem Zuständigkeitsbereich … organisierte und koordinierte“. Diese Daten beziehen sich ausschließlich auf die jeweilige Person des Dritten; sie sind nicht

zugleich auch Daten des Anmelders. Ihre Übermittlung an den Anmelder hat daher aus Datenschutzgründen zu unterbleiben.

Für die ausweislich der Begründung der Verbotsverfügung ebenfalls herangezogenen Informationen des LfV, die mir nicht vorlagen, gilt Entsprechendes. Auch hier darf zur Wahrung des Datenschutzes möglichst nur die Information zur Substantiierung der Verbotsverfügung herangezogen werden, die sich auf den Anmelder bezieht. Der Anmelder darf nicht - quasi über den Umweg der Begründung der Verbotsverfügung - Kenntnis von den zu anderen als seiner Person gespeicherten Daten des LfV oder des LKA erhalten.

6 Finanzen

6.1 Fehlerhafter Rückversand von Belegen im Einkommenssteuerverfahren

Im Berichtszeitraum sind mir mehrere Einzelfälle bekannt geworden, in denen Belege, die von Steuerpflichtigen im Rahmen ihrer Jahreseinkommenssteuererklärung eingereicht worden waren, von Finanzämtern versehentlich Dritten rückversandt worden sind. Die jeweils Betroffenen erhielten ihre Unterlagen durch diese Dritten zurück, reichten Dienstaufsichtsbeschwerden ein und riefen mich nach § 24 SächsDSG als Kontrollbehörde an. Die Finanzämter teilten mir mit, dass sie sich bereits entschuldigt hätten, ihre Bediensteten erneut auf die auch in Routinevorgängen gebotene Sorgfalt hingewiesen und den behördlichen Datenschutzbeauftragten unterrichtet hätten.

Ich habe daraufhin von einer förmlichen Beanstandung dieser - soweit ersichtlich - Einzelfälle abgesehen. Dies erschien mir trotz des hohen Gewichts des Steuergeheimnisses (§ 30 AO) vertretbar, da den Betroffenen jeweils kein Schaden entstanden war und sie ihre Unterlagen zurückerhalten hatten. Sollten sich jedoch solche Verstöße in einem Finanzamt wiederholen oder sollte einem Betroffenen daraus ein Schaden entstehen, würde ich dies zu beanstanden haben.

6.2 Fördermittelvergabe durch die Sächsische Aufbaubank

Die Anfrage einer Gemeinde zur Verfahrensweise der Sächsischen Aufbaubank (SAB) bei der Vergabe von Fördermitteln veranlasste mich, die Verarbeitung personenbezogener Daten bei der Vergabe von Fördermitteln durch die Bank zu kontrollieren. Nach dem mir in Kopie vorgelegten Formular der SAB für Unterschriftsproben/Zeichnungsbefugnisse verlangte die Bank vom Antragsteller die Kopie des Personalausweises (Vorder- und Rückseite) jeder der auf dem Formular aufgeführten Personen, soweit der Antragsteller nicht in einem öffentlichen Register eingetragen ist (und ein Registerauszug beigefügt werden kann), aus dem sich die Legitimation der zur Stellvertretung berechtigten Personen ergibt.

Seitens der Gemeinde wurde diese Verfahrensweise mit Blick auf die personenbezogenen Daten der Beschäftigten als unangemessen angesehen.

Eine Bank als Kreditinstitut hat Name und Anschrift des Inhabers und des Verfügungsberechtigten eines Kontos zu speichern. Das Kreditinstitut muss sich Gewissheit über Personen und Anschriften Verfügungsberechtigter verschaffen. Als Rechtsgrundlagen sind § 24c Abs. 1 KWG i. V. m. § 154 Abs. 2 Satz 1 AO maßgeblich. Jedes Verfahren zur Legitimationsprüfung (auch ein persönliches Erscheinen und Ausweisen des Betrof-

fenen bei der Bank) kann den datenschutzrechtlichen Anforderungen nur gerecht werden, wenn es sich ausschließlich auf die Erhebung der erforderlichen Daten beschränkt. Durch die gesetzliche Regelung nicht gedeckt sind die mit der Vorlage der Kopie des Personalausweises zusätzlich erhobenen Daten wie Körpergröße, Augenfarbe etc.

Ich halte im Falle von Förderanträge stellenden Gebietskörperschaften und deren Vertretern eine Legitimationsprüfung anhand eines Vergleichs der Daten des Antrags mit denen eines aktuellen Registerauszuges für die betroffene Gebietskörperschaft als Legitimationsnachweis in der Regel für ausreichend.

In Ihrer Stellungnahme wies die SAB darauf hin, dass sie, um eine gesetzeskonforme Geschäftstätigkeit zu gewährleisten, verbindliche Arbeitsanordnungen für die Mitarbeiter erlassen habe. Darunter die Arbeitsanordnung 2460-6 „Legitimationsprüfung und Feststellung des wirtschaftlich Berechtigten bei der Eröffnung von Kredit- und Zuschusskonten“.

In dieser mir vorgestellten Arbeitsanordnung wird unter Punkt 1.1.3 „Zuschüsse im Direktgeschäft“ geregelt, abweichend vom Kreditgeschäft Angaben über Art, Nummer und ausstellende Behörde des amtlichen Ausweises nicht zu erheben, sofern Gewissheit über die Identität des Kunden besteht. Spezielle Festlegungen trifft Punkt 4.2 „Vertreter von juristischen Personen des öffentlichen Rechts“: „Bei Vertretern juristischer Personen des öffentlichen Rechts (einschließlich Eigenbetriebe) kann auf eine Legitimationsprüfung verzichtet werden, es sei denn, es bestehen begründete Zweifel an der Identität … Auf die Unterschriftsprobe und die Ausweiskopie kann in der Regel verzichtet werden, wenn aufgrund der der SAB bekannten Umstände glaubhaft ist, dass die Person, die gegenüber der SAB als Verfügungsberechtigter auftritt, die zur Vertretung bestellte Person (z. B. Bürgermeister, Verbandsgeschäftsführer, sonstige Personen) ist.“

Die SAB versichert in ihrer Stellungnahme, dass in der betroffenen Abteilung hinsichtlich der Verwaltungspraxis in Bezug auf die Identifizierungspflichten die entsprechenden Vorgaben der Arbeitsanordnung befolgt werden und Ausweiskopien nicht abverlangt werden. Jedoch wird eingeräumt, der Vordruck „Unterschriftsproben/Zeichnungsbefugnisse“ könnte den Eindruck vermitteln, dass Kopien erforderlich wären, da dieser auch für andere Geschäftsvorfälle Verwendung findet, bei denen Kopien wegen der Identifizierungspflicht tatsächlich angefordert werden.

Um zukünftig Missverständnisse bei den Antragstellern zu vermeiden sicherte die SAB zu, zur Klarstellung auf dem Vordruck „Unterschriftsproben/Zeichnungsbefugnisse“ eine Fußnote anzubringen, die einen Hinweis auf das Entfallen der an anderer Stelle

gegebenenfalls abverlangten Kopie des Personalausweises für die gesetzlichen Vertreter von Anstalten und Körperschaften des öffentlichen Rechts enthält.

6.3 Datenpanne im Finanzamt

In einem sächsischen Finanzamt rief ein Mann an, der sich als „Herr Müller“ von der OFD ausgab und eine Bedienstete des Finanzamtes um Auskunft über Steuerdaten eines Ehepaares bat. Der Anrufer teilte das zutreffende Geburtsdatum eines der Eheleute mit. Außerdem nannte er eine unzutreffende Anschrift, von der er behauptete, sie in dem internen Namensabfragesystem der Finanzverwaltung ermittelt zu haben. In der Annahme, bei dem Anrufer handele es sich um eine in der OFD tätige Person, erteilte ihm die Bedienstete am Telefon Auskünfte über Steuernummer, Anschrift, familiäre Verhältnisse, Bankverbindung, letzte Veranlagung, eventuell vorhandene Steuerrückstände, Einkünfte und Einzelheiten zu angemeldeten Kraftfahrzeugen. Wegen darüber hinaus begehrter einkommenssteuerlicher Auskünfte verwies die Bedienstete den Anrufer an die zuständige Sachbearbeiterin und nannte deren Telefonnummer. Kurze Zeit später rief derselbe Anrufer diese Sachbearbeiterin an, stellte sich wiederum als Mitarbeiter der OFD vor und bat unter Angabe von Geburtsdaten und der ihm zuvor offenbarten Steuernummer um weitere Auskünfte zu dem Ehepaar. Auf Nachfrage, wofür er diese benötige, erklärte er, ihm liege eine Berichtsaufforderung vor. Die Sachbearbeiterin teilte ihm, auch sie in der Annahme, bei dem Anrufer handele es sich um einen Beschäftigten der OFD, weitere Einzelheiten zu den verschiedenen Einkünften des Ehepaares sowie zu deren persönlichen Verhältnissen mit.

Als die Bedienstete am folgenden Tag versuchte, den Anrufer unter der von ihm hinterlassenen Durchwahl zurückzurufen, stellte sie fest, dass weder die mitgeteilte Durchwahl noch der Mitarbeiter bei der OFD existierten.

Das Finanzamt teilte den Sachverhalt sogleich der OFD mit, dessen Präsident das Ehepaar noch am selben Tag über den Vorfall in Kenntnis setzte und den Sachverhalt bei der zuständigen Staatsanwaltschaft anzeigte.

Ich habe das Finanzamt wegen der unzulässigen Übermittlung dem Steuergeheimnis unterliegender personenbezogener Daten an eine nicht-öffentliche Stelle beanstandet.

Die OFD hat den Vorfall zum Anlass genommen, die Beschäftigten der sächsischen Finanzämter nochmals eingehend schriftlich auf die notwendigen Vorsichtsmaßnahmen bei telefonischen Anfragen hinzuweisen. Insbesondere wurden die Beschäftigten belehrt, dass

- zur zweifelsfreien Feststellung der Identität eines Anrufers in der Regel ein Rückruf oder vergleichbare Maßnahmen erfolgen sollen,
- die Rufnummernanzeige im Telefondisplay keinen zweifelsfreien Identitätsnachweis erbringen kann,
- Kenntnisse über den Zweck der Datenübermittlung und die funktionale Zuständigkeit des Anrufers einzuholen sind und
- Betroffene im Fall einer unzulässigen Datenübermittlung unverzüglich in Kenntnis zu setzen sind.

Der Vorfall zeigt auch, wie betroffenenfreundlich und verantwortungsbewusst eine Behörde mit einer eingetretenen selbstverschuldeten Datenpanne umgehen sollte.

7 Kultus

7.1 Schulverwaltungssoftware SaxSVS

Bereits im letzten Berichtszeitraum hatte ich über die Schulverwaltungssoftware SaxSVS berichtet, 13/7.1.

Im aktuellen Berichtszeitraum kontrollierte meine Behörde die Datenverarbeitung beim beauftragten Dienstleister der öffentlichen Stelle in Kamenz und konnte dabei eine Zwischenbilanz ziehen.

Bis Ende des Jahres 2009 ist beabsichtigt, neben Grund- und Mittelschulen auch die Gymnasien mit dem Verfahren auszustatten. Weiterhin lege ich großen Wert darauf, dass das Verfahren auf die äußeren, die Verwaltungsdaten der Schüler, Eltern, Lehrer und sonstigen Betroffenen beschränkt bleibt und keine Zeugnisdaten in dem Verfahren verarbeitet werden. Eine profilhafte, zu umfassende Datenverarbeitung bin ich nicht bereit mitzutragen. Die berufsbildenden Schulen sind an dem Verfahren nicht beteiligt. Für diese soll ein spezielles Verfahren zum Einsatz kommen, das aber noch nicht beauftragt worden ist. Auch nicht beteiligt an dem System sind die Schulen in freier Trägerschaft bzw. Privatschulen.

Die Kontrolle des relationalen Datenbanksystems von SaxSVS verlief in Bezug auf den Datenschutz und die Datensicherheit zufriedenstellend. In der Datenbankzentrale selbst konnten keine Schülerdaten bezogen werden. Schülerdaten können nur an der jeweiligen Schule selbst zugänglich gemacht werden. Simuliert werden konnte der Zugriff auf Bediensteten-, insbesondere Lehrerdaten aus Sicht der personalverwaltenden Bildungsagentur. Die Zugriffsberechtigungen waren in Umfang und Tiefe angemessen geordnet. Datensicherheitslücken konnten nicht festgestellt werden. Automatisierte Löschroutinen sollen allerdings noch vorgesehen werden. Insoweit ist das Verfahren noch ausbaufähig.

Perspektivisch soll an jeder Schule ein sicherer Anschluss über ein Subnetz des Landes eingerichtet werden, auch um das Verfahren SaxSVS an den Schulen datensicher einzusetzen. Aus Datensicherheitsgründen halte ich dies auch für erforderlich. Die Kontrolle der Anwendung des Verfahrens im Schulbereich durch meine Behörde wird in einem nächsten Schritt erfolgen.

8 Justiz

8.1 Fachverfahren forumSTAR - zentrale Datenbank in Sachsen tätiger Rechtsanwälte

Bereits im vergangenen Berichtszeitraum bat mich die Rechtsanwaltskammer Sachsen, eine Körperschaft des öffentlichen Rechts, im Wege einer Vorabprüfung die Zulässigkeit einer regelmäßigen Übermittlung ihrer Mitgliederdaten an das SMJus zum Zwecke der Errichtung einer zentralen Datenbank aller in Sachsen zugelassenen und tätigen Rechtsanwälte namens forumSTAR zu prüfen. Die geplante Datenbank solle im Rahmen eines Entwicklungsverbundes zusammen mit Bayern, Baden-Württemberg und Rheinland-Pfalz errichtet werden und sei nach Auskunft des SMJus ein Hilfsmittel für die gerichtliche Verfahrensbearbeitung. ForumSTAR sehe neben bestimmten Pflichtdaten zur Person des Rechtsanwalts und seiner Kanzlei (Name, Anrede etc.) auch optionale Datenfelder zur Anschrift, zu Telekommunikations- und Bankverbindungen etc. vor. Auf längere Sicht solle diese Datenbank wohl die bisher auf Grundlage der jeweiligen Prozessordnung bei den Instanzgerichten geführten Rechtsanwalts-Listen ersetzen.

Mit dem beschriebenen Verfahren erhebt das SMJus personenbezogene Daten der Rechtsanwälte bei einem Dritten, namentlich der Rechtsanwaltskammer. Dies ist nach § 12 Abs. 1 und 4 Nr. 1 und 2 SächsDSG nur zulässig, wenn eine Rechtsvorschrift dies ausdrücklich vorsieht oder die Betroffenen wirksam eingewilligt haben. Zudem müssen die so erhobenen Daten zur Aufgabenerfüllung des SMJus erforderlich sein; die Justizverwaltung dürfte ohne Kenntnis der Daten ihre Aufgaben nicht, nicht rechtzeitig oder nicht vollständig erfüllen können. An diesen Voraussetzungen fehlte es: Für mich ist aus den Prozessordnungen oder der Bundesrechtsanwaltsordnung keine gesetzliche Befugnis ersichtlich, auf welche die Datenübermittlung durch die Rechtsanwaltskammer gestützt werden könnte. Damit verbliebe einzig die Möglichkeit einer auf die schriftliche Einwilligung der Betroffenen gestützten Datenverarbeitung. Hinzu kommt: Die gerichtliche Verfahrensbearbeitung wäre ohne die Aktualisierung von forumSTAR mit Hilfe der Rechtsanwaltskammer nicht unmöglich. Dabei verkenne ich nicht die Zweckdienlichkeit einer solchen Aktualisierung; sie genügt jedoch nicht dem strengen Erforderlichkeitsgrundsatz des § 12 Abs. 1 SächsDSG.

Das SMJus teilte daraufhin mit, dass noch vertiefend zu prüfen sei, ob die Datensätze der Rechtsanwaltskammer zur Aktualisierung genutzt werden könnten oder ob die Daten jeweils anlässlich eines neu eingehenden Verfahrens eingepflegt werden müssten.

8.2 Auskunftserteilung aus Finanzgerichtsakten an die Landesjustizkasse

Die Beitreibung der Gerichtskosten ist in Sachsen zentral der Landesjustizkasse Chemnitz (LJK) übertragen, § 29b SächsJOrgVO i. V. m. § 1 JBeitrO. Sie ist daher auch für die Beitreibung der Gerichtskosten finanzgerichtlicher Verfahren zuständig.

In diesem Zusammenhang unterrichtete mich das Sächsische Finanzgericht darüber, dass die LJK in Fällen, in denen die Kostenschuldner nicht freiwillig die festgesetzten Gerichtskosten entrichten, beim Finanzgericht anfragt, ob sich aus den finanzgerichtlichen Akten des Erkenntnisverfahrens Näheres über die Einkommens- und Vermögensverhältnisse der Kostenschuldner, insbesondere über das Vorhandensein pfändbarer Ansprüche, ergibt. Der Präsident gab zu bedenken, dass die Erteilung derartiger Auskünfte durch seine Mitarbeiter das Steuergeheimnis nach § 30 AO verletzen könnte, wenn das Verfahren der Kostenerhebung und -beitreibung kein Teil des *gerichtlichen Verfahren(s) in Steuersachen* i. S. v. § 30 Abs. 2 Nr. 1 Buchst. a AO wäre, da in diesem Fall die Übermittlung von Steuerdaten an die LJK nicht mehr von der Offenbarungsbefugnis des § 30 Abs. 4 Nr. 1 AO getragen sei. Er wies insoweit vor allem darauf hin, dass sich der statthafte Rechtsbehelf gegen eine Kostenrechnung aus dem Gerichtskostengesetz (hier: [Erst-]Erinnerung nach § 66 GKG) statt aus der Finanzgerichtsordnung ergebe, was dafür sprechen könne, dass sich das Verfahren der Kostenerhebung und -beitreibung vielleicht nicht als Teil des *gerichtlichen Verfahren(s) in Steuersachen* i. S. v. § 30 Abs. 2 Nr. 1 Buchst. a AO anzusehen sei. Zudem treibe die LJK auch Kosten anderer, finanzgerichtswegfremder Verfahren bei. Die Nutzung der aus Finanzgerichtsakten erteilten Auskünfte sei jedenfalls dann mit einer Zweckänderung verbunden, welcher es aber ersichtlich an der erforderlichen Rechtsgrundlage fehle.

Nach eingehender Prüfung teilte ich dem Finanzgericht mit, dass meiner Auffassung nach die Beitreibung der Gerichtskosten eines finanzgerichtlichen Verfahrens ein Teil eben dieses Verfahrens und somit eines *gerichtlichen Verfahren(s) in Steuersachen* i. S. v. § 30 Abs. 2 Nr. 1 Buchst. a AO ist und die Übermittlung von dem Steuergeheimnis unterfallenden Daten aus Finanzgerichtsakten an die LJK zum Zwecke der Beitreibung dieser Gerichtskosten datenschutzrechtlich daher nicht zu beanstanden ist, da dies von der Offenbarungsbefugnis des § 30 Abs. 4 Nr. 1 AO getragen wird. (So wohl auch die im Schrifttum vorherrschende Ansicht; vgl. Tipke/Kruse, AO, § 30 Rdnr. 69; Klein, AO, 9. Aufl., § 30 Rdnr. 77; Bilsdorfer, DStZ 1993, 295.)

Auch der Umstand, dass sich der statthafte Rechtsbehelf gegen eine Kostenrechnung nicht aus der finanzgerichtlichen Verfahrensordnung selbst, sondern aus dem Gerichtskostengesetz ergibt, vermag gegen diese Ansicht wohl eher nicht zu sprechen. Denn

gemäß § 66 Abs. 1 GKG bleibt das Gericht für die Entscheidung über den statthaften Rechtsbehelf der (Erst-)Erinnerung zuständig, bei dem die Kosten angesetzt worden sind, mithin das Finanzgericht bzw. der Bundesfinanzhof. Der Gesetzgeber hat sich lediglich dafür entschieden, ein für eine Vielzahl von Gerichtsverfahren geltendes, vereinheitlichtes Gerichtskostengesetz (§ 1 GKG) zu erlassen, anstatt das Kostenverfahren in jeder einzelnen Verfahrensordnung separat zu regeln. Daher muss das sich anschließende Kostenverfahren meines Erachtens auch als Teil des jeweils vorangegangenen gerichtlichen Erkenntnisverfahrens angesehen werden. Die Beitreibung von Ansprüchen aus dem finanzgerichtlichen Erkenntnisverfahren ist damit Teil des *gerichtlichen Verfahren(s) in Steuersachen* i. S. v. § 30 Abs. 2 Nr. 1 Buchst. a AO.

Zutreffend weist das Finanzgericht darauf hin, dass der LJK mitgeteilte Daten aus Finanzgerichtsakten nicht auch für die Beitreibung anderer, finanzgerichtswegfremder Ansprüche nutzen darf. Die Auskunftserteilung aus Finanzgerichtsakten zu derart anderen Zwecken wird von der Offenbarungsbefugnis des § 30 Abs. 4 Nr. 1 AO nicht umfasst; eine solch zweckändernde Verwertung verstößt gegen § 30 Abs. 2 Nr. 1 Buchst. a AO.

Dies steht der Auskunftserteilung zum Zwecke der Beitreibung von Gerichtskosten im Finanzgerichtsverfahren jedoch nicht entgegen. Denn die mit der Auskunftserteilung übermittelten, weiterhin dem Steuergeheimnis nach § 30 AO unterliegenden Daten werden nicht an die LJK als Organisationseinheit im Ganzen übermittelt, sondern nur an die organisatorische Teileinheit, welche die Aufgabe „Beitreibung von Ansprüchen aus Finanzgerichtsverfahren“ erfüllt. Dem Datenschutzrecht liegt insofern und im Hinblick auf dessen Schutzzweck der sogenannte *funktionale Stellenbegriff* zugrunde, wonach sich die Zulässigkeit der Datenverarbeitung allein an den Aufgaben der Daten verarbeitenden Stelle ausrichtet (Dammann in Simitis, BDSG, 6. Aufl., § 2 Rdnr. 142 und § 3 Rdnr. 227; Bergmann/Möhrle/Herb, Datenschutzrecht, § 3 BDSG Rdnr. 152 ff.). Sobald also die übermittelten Daten von der LJK im Rahmen einer anderen Aufgabe oder Funktion verwendet werden, handelt es sich auch um getrennte Stellen. Der LJK obliegt es insoweit gemäß § 9 Abs. 1 Satz 1 SächsDSG *alle angemessenen personellen, technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind*, um sicherzustellen, dass die erteilten Auskünfte aus Finanzgerichtsakten eben auch nur im Rahmen der Beitreibung von Ansprüchen aus Finanzgerichtsverfahren genutzt werden. Dies kann meiner Auffassung nach dadurch erreicht werden, dass für die Beitreibung von Ansprüchen aus unterschiedlichen Gerichtswegen jeweils eigene organisatorische Teileinheiten eingerichtet werden, die eigene Kassenakten führen.

Im Sinne des Datenschutzes habe ich das Finanzgericht gebeten, die LJK im Rahmen der Auskunftserteilung aus Finanzgerichtsakten vorbeugend darauf hinzuweisen, dass

die insoweit übermittelten Daten gemäß § 30 Abs. 2 Nr. 1 Buchst. a AO ausschließlich zur Beitreibung von Ansprüchen aus Finanzgerichtsverfahren verwertet werden dürfen. Mir verbleibt es nunmehr zu prüfen, ob die LJK die nach § 9 SächsDSG erforderlichen Maßnahmen zur Gewährleistung des Steuergeheimnisses getroffen hat.

8.3 Staatsanwaltschaftsinterne Bekanntgabe der Auflagen, Geldbeträge zugunsten bestimmter gemeinnütziger Einrichtungen zu zahlen

Im Berichtszeitraum wurde mir bekannt, dass jeder Staatsanwalt programmgestützt auf die Daten seiner Kollegen zugreifen kann, aus denen sich ergibt, in welcher Höhe und zu wessen Gunsten diese nach § 153a Abs. 1 StPO Beschuldigte mit der Zahlung von Geldbeträgen beauflagt haben. Welcher Geldbetrag an welche Einrichtung dabei zu zahlen ist, liegt im Ermessen des zuständigen Staatsanwalts.

Sowohl die Generalstaatsanwaltschaft als auch das SMJus schlossen sich meiner Rechtsauffassung an, wonach die personenbezogene Zuordnung staatsanwaltschaftlich angeordneter Geldauflagen einzig für den Behördenleiter zur Ausübung der ihm obliegenden Dienstaufsicht erforderlich ist. Allen anderen Beschäftigten ist der Zugriff auf diese Daten infolge der nicht gegebenen Erforderlichkeit für die Erfüllung ihrer Aufgaben (Erforderlichkeitsgrundsatz) vorzuenthalten.

Nach Auskunft der Generalstaatsanwaltschaft lassen sich die entsprechenden Zugriffsrechte im Programm web.sta.3 jedoch nicht ohne Weiteres beschränken. Notwendig sei vielmehr eine Umprogrammierung, die zwar in Auftrag gegeben worden, deren Umsetzung aber zeitlich schwer einzuschätzen sei. Die Generalstaatsanwaltschaft hat mir zugesagt, mich in dieser Angelegenheit über erfolgte Änderungen zu informieren.

8.4 Setzt der Beschluss eines Ermittlungsrichters über die Statthaftigkeit einer Ermittlungsmaßnahme der datenschutzrechtlichen Kontrolle der Staatsanwaltschaft hinsichtlich der Durchführung eben dieser Ermittlungsmaßnahme Grenzen?

Die datenschutzrechtliche Kontrolle einer beabsichtigten Durchsicht eines beim Beschuldigten sichergestellten Datenbestandes nach § 110 StPO - die im Ergebnis nicht zu beanstanden war - warf die Frage auf, ob der Beschluss des zuständigen Ermittlungsrichters, der die Durchsicht für statthaft erklärte und deren zeitnahe Vollstreckung ausdrücklich anmahnte, eine Bindungswirkung gegenüber der Staatsanwaltschaft entfaltet, aufgrund derer die Staatsanwaltschaft auch für den Fall zur Vollstreckung der für statt-

haft erklärten Maßnahme berufen ist, dass ich diese Ermittlungsmaßnahme datenschutzrechtlich für unzulässig hielte.

Insofern stellte die Staatsanwaltschaft in Frage, ob es über die gerichtliche Entscheidung zur Zulässigkeit der Durchsicht der sichergestellten Daten hinaus überhaupt noch einen Regelungsgehalt gibt, aus dem sich weitergehende Einschränkungen datenschutzrechtlicher Art ergeben könnten. Sie bekundete die Auffassung, die Gerichtsentscheidung zur Statthaftigkeit der Durchsicht sei abschließend und erschöpfe auch diejenigen Anforderungen vollumfänglich, welche sich aus datenschutzrechtlichen Bestimmungen ergäben. Der sich aus der Gerichtsentscheidung daher ergebenden Bindungswirkung würde sich die Staatsanwaltschaft unterwerfen.

Dieser Argumentation vermochte ich mich indessen nicht anzuschließen. Die Tätigkeit der Staatsanwaltschaft unterliegt trotz eines richterlichen Beschlusses über die Zulässigkeit einer Ermittlungsmaßnahme weiterhin meiner Kontrolle. Die Einschränkung des § 27 Abs. 4 SächsDSG (keine datenschutzrechtliche Kontrolle unmittelbar der Rechtsprechung dienender Tätigkeiten) greift hier nicht, auch ordnet das Gericht nicht den Vollzug der Ermittlungsmaßnahme selbst an. Die Durchführung der Maßnahme steht trotz des Gerichtsbeschlusses vielmehr weiterhin im pflichtgemäßen Ermessen der Staatsanwaltschaft. Dabei verkenne ich nicht, dass aus dem strafprozessrechtlichen Legalitätsprinzip für die Staatsanwaltschaft eine Verpflichtung erwachsen kann, die gerichtlich für statthaft erklärte Ermittlungsmaßnahme durchzuführen. Dies namentlich dann, wenn etwa wegen weiterem zeitlichen Aufschub deren zukünftige Unverhältnismäßigkeit zu besorgen ist und daher die Verletzung des Legalitätsprinzips droht. Eine sich aus dem Gerichtsbeschluss unmittelbar ergebende Bindungswirkung, welcher sich die Staatsanwaltschaft zu unterwerfen habe, ergibt sich meines Erachtens aber nicht. Eine solche Bindungswirkung kann sich allenfalls aus höchstrichterlicher Rechtsprechung ergeben (Meyer-Goßner, StPO, 50. Aufl., Vor § 141 GVG Rdnr. 11 m. w. N.).

Ich sehe mich daher grundsätzlich nicht gehindert, die Durchführung einer gerichtlich für statthaft erklärten staatsanwaltschaftlichen Ermittlungsmaßnahme gegebenenfalls datenschutzrechtlich zu beanstanden.

8.5 Vorlage von Personalausweiskopien Angehöriger bei Verlegungsanträgen Gefangener

Ein Gefangener stellte einen Antrag auf Verlegung in eine andere JVA und rechtfertigte seinen Verlegungsantrag mit der dort besseren Realisierung seiner Kontakte zu Angehörigen (§ 8 Abs. 1 Nr. 1 StVollzG). Die Strafvollzugsanstalt forderte den Gefangenen zum Nachweis des Verlegungsgrundes zur Vorlage der Kopien der Personalausweise

seiner dort lebenden Angehörigen auf und nahm diese Kopien sodann auch zur Gefangenenpersonalakte. Der Gefangene wandte sich mit der Bitte um Prüfung an mich, ob diese Verfahrensweise datenschutzrechtlich zulässig sei.

Ich habe der JVA daraufhin mitgeteilt, dass ich die Vorlage und Speicherung der Personalausweiskopien in der Gefangenenpersonalakte zur Erfüllung ihrer Aufgabe, Prüfung des Verlegungsantrages, für nicht erforderlich erachte. Der Vollzugsanstalt stehen andere, weniger in das Grundrecht auf informationelle Selbstbestimmung sowohl des Gefangenen als auch seiner Angehörigen eingreifende Beweismittel zur Verfügung. So etwa die namentliche Benennung der Angehörigen mit Adressen und ggf. Telefonnummern. Dies ermöglicht der Vollzugsanstalt durch Vergleich mit den Daten aus der Gefangenenpersonalakte oder durch Einholung einfacher Auskünfte (Telefonbuch, Kontrollanruf, einfache Melderegisterauskunft) die Überprüfung der Angaben, auf die sich der Verlegungsantrag stützt. Für den Fall, dass diese Möglichkeiten ausnahmsweise nicht zum Nachweis des Verlegungsgrundes ausreichen sollten, erachte ich die bloße Vorlage und Zurkenntnisnahme der Ausweiskopien als noch zulässig; deren Zuraktennahme jedoch nicht, da insoweit ein einfacher Aktenvermerk in der Art „Richtigkeit der Angaben durch Vorlage der Ausweiskopien nachgewiesen“ völlig ausreicht.

Die JVA teilte daraufhin mit, dass die Vorlage von Ausweiskopien künftig nicht mehr erbeten werde und in dem betreffenden Fall zur Gefangenenpersonalakte genommene Kopien aus dieser entfernt und vernichtet worden seien.

8.6 Überwachung des geschützten Schriftverkehrs in den Justizvollzugsanstalten

Die Beanstandung einer JVA wegen Verstoßes gegen das Überwachungsverbot bezüglich eingehender Schreiben eines Landtagsabgeordneten (§ 29 Abs. 2 Satz 3 StVollzG), warf die Frage auf, ob der nach § 29 StVollzG geschützte Schriftverkehr auch bei so genannten Zellenrevisionen grundsätzlich von der Kontrolle ausgenommen sein muss.

Nach § 30 Abs. 3 StVollzG hat der Gefangene *eingehende Schreiben unverschlossen zu verwahren, soweit nichts anderes gestattet wird; er kann sie verschlossen zu seiner Habe geben*. Dies ist grundsätzlich auch sachgerecht, da in verschlossenen Umschlägen verbotene Gegenstände versteckt und so der Kontrolle der Bediensteten entzogen werden könnten. Den Gefangenen verbleibt es, eine Kontrolle zu vermeiden, indem sie die Schreiben verschlossen zu ihrer Habe geben. Aber auch im Rahmen des § 30 Abs. 3 StVollzG muss die vom Gesetzgeber in § 29 StVollzG getroffene Wertung Berücksichtigung finden. Dieser hat in Kenntnis einer möglichen Missbrauchsgefahr und unter Abwägung der widerstreitenden Interessen sich in § 29 StVollzG bewusst gegen

jegliche Überwachung (Sicht- und Inhaltskontrolle) des geschützten Schriftverkehrs entschieden. Dementsprechend haben die Gerichte in ständiger Rechtsprechung der Posteingangskontrolle strengste Maßstäbe auferlegt (beispielhaft OLG Frankfurt B. v. 23. Oktober 2003, 3 Ws 897/03 und 898/03), um auszuschließen, dass Vollzugsbedienstete bewusst oder unbewusst auch nur Bruchstücke des Inhaltes der Schreiben wahrnehmen können, wie dies bereits bei einer bloßen Sichtkontrolle nach unerlaubten Gegenständen regelmäßig der Fall ist. Für mich ist kein nachvollziehbarer Grund ersichtlich, weshalb diese gesetzgeberische Wertung und die sich daraus ergebenden Maßstäbe der Posteingangskontrolle bei Kontrollen in den Hafträumen nicht gelten sollten. Auch würde anderenfalls das Überwachungsverbot des § 29 StVollzG unterlaufen werden, denn schon die bloße Sichtung tangiert bereits den Bereich der Inhaltskontrolle. Diese Auffassung wird meines Erachtens auch mehrheitlich in der einschlägigen Literatur vertreten (Calliess/Müller-Dietz, StVollzG, 10. Aufl., § 30 Rdnr. 2; Joester/Wegner in Feest (Hrsg.), StVollzG, 5. Aufl., § 30 Rdnr. 4; Schwind/Böhm, StVollzG, 4. Aufl., § 30 Rdnr. 4 mit Einschränkungen). Indessen hält das SMJus die Sichtkontrolle im Rahmen der Zellenrevision für uneingeschränkt zulässig und beruft sich insoweit vor allem auf Arloth/Lückemann, StVollzG, § 30 Rdnr. 5, und Teile der Rechtsprechung (Kammergericht Berlin, B. v. 23. Mai 2003, 5 Ws 99/03 Vollz; OLG München, B. v. 30. September 2006, 3 Ws 902, 903/06 R; OLG Koblenz, B. v. 15. Juli 2007, 1 Ws 243/07).

Ich habe dem SMJus mitgeteilt, dass ich auch künftig an meiner Rechtsauffassung festhalten und entsprechende Verstöße, wenn nötig, beanstanden werde.

Vielleicht ist aber auch eine allen Seiten gerecht werdende Kontrollpraxis nach der von Schwind (in Schwind/Böhm, StVollzG, 4. Aufl., § 30 Rdnr. 4) vertretenen Auffassung möglich, wonach eine Sichtkontrolle des geschützten Schriftverkehrs bei Zellenrevisionen ausnahmsweise in den Fällen zulässig sein sollte, in denen eine konkrete Gefahr des Missbrauchs des Überwachungsverbotes seitens des Gefangenen besteht.

8.7 Gesetzliche Regelung der Aufbewahrung von Schriftgut der Justiz

Im Nachgang des Gesetzentwurfs der länderoffenen Arbeitsgruppe zur Regelung der Aufbewahrungsbestimmungen (Schriftgutaufbewahrungsgesetz), welches in der 78. Justizministerkonferenz einstimmig zur Kenntnis genommen wurde, obliegt es nun den einzelnen Ländern, ein entsprechendes Gesetz und die erforderliche Rechtsverordnung zur Regelung der Aufbewahrungsfristen zu erlassen.

Das SMJus hat mir auf meine Anfrage, welche Verfahrensweise insoweit beabsichtigt sei, mitgeteilt, dass aus Gründen der Deregulierung auf ein eigenständiges Gesetz verzichtet werden soll. Der Regelungsgehalt würde sich auf eine Rechtsverordnungsermächtigung beschränken. Deshalb sei vorgesehen, diese Ermächtigung in das Sächsische Justizgesetz aufzunehmen. Für die danach zu erlassende Rechtsverordnung sei nach Abwägung aller Vor- und Nachteile vorgesehen, die bundeseinheitlichen Regelungen der Aufbewahrungsbestimmung zu übernehmen und auf abweichende oder ergänzende Regelungen der einzelnen Aufbewahrungsfristen zu verzichten.

Ich werde im Rahmen des sich anschließenden Gesetzgebungsverfahrens darauf achten, ob so auch verfahren wird.

8.8 Übersendung von (psychiatrischen) Gutachten an die Justizvollzugsanstalten

Im Berichtszeitraum erhielt ich Kenntnis davon, dass die Justizvollzugsanstalten daran interessiert sind, von den Staatsanwaltschaften *unaufgefordert* vorliegende (psychiatrische) Gutachten aus Strafverfahren zu erhalten. Dies sollte im Einzelfall sowohl einen Beitrag zum Erreichen des Vollzugsziels leisten, als auch der Sicherheit und Ordnung in den Justizvollzugsanstalten dienen.

Dem Ansinnen trat ich zunächst gegenüber der Generalstaatsanwaltschaft mit der Bitte entgegen, wegen des Fehlens der dazu erforderlichen gesetzlichen Grundlage davon abzusehen.

Die einschlägige spezielle Rechtsvorschrift des § 31 Abs. 2 StVollStrO erlaubt die Übersendung von psychiatrischen Gutachten nur im Einzelfall unter strengen Voraussetzungen. Sowohl die jeweilige Vollzugsanstalt als auch die jeweilige Staatsanwaltschaft müssen dazu im Einzelfall prüfen, ob eine Anforderung bzw. Übersendung von Gutachten aus Strafakten „*für den Vollzug von Bedeutung sein kann*“, also erforderlich ist oder nicht. Dabei müssen sie berücksichtigen, dass es sich um besonders heikle personenbezogene Daten über den (psychiatrischen) Zustand des Gefangenen handelt, die aufgrund der EG-Datenschutzrichtlinie einem besonderen Schutz unterfallen (vgl. § 4 Abs. 2 SächsDSG). Gegen eine anlasslose generelle Übersendung von Gutachten aus Strafakten spricht zudem deren früherer Erstellungszeitpunkt (Aktualität) und die Frage, inwieweit sie in der gerichtlichen Hauptverhandlung überhaupt Bestand gehabt haben (Validität). Meine Argumentation überzeugte: Die Generalstaatsanwaltschaft teilte danach sowohl den Leitenden Oberstaatsanwälten als auch dem SMJus mit, „*dass die Staatsanwaltschaften ihnen vorliegende psychiatrische Gutachten über Inhaftierte den Justizvollzugsanstalten nicht unaufgefordert zur Verfügung stellen werden, sondern*

dass eine (auszugsweise) Übersendung von derartigen Gutachten von einer Prüfung des Einzelfalls abhängig gemacht werden muss“.

Das SMJus vertrat daraufhin gegenüber der Generalstaatsanwaltschaft die Auffassung, die Übersendung sei unabhängig vom Einzelfall auch generell zulässig. Einer besonderen Ermächtigungsgrundlage für die Übersendung von Gutachten bedürfe es zumindest in demselben Strafverfahren nicht, da die Vollstreckung einer Freiheitsstrafe Bestandteil des Strafverfahrens sei.

Dieser Rechtsauffassung musste ich entgegentreten. Der Strafvollzug gehört nicht zum Vollstreckungsverfahren im engeren Sinne und daher auch nicht zum Strafverfahren (Meyer-Goßner, StPO, 48. Aufl., Einl. Rdnr. 68; Pfeiffer in Karlsruher Kommentar, StPO, 5. Aufl., Einl. Rdnr. 54 ff.). Während die Strafvollstreckung, d. h. bei Freiheitsstrafen die Herbeiführung des Strafantritts und die Überwachung der Urteilsdurchsetzung, als letzter Teil des Strafverfahrens angesehen wird, steht der Strafvollzug selbst außerhalb des Strafverfahrens. Die Verwendung von psychiatrischen Gutachten im Strafvollzug erfolgt daher auch nicht mehr innerhalb des Erhebungszwecks „Strafverfahren“. Daher bedarf auch die Übermittlung von Gutachten an die Justizvollzugsanstalten einer eigenen Ermächtigungsgrundlage. Eine solche gibt es aber jedenfalls für die Übermittlung in demselben Strafverfahren unabhängig von einer Einzelfallprüfung (§ 31 Abs. 2 StVollstrO) nicht.

Das SMJus hielt grundsätzlich an seiner Rechtsauffassung fest, teilte aber mit, dass die Übersendung von psychiatrischen Gutachten durch Staatsanwaltschaften an die Justizvollzugsanstalten nur nach einer Prüfung im Einzelfall erfolgen werde. In bestimmten Fallgruppen (Sexual- oder Gewalttäter) - so das SMJus in einem Schreiben an die Generalstaatsanwaltschaft - solle aber die Bedeutung des Gutachtens für den Strafvollzug regelmäßig gegeben sein, eine Übersendung des Gutachtens nur in Einzelfällen unterbleiben können. Ich bat das SMJus daraufhin, gegenüber der Generalstaatsanwaltschaft klarzustellen, dass in jedem Fall eine ergebnisoffene Prüfung des Einzelfalls zu erfolgen hat. Das Erfordernis einer durch Rechtsvorschrift vorgegebenen Einzelfallprüfung ist angesichts der besonders schutzbedürftigen personenbezogenen Daten mit einer schematischen Betrachtung unvereinbar. Das SMJus bestätigte mir, dass auch in den genannten Fallgruppen die Strafvollstreckungsbehörde eine Beurteilung im Einzelfall vorzunehmen habe.

Damit bleibt es letztlich bei der mir zuvor durch die Generalstaatsanwaltschaft zugesagten Verfahrensweise.

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

Der größte Reihengentest in der Geschichte der Bundesrepublik Deutschland (vgl. 13/8.3) konnte am 17. Juni 2008 mit der Festnahme eines dringend Tatverdächtigen abgeschlossen werden. An diesem Tag erhielt die von einer Sonderkommission zu einer Ermittlungsgruppe herabgestufte „EG Heller“ aus dem Untersuchungslabor die Mitteilung, dass eine am 21. Mai 2008 außerplanmäßig genommene Speichelprobe eine vollständige Übereinstimmung des DNA-Identifizierungsmusters mit der Täter-DNA aufwies.

Tatsache ist, dass die Polizei, nachdem sie die Betroffenen mit Wohnsitz im engeren Umkreis des vermuteten Tatorts ergebnislos untersucht hatte, am Ende eine aus dem Fahrzeugregister ermittelte Gruppe von Haltern von Fahrzeugen mit dem Buchstabenfragment „DD-D“ (diesen Hinweis gab ein Zeuge) sozusagen rückwärts mit einem weiteren vermuteten Merkmal, namentlich dem früheren Wohnsitz im Bereich des Tatortes, abgeglichen hat. Dabei kam nach Information durch das LKA der Täter als einziger heraus. Da dieser zudem eine der im August 2007 durch Abgleich der 127.000 Einwohnermeldeamts-Datensätze mit einer polizeilichen Datenbank herausfiltrierten ca. 15.000 Personen war, bestand nun Übereinstimmung bei einem Ansatzpunkt (frühere polizeiliche Auffälligkeit [Unfallflucht]) und zwei Merkmalen: Kfz-Kennzeichen und ehemalige Anschrift in der Nähe des Tatortes. Daraufhin suchten ihn die Polizisten am 21. Mai 2008 auf, er gab die Speichelprobe ab und wurde im normalen Verlauf der Probenuntersuchung am 17. Juni 2008 identifiziert. Allerdings wäre er im Rahmen der DNA-Reihenuntersuchung zum 31. Mai/1. Juni 2008 ohnehin eingeladen worden.

Hieraus wird deutlich, dass der Täter durch klassische kriminalistische Arbeit (Eingrenzung des Täterkreises durch Rasterung bestimmter bekannter oder vermuteter Merkmale) ermittelt wurde, wenn auch die im Zusammenhang mit dem Reihengentest gewonnenen Erkenntnisse mittelbar dazu beigetragen haben.

Die Tatsache, dass letztlich die Schwerpunktbildung (Rasterfahndung durch Abgleich der von den Einwohnermeldeämtern übermittelten Personen mit den in polizeilichen Auskunftssystemen bereits vorhandenen Tätern) dazu geführt hat, den mittels DNA-Probe zu überprüfenden Personenkreis einzuengen und somit überschaubar zu machen, zeigt, dass es erforderlich ist, vor der Durchführung eines solchen Verfahrens den Personenkreis einzugrenzen und somit auch das Mittel des Reihengentests effizient (und grundrechtsschonend) zu gestalten.

Der Gesamtablauf spricht eher gegen den (vorschnellen) Einsatz sehr großer Reihengentests. Hierdurch werden Kapazitäten gebunden, und es besteht die Gefahr, dass die normale Ermittlungsarbeit vernachlässigt wird. Auch der konkrete Verlauf, wonach 19 Monate nach Beginn noch nicht mal 10 % der von den Einwohnermeldeämtern gemeldeten Männern mit Wohnort in der Nähe des Tatortes getestet worden waren, zeigt, dass dies kein geeignetes Verfahren bei Massenanwendung ist. Denn neben dem hiermit verbundenen hohen personellen und finanziellen Aufwand ist die zu bewältigende Datenmenge für die Ermittler kaum handhabbar.

Auf die Erforderlichkeit der Schwerpunktsetzung mit Eingrenzung des zu untersuchenden Personenkreises bzw. Abschichtung nach bestimmten priorisierten Merkmalen habe ich bereits frühzeitig (s. 13/8.3) und auch während des gesamten Verfahrens hingewiesen.

Im Hinblick auf die gesetzlichen Anforderungen der Erforderlichkeit und Verhältnismäßigkeit kann der Reihengentest im Übrigen nur eine außergewöhnliche und selten anzuordnende Maßnahme sein. Sie kommt grundsätzlich nur in Betracht, falls alle anderen Ermittlungsmethoden erfolglos geblieben sind (ultima ratio).

Nachdem der Spurenverursacher festgestellt worden war und ein Geständnis abgelegt hatte, habe ich das Verfahren zur unverzüglichen Löschung der Aufzeichnungen über die durch die Maßnahme festgestellten DNA-Identifizierungsmuster der ca. 14.000 Probanden, mit Ausnahme von Personen, die gegen die Strafverfolgungsbehörden Beschwerde erhoben oder Ansprüche geltend gemacht haben, begleitet. Die beim LKA vorhandenen Unterlagen (komplette Datenbank zum Reihengentest sowie begleitende Akten) wurden im Oktober 2008 gelöscht bzw. vernichtet. Die Speichelproben sowie die DNA-Identifizierungsmuster wurden - wie gesetzlich gefordert - ohnehin unmittelbar nach der Verformelung bzw. nach dem negativen Abgleich mit der Täter-DNA vernichtet.

1. Das war das erste Massengentestverfahren nach dem Inkrafttreten des neuen § 81h StPO. Ich habe dieses Verfahren von Anfang an begleitet, auch mit der erklärten Absicht, dass alle Beteiligten aus Fehlern lernen und wir einen Rahmen schaffen, der zukünftig angewendet werden kann.

2. In diesem Zusammenhang möchte ich mich beim LKA Sachsen sowie bei der Staatsanwaltschaft Dresden noch einmal für meine frühzeitige Einbindung in das Verfahren sowie die fortlaufenden Informationen bedanken.

3. Das hierbei entwickelte Verfahren kann einschließlich der Formulare - insbesondere das Einladungsschreiben mit umfänglichen Erläuterungen und die Einwilligungserklärung - als Maßstab für künftige Vorgänge gelten.

8.10 Anbringung von Hauben zum Telefonieren in den Justizvollzugsanstalten

Ein Petent wandte sich u. a. mit folgendem Vortrag an mich: Er sitze derzeit in einer sächsischen JVA ein. Auf seiner Station gebe es auf dem Gang einen Telefonapparat zur Nutzung durch die Gefangenen. Die örtlichen und baulichen Verhältnisse seien jedoch so, dass ein ungestörtes und vertrauliches Telefongespräch nicht möglich sei. Er könne nicht telefonieren, ohne dass Mitgefangene dies - gewollt oder ungewollt - mithörten.

Meine Ermittlungen haben diesen Vortrag im Wesentlichen bestätigt. Der Apparat war an der Wand befestigt, eine Haube oder eine andere Einrichtung, die das (ungewollte) Mithören von Telefongesprächen durch Mitgefangene verhindert hätte, war nicht vorhanden. Da die Stationswände aus einem harten ungedämmten Material bestehen, war die akustische Situation tatsächlich so, dass ein Telefonat auch einige Meter entfernt mitgehört werden konnte. Dies hatte im konkreten Fall zu erheblichen Konsequenzen geführt, denn der Petent hatte bei einem seiner Telefonate eine tätliche Auseinandersetzung mit einem Mitgefangenen, der ihm beim Telefonieren zu nahe kam und von dem er sich gestört fühlte. Er wurde deshalb erneut und schwer verurteilt.

Klar ist: Telefongespräche Gefangener können der gesetzlich geregelten Überwachung durch die Anstalt unterliegen. Dann darf ein Bediensteter im Auftrag der Anstaltsleitung inhaltlich mithören, was der Gefangene am Telefon bespricht. Solche Eingriffe in das Fernmeldegeheimnis (Art. 10 GG) sind, soweit sie verhältnismäßig bleiben, durch das Interesse an einem reibungslosen Vollzug der Freiheitsstrafe und der Prävention von weiteren Straftaten gerechtfertigt. Keine Rechtfertigung gibt es dagegen für das Mithören von Telefonaten durch Mitgefangene. Im Gegenteil: Ein solches Mithören erschwert den zulässigen und für die Wiedereingliederung des Gefangenen erforderlichen Austausch von Gedanken und Meinungen mit Familienangehörigen, Freunden, Bekannten oder gar den gesetzlich besonders geschützten notwendigen Austausch mit dem Verteidiger. Das ungewollte Mithören von Mitgefangenen ist daher kontraproduktiv und, wie im Einzelfall des Petenten zu beobachten war, u. U. auch Anlass für erneute Straftaten.

Ich habe deshalb die Anstalt und das SMJus gebeten, Bedingungen zu schaffen, unter denen Gefangene ohne die Möglichkeit des Mithörens durch Mitgefangene telefonieren können. Dazu sind die Anstalten als öffentliche Gewalt verpflichtet.

Das SMJus und die JVA haben mich sachgerecht unterstützt; mein Anliegen wurde offen aufgenommen. Mittlerweile sind zumindest in der betreffenden JVA Hauben über den Telefonapparaten installiert worden, die ein ungestörteres Telefonieren ermöglichen. In den übrigen Justizvollzugsanstalten sollten ebenfalls Bedingungen für möglichst ungestörtes Telefonieren geschaffen werden, soweit dies nicht bereits geschehen ist.

9 Wirtschaft und Arbeit

9.1 Straßenverkehrswesen

9.1.1 Herausgabe von Kfz-Halterdaten an Private

Mehrfach erreichten mich Anfragen darüber, ob es rechtmäßig sei, dass eine Parkplatz betreibende private Firma wegen der Rechnungsstellung von Parkkosten Kfz-Halterdaten von der Kfz-Zulassungsbehörde erhalten darf.

Durch die örtliche Zulassungsbehörde oder das Kraftfahrt-Bundesamt ist die sogenannte einfache Registerauskunft nach § 39 Abs. 1 StVG zu erteilen, wenn der Empfänger unter Angabe des betreffenden Kennzeichens darlegt, dass er die Daten zur Geltendmachung, Sicherung oder Vollstreckung oder zur Befriedigung oder Abwehr von Rechtsansprüchen im Zusammenhang mit der Teilnahme am Straßenverkehr oder zur Erhebung einer Privatklage wegen im Straßenverkehr begangener Verstöße benötigt. Die zu übermittelnden Daten sind genau bestimmt.

Bei dem Rechtsanspruch auf Auskunftserteilung „im Zusammenhang mit der Teilnahme am Straßenverkehr“ genügt ein mittelbarer Zusammenhang. Es genügt, wenn das Fahrzeug auf einem Privatparkplatz abgestellt ist und das Fahrzeug dort z. B. einen Schaden verursacht oder selbst einen Schaden erleidet oder durch Gebrauch des Fahrzeugs sonst Rechte anderer verletzt werden (z. B. Eigentum, Besitz am Grundstück). Der Zusammenhang ist auch zu bejahen bei einer unbefugten Inanspruchnahme von Abstellplätzen auf Privatgelände (vgl. 1. Merkblatt für Anfragen und Auskünfte aus den Fahrzeugregistern nach § 39 Abs. 1 und 2 StVG v. 21. Juni 1993 (Verkehrsblatt Nr. 126, S. 525).

Die Zulassungsbehörden sind daher befugt, Halterdaten zu übermitteln, so dass der private Parkplatzbetreiber an den Kfz-Halter wegen entstandener Forderungen (Parkplatzkosten) herantreten kann.

Die Benutzung eines privat betriebenen Parkplatzes unterliegt allerdings dem Zivilrecht, auch wenn nicht seriöse Parkplatzbetreiber schon durch die optische Gestaltung ihrer Briefbögen, den Eindruck zu erwecken versuchen mögen, es ginge um Forderungen einer Gemeinde oder öffentlich-rechtliche Gebühren. Für die Zahlung der Benutzungsgebühr des Parkplatzes kommt es darauf an, wer konkret Vertragspartner der Betreiberfirma geworden ist und das ist in der Regel der Fahrzeugführer, der aber mit dem Fahrzeughalter nicht identisch sein muss.

9.1.2 Ungeschwärzte Speicherung von Bildabzügen aus Videoaufzeichnungen in der Verfahrensakte

Gegen einen Petenten leitete die Bußgeldstelle des zuständigen RP (nunmehr Landesdirektion) ein Verkehrsordnungswidrigkeitsverfahren wegen des Unterschreitens des gebotenen Mindestabstandes zum vorausfahrenden Fahrzeug ein. Im Rahmen des Verfahrens beantragte der Rechtsanwalt des Betroffenen Akteneinsicht. Dabei stellte er fest, dass die Bußgeldstelle der Akte ein Datenblatt beigefügt hatte, welches nicht nur die Messdaten der Abstandsmessung enthielt, sondern auch Bildabzüge aus der Videoaufzeichnung. Auf einem der Bildabzüge war der Beifahrer des Betroffenen zu erkennen. Eine mögliche Schwärzung unterließ die Behörde.

Auf meine Kontrolle hin rechtfertigte sich das RP damit, dass nach ihrem Dafürhalten die Akteneinsicht dem Betroffenen auch Aufschluss über in Betracht kommende Zeugen geben müsse. Daher sei der Beifahrer auf dem Bildabzug nicht geschwärzt worden. Zudem verwies das RP auf das Recht des Verteidigers auf Einsichtnahme in die tatsächlich unveränderbare Videoaufzeichnung der Abstandsmessung, bei der ebenfalls der Beifahrer zu erkennen sei. Da diese Videosequenzen unveränderbar seien, müssten auch die zur Akte genommenen Bildabzüge nicht geschwärzt werden. Anderenfalls sei das Akteneinsichtsrecht des Betroffenen tangiert.

Die Speicherung der Ablichtung des Beifahrers in der Verfahrensakte war unzulässig, da zur Aufgabenerfüllung der Bußgeldstelle - hier die Verfolgung einer Ordnungswidrigkeit gegen den Fahrer - nicht erforderlich, §§ 4, 13 SächsDSG (vgl. 4/5.9.10). Daran vermag auch der Umstand nichts zu ändern, dass aufgrund tatsächlich unveränderbarer Videosequenzen nicht zur Aufgabenerfüllung erforderliche personenbezogene Daten auf den Videobändern gespeichert und im Wege der Akteneinsicht möglicherweise Dritten bekannt werden. Denn § 13 Abs. 5 SächsDSG sieht explizit für den Fall, dass zur Aufgabenerfüllung erforderliche Daten mit nicht erforderlichen Daten des Betroffenen oder eines Dritten untrennbar verbunden sind, eine Rechtsgrundlage auch für deren Speicherung vor. Indessen ist die Löschung nicht erforderlicher Daten durch Schwärzung unproblematisch möglich, wenn Bildabzüge aus der Videoaufzeichnung zur Papierakte genommen werden. Aus datenschutzrechtlicher Sicht vermag ich sogar eine Pflicht der Verwaltungsbehörde dahingehend zu erkennen, entsprechend geschwärzte Bildabzüge zur Papierakte zu nehmen und nur dann Einsicht auch in die unveränderbaren Videoaufnahmen zu gewähren, wenn die zur Akte genommenen Bildabzüge dem Recht auf umfassende Akteneinsicht bzw. dem Anspruch auf rechtliches Gehör nicht genügen sollten (ähnlich Göhler, OWiG, 14. Aufl., § 60 Rdnr. 49 a. E.). Die nicht erfolgte Schwärzung des Beifahrers in der Verfahrensakte begründet daher

einen datenschutzrechtlichen Verstoß unabhängig davon, ob der Beifahrer weiterhin durch die Einsichtnahme in die Videoaufzeichnung erkennbar ist.

Das RP schloss sich meiner Rechtsauffassung an und sicherte mir die künftige Schwärzung des Beifahrers auf den zur Akte genommenen Datenblättern ebenso zu, wie die kritische Prüfung der Voraussetzungen einer Akteneinsicht in die unveränderbaren Videoaufnahmen.

9.1.3 VEMAGS - Verfahrensmanagement Großraum- und Schwertransporte

Das bundesweit für eine Zusammenarbeit der Genehmigungsbehörden nach §§ 29, 46 StVO vorgesehene und in Sachsen wie in anderen Ländern im Rahmen eines vorläufigen Betriebs zur Vorbereitung des Regelbetriebs eingesetzte IT-Verfahren VEMAGS bedarf für den Regelbetrieb einer normenklaren gesetzlichen Grundlage. VEMAGS ist eine länderübergreifende Datei mit automatisiertem Abrufverfahren, die gegenwärtig aufgrund einer Verwaltungsvereinbarung zwischen den Ländern betrieben wird. Für einen dem Schutz personenbezogener Daten gerecht werdenden Betrieb von VEMAGS ist eine gesetzliche Regelung vorzugsweise durch Festlegungen im Straßenverkehrsgesetz - wie sie vom *Arbeitskreis Verkehr der Datenschutzbeauftragten des Bundes und der Länder* empfohlen worden ist, zwingend erforderlich. Allein der Hinweis des SMWA auf die federführende Leitung bei der Einführung des Verfahrens durch ein anderes Bundesland befugt nicht zu einer personenbezogenen Datenverarbeitung im Freistaat Sachsen, § 4 Abs. 1 SächsDSG. Die unklare Rechtslage, das zeigen an mich gerichtete Anfragen, führt zu einer Verunsicherung der zur Anwendung von VEMAGS aufgeforderten sächsischen Behörden, die um einen gesetzmäßigen Verwaltungsvollzug bemüht sind. Vorstöße eines anderen Landes, das für entsprechende gesetzliche Ergänzungen des Straßenverkehrsgesetzes eintritt, haben sich noch nicht als erfolgreich herausgestellt. Auch eigene Initiativen des zuständigen sächsischen Staatsministeriums zur Schaffung der erforderlichen gesetzlichen Grundlage sind vor dem Hintergrund der schon jetzt mit dem vorläufigen Betrieb verbundenen Verarbeitung personenbezogener Daten notwendig. Sollten alle Bemühungen in dieser Richtung scheitern, ist die Datenverarbeitung seitens der sächsischen Behörden jedenfalls endgültig einzustellen.

9.1.4 Vollzug der Fahrerlaubnisverordnung: Weitergabe von Gesundheitsdaten an die Fahrerlaubnisbehörde

In einem mir bekannt gewordenen Vorgang teilte das Ordnungsamt einer Gemeinde als Verwaltungsbehörde im Sinne des Sächsischen Gesetzes über die Hilfen und die Unterbringung bei psychischen Krankheiten der im selben Amt angesiedelten Fahrerlaubnisbehörde unverlangt Bedenken gegen die körperliche oder geistige Eignung eines Be-

troffenen beim Führen von Kraftfahrzeugen mit. Zudem gab die Verwaltungsbehörde der Fahrerlaubnisstelle ein ärztliches Zeugnis bezogen auf den Betroffenen zur Unterbringung nach dem Sächsischen Gesetz über die Hilfen und die Unterbringung bei psychischen Krankheiten zur Kenntnis.

Von vergleichbaren Mitteilungen an die Fahrerlaubnisbehörden erhielt ich im letzten Berichtszeitraum mehrmals Kenntnis. Bei den Datenübermittlungen handelte es sich jeweils um einen Verstoß gegen den Grundsatz der informationellen Gewaltenteilung (vgl. BVerfGE vom 15. Dezember 1983 - 1 BvR 209/83, 1 BvR 269/83, 1 BvR 362/83, 1 BvR 420/83, 1 BvR 440/83, 1 BvR 484/83, Rdnr. 208).

Das Sächsische Datenschutzgesetz gilt unter anderem für die Verarbeitung personenbezogener Daten durch Behörden und sonstige öffentliche Stellen der Gemeinden. Gemäß § 4 Abs. 2 Nr. 1 SächsDSG ist die Verarbeitung personenbezogener Daten über die Gesundheit nur zulässig, wenn aus Gründen eines wichtigen öffentlichen Interesses eine besondere Rechtsvorschrift dies ausdrücklich vorsieht oder zwingend voraussetzt.

Die Fahrerlaubnisverordnung setzt zwar zwingend voraus, dass der Fahrerlaubnisbehörde Gesundheitsdaten über die Eignung zum Führen von Kraftfahrzeugen übermittelt werden, da unter anderem ihre Aufgabe auch die Entziehung der Fahrerlaubnis bei Nichteignung ist. Die Entziehung der Fahrerlaubnis steht auch im wichtigen öffentlichen Interesse, da damit der Schutz von Leben und Gesundheit der Öffentlichkeit verbunden ist. So ist z. B. gemäß § 3 Abs. 1 Satz 1 StVG i. V. m. § 46 Abs. 1 Satz 1 FeV die Fahrerlaubnis zu entziehen, wenn sich deren Inhaber als ungeeignet zum Führen von Kraftfahrzeugen erweist. Ungeeignet ist der Fahrerlaubnisinhaber auch, wenn psychische Störungen oder Erkrankungen vorliegen, die eine Eignung zum Führen eines Kraftfahrzeuges ausschließen.

Die Fahrerlaubnisbehörde darf ein ärztliches Zeugnis nach § 4 Abs. 2 Nr. 1 SächsDSG zur Akte nehmen, da die Verarbeitung von Gesundheitsdaten durch die Fahrerlaubnisverordnung ausdrücklich vorgesehen ist. So muss sie die ihr bekannt gewordenen Tatsachen, die Bedenken gegen die körperliche oder geistige Eignung eines Fahrerlaubnisinhabers dokumentieren, zur Akte nehmen (§ 11 Abs. 2 FeV), um dann ggf. Maßnahmen zur Klärung von Eignungszweifeln ergreifen zu können.

Vorgenanntes betrifft aber lediglich die Fahrerlaubnisbehörde als die *Daten empfangende Stelle*.

Aber auch die übermittelnde Stelle, im Ausgangsfall die Verwaltungsbehörde, hat ihre Datenverarbeitung auf eine gesetzliche Grundlage zu stützen. Zu beachten ist hier der

Sonderfall, dass die Informationen, die weitergegeben wurden, ursprünglich der ärztlichen Schweigepflicht unterlagen.

Da es keine spezielleren Datenverarbeitungsbestimmungen gibt, sind für die *Daten übermittelnde Stelle* das Sächsische Datenschutzgesetz und für den Fall, dass die Gesundheitsdaten aus einem Krankenhaus bezogen wurden, das Sächsische Krankenhausgesetz zu beachten. Nach § 14 Abs. 3 SächsDSG hat die Daten empfangende (und dann die Daten weiterübermittelnde) öffentliche Stelle die ihr übermittelten Daten nur für den Zweck zu verarbeiten, zu deren Erfüllung sie ihr übermittelt worden sind. Eine Zweckänderung, also eine Verarbeitung für andere Zwecke ist nur unter den Voraussetzungen des § 13 Abs. 2 SächsDSG zulässig, so unter anderem in den Fällen des § 12 Abs. 4 Nr. 6 und Nr. 7 SächsDSG (vgl. auch § 33 Abs. 3 Nr. 3 SächsKHG), d. h. z. B. in nothilfeähnlichen Situationen. Allerdings bestimmt § 14 Abs. 3 Satz 3 SächsDSG, dass, wenn die übermittelten Daten einem Berufs- oder besonderen Amtsgeheimnis unterliegen, ihre Verarbeitung für andere Zwecke nur zulässig ist, wenn die zur Verschwiegenheit verpflichtete Person oder Stelle eingewilligt hat. Weitergehender ist sogar die speziellere Vorschrift des § 33 Abs. 4 SächsKHG, die anzuwenden ist, wenn die Gesundheitsdaten aus einem Krankenhaus stammen. Im vorliegenden Fall war die Vorschrift missachtet, eine Einwilligung des Arztes nicht eingeholt worden bzw. die Verpflichtung, die Angaben - wie das Krankenhaus selbst - geheim zu halten, war nicht eingehalten worden. Ein Datenschutzverstoß lag damit vor, da auch Gefahrensituationen im Sinne von § 12 Abs. 4 Nr. 6 und Nr. 7 SächsDSG und § 33 Abs. 3 Nr. 3 SächsKHG nach meiner Überzeugung nicht zu bejahen gewesen waren.

Auch bei organisatorisch in einem Amt angesiedelten funktionalen Stellen nach dem Sächsischen Datenschutzgesetz sind die Zweckbestimmungen regelmäßig einzuhalten und sofern eine Zweckänderung erwogen wird, ist das tatbestandliche Vorliegen einer die Datenverarbeitung rechtfertigenden Zweckänderung sorgfältig zu prüfen. Die Zweckänderung ist eben die Ausnahme, nicht die Regel.

9.2 Gewerberecht

9.2.1 Zertifizierung durch den TÜV SÜD

Eine zum TÜV SÜD gehörende Service Gesellschaft verwendet für die Abwicklung ihrer Geschäfte ein Zertifizierungsformular „Schweißer-Prüfungsbescheinigung“. In dem Zertifikat ist in den Feldern Nr. 6 bis 10 die Ausweisung personenbezogener Daten des Bedieners von Schweißeinrichtungen vorgesehen, auf den das Zertifikat ausgestellt wird. Neben einem Passbild, dem vollständigen Namen, Geburtsdatum, Geburtsort und dem Arbeitgeber ist zur Legitimation auch die Angabe der Personalausweis- oder Pass-

nummer mit Benennung des dazugehörigen Dokuments anzugeben. Gegen den Umfang der Erhebung personenbezogener Daten wandte sich ein Betroffener.

Der TÜV SÜD nimmt als „benannte“ Stelle nach der Druckgeräterichtlinie (97/23/EG) bzw. „zugelassene“ Stelle nach § 11 GPSG die Prüfung von Bedienern von Schweißeinrichtungen vor. Er nimmt in diesem Rahmen staatliche Aufgaben wahr und handelt als Beliehener - und gilt damit als öffentliche Stelle im Sinne von § 2 Abs. 1 Satz 2 SächsDSG. Für die Verarbeitung personenbezogener Daten bei Behörden und sonstigen öffentlichen Stellen in Sachsen ist das Sächsische Datenschutzgesetz einschlägig, soweit keine spezielleren Bestimmungen greifen, § 2 Abs. 4 SächsDSG.

Soweit eine spezialgesetzliche Regelung die Datenerhebung im Zusammenhang mit der auf dem Formular „Zertifikat/Schweißer-Prüfungsbescheinigung“ übertragenen staatlichen Aufgabe im Einzelnen nicht zwingend vorschreibt, regelt sich die Erhebung personenbezogener Daten also nach § 12 SächsDSG. Nach § 12 Abs. 1 SächsDSG ist die Erhebung personenbezogener Daten nur zulässig, wenn ihre Kenntnis zur Erfüllung der Aufgaben der erhebenden Stelle erforderlich ist. Vorliegend ist der Umfang der erhobenen personenbezogenen Daten auf dem Formular zur Identifizierung des Betroffenen nicht erforderlich, da zur Identifizierung einer Person regelmäßig neben dem Namen und Vornamen der Tag und der Ort der Geburt ausreichen. Für die zusätzlich auf dem verwendeten Formular erhobenen Daten des zu Prüfenden: Arbeitgeber, Personalausweis- oder Passnummer mit Benennung des dazugehörigen Dokuments und Passbild, erscheint eine Erforderlichkeit nicht begründet.

In seiner Stellungnahme machte der TÜV SÜD darauf aufmerksam, dass die verwendeten Formulare den Vorgaben der DIN EN 287-1 entsprechen und gleichermaßen unverändert bei allen anderen anerkannten Zertifizierungsstellen Anwendung finden. Das Foto werde von der TÜV SÜD niemals, allerdings häufig vom Arbeitgeber der Schweißer gefordert.

Die DIN-Autoren wären aufgefordert, zur datenschutzgerechten Umsetzung die Verarbeitung personenbezogener Daten im Zusammenhang mit einer Schweißerprüfung Formulare datensparsam zu gestalten. DIN-Normen sind keine Gesetze und sind unter Berücksichtigung des Datenschutzrechts und einer Erforderlichkeit der Einzelangaben abzusetzen.

Leider ist im „zusammenwachsenden Europa“ durchaus verstärkt zu beobachten, dass unterschiedliche nationale Standards und eben auch datenschutzrechtliche Niveaus bei vereinheitlichten Standards zu einem geringeren Schutz personenbezogener Daten in Deutschland führen.

Den TÜV SÜD habe ich in seiner Haltung nur bestärken können, auch weiterhin kein Foto für das Zertifikat zu verlangen. Gegebenenfalls wären zusätzliche Informationen auch als nicht erforderliche Daten zurückzuweisen.

9.2.2 Weitergabe von Handwerkerdaten an einen Wettbewerbsverein

Mir sind mehrere Vorgänge vorgestellt worden, die in den Zuständigkeitsbereich einer Landkreisverwaltung fielen und in denen Handwerker durch das Ordnungsamt kontrolliert wurden. Als Inhaber gewerberechtlicher Erlaubnisse waren die Handwerker nicht berechtigt, bestimmte Werbemaßnahmen durchzuführen. Nach den Kontrollen durch das Ordnungsamt ergingen jeweils Bußgeldbescheide gegen die Betroffenen.

In der Folge erhielten die Betroffenen aber zusätzlich auch Abmahnungen eines Wettbewerbsvereins mit Sitz in Berlin. Hierin wurde den Betroffenen widerrechtliche Werbung vorgehalten und unter anderem auf Briefbögen hingewiesen, von denen in einem Fall nur einmalig Mitarbeiter des Landratsamtes oder der Industrie- und Handelskammer, die von der Landkreisverwaltung unter Beifügung des Vorgangs informiert worden war, Kenntnis haben konnten. Weiterhin wurde dem Betroffenen vorgeworfen, dass er diese Werbung auf seinen Briefbögen verwendet. Der Geschäftsbriefbogen wurde den Betroffenen durch den Wettbewerbsverein auch in Kopie übersandt.

Bis zum Ende des Berichtszeitraums konnte der Vorgang nicht insoweit aufgeklärt werden, dass die Urheberschaft von Mitarbeitern der Kammer oder des Landratsamtes für die Datenweitergabe belegt werden konnte. Für eine Weitergabe an einen Wettbewerbsverein gab es nach meiner Überzeugung jedenfalls keine Rechtfertigung. Im Gegenteil: Die amtlichen Vorgänge sind vertraulich zu behandeln. Es gelten die Amtsverschwiegenheit und das Datengeheimnis.

Vielmehr legt der Vorgang nahe, dass der Wettbewerbsverein bereichert, beziehungsweise die Handwerker durch die Abmahnkosten belastet und geschädigt werden sollte, § 39 i. V. m. § 38 Abs. 1 Nr. 1, 3 SächsDSG. Datenschutzverstöße können bei Hinzutreten gesetzlich genannter subjektiver Absichten strafbewehrt sein.

9.3 Industrie- und Handelskammern; Handwerkskammern

In diesem Jahr nicht belegt.

9.4 Offene Vermögensfragen

In diesem Jahr nicht belegt.

10 Gesundheit und Soziales

10.1 Gesundheitswesen

10.1.1 Nicht-Einführung der elektronischen Gesundheitskarte

Bereits in meinen vorangegangenen Tätigkeitsberichten hatte ich über die Elektronische Gesundheitskarte (eGK) und über Testmaßnahmen in Sachsen referiert, 12/10.1.2 und 13/10.1.1.

Wenig hat sich im Berichtszeitraum getan. Die Entwicklung der den Bürgern verordneten eGK und der anzupassenden Infrastruktur im Gesundheitswesen zieht sich hin. Im letzten Berichtszeitraum wurde seitens der gematik, der die Entwicklung koordinierenden Betriebsorganisation, ein übergreifendes Datenschutz- und Datensicherheitskonzept vorgestellt. Endlich.

Auch auf die vorgesehene Testphase der eGK in Sachsen durch SaxMediCard in der Testregion Löbau-Zittau bin ich bereits im 13. Tätigkeitsbericht eingegangen. In der Testregion Löbau-Zittau wurden im letzten Berichtszeitraum letztendlich an circa 11.000 Versicherte Gesundheitskarten ausgegeben. Von der ursprünglichen Vorstellung, einen Großtest in Sachsen mit 100.000 Anwendern durchzuführen, nahm man seitens der gematik Abstand. Getestet wurde das Auslesen von geschützten und ungeschützten Versichertenstammdaten von der eGK, das Erstellen, Transportieren und Einlösen einer Verordnung für apothekenpflichtige Arzneimittel (eRezept) - mit Ausnahme von Betäubungsmitteln - und das Ablegen, Auslesen, Aktualisieren und Löschen von Notfalldaten. Neben den Karten der Versicherten kamen u. a. Heilberufsausweise, Kartenlesegeräte und Konnektoren zur Integration vorhandener und hinzukommender Hard- und Software in den circa 25 Arztpraxen, 29 Apotheken und dem Krankenhaus zum Einsatz. Nach dem Abschlussbericht des Projektbüros wurden rund 19.000 Versichertenstammdatensätze gelesen und 3.400 eRezepte erstellt.

Bei den Tests stellten sich gewisse Schwierigkeiten bei der Einbindung der Arztpraxis-Systemhersteller heraus. Auch bei der Lieferung der Karten gab es immer wieder Verzögerungen. Unter anderem stellten sich die Freigabeverfahren der gematik als sehr langwierig und umständlich heraus.

Bei einem Kontrollbesuch des Projektbüros durch meine Behörde zum Ende des Berichtszeitraums vor Ort in einer Arztpraxis und einer Apotheke traten vielfältige Probleme mit dem elektronischen Rezept zutage. In dem elektronischen Verfahren konnten auch, wie von mir befürchtet, Prozessänderungen nicht in der notwendigen Flexibilität berücksichtigt werden. So konnten z. B. gängige Rücksprachen mit dem verordnenden Arzt in Bezug auf eine andere Medikamentenvergabe oder Fehler und Abweichungen

bei Artikelnummern, Packungsgrößen und in Referenzdatenbanken nicht berücksichtigt werden, so dass die Apotheker die Bearbeitungsprozesse über die Karte und das eRezept abbrachen und auf die herkömmlichen Systeme auswichen bzw. erforderliche Daten mit anderen Einleseverfahren herstellten. Softwaretechnische Probleme traten bei der Bearbeitung des eRezepts selbst auf. Weitgehend ungeklärt scheint zudem auch noch, wie bei Fehlverordnungen, Reklamationen und Nichtverfügbarkeit von Medikamenten verfahren werden kann. Hier scheint die Karte gegenüber der Papierform mehr Problem als Lösung zu sein. Durch die nicht reibungslosen Abläufe wurden die Kassen blockiert bzw. verlängerte sich der Zeitaufwand aufgrund doppelter Bearbeitungen. Bei den Ärzten wiederum findet das eRezept - so die Projektleitung SaxMediCard - wegen der schwer handhabbaren Stapelsignatur bzw. der Notwendigkeit von Pineingaben wenig Akzeptanz. Der Testverlauf im Krankenhaus war in Bezug auf das eRezept nicht entscheidend, hinsichtlich der Notfalldatensätze mangels Fallmengen nicht aussagefähig.

Seitens SaxMediCard wird im Abschlussbericht zu Release 1 (Seite 22 f.) zwischenzeitlich eine schriftliche Einwilligung des Versicherten in die freiwilligen Anwendungen der eGK (u. a. Notfalldatensatz, Medikamentenhistorie, elektronische Patientenakte) in der Arztpraxis in Frage gestellt. Eine schriftliche Einwilligung wird als „Zumutung“ betrachtet, da auch die Pineingabe durch den Versicherten im Prozess ausreichen solle. Die Ausführungen bleiben insofern - abgesehen von der Sicherstellung einer tatsächlichen Einwilligung des Patienten - einigermaßen unverständlich, wird eine rechtswirksame Einwilligung nur mittels Unterschrift oder qualifizierter Signatur hergestellt werden können, zumal die Ärzte dokumentationspflichtig bleiben. So ist auch im herkömmlichen Verfahren unstreitig eine Unterschriftsleistung erforderlich.

Ursprünglich sollte die eGK zum 1. Januar 2006 ausgegeben werden. Zwischenzeitlich warnen Lobbyisten mit dem Hinweis und maßgeblichen Argument schon getätigter Milliarden-Investitionen vor einem Ausstieg. Man wird dabei an die Romanfiguren aus Dostojewskis Werk *Der Spieler* erinnert, die sich verzockt haben und nur noch auf eine zwischenzeitliche Erbschaft hoffen oder darauf, dass sich der die Verhältnisse übersteigende Einsatz endlich in einem nächsten Spiel am Roulettetisch in einen satten rettenden Gewinn verwandeln möge. Ob die eGK neben den investiven Risiken, die ja wohl primär eher für die Versicherten und die Ärzte bestehen, die das Ganze bezahlen dürfen, aber auch fachlich der große Wurf sein wird, bliebe, sofern die eGK denn tatsächlich kommt, abzuwarten. Für eine Minorität der Versicherten jedenfalls, z. B. chronisch Kranke und Patienten, die in dezentralen Behandlungsverbünden betreut werden, mag ein übergreifendes Telematikkonzept interessant sein. Elektronische Kommunikation, der Transport von Bild-, Labor-, und anderen Patientendaten, mobil,

ambulant und stationär, elektronische Fallakten, die Verwaltung elektronischer Patientenakten und sog. *Disease-Management-Systeme* versprechen der IT-Branche Rendite. Es ist legitim, wenn in diesen Bereichen weiterentwickelt wird. Die langsame Entwicklung der eGK jedoch wirft Fragen auf:

- Soll die eGK zukünftig noch Basis für Telematik-Gesamtlösungen in Deutschland sein oder ist der Anspruch zu groß und ist die Karte vielleicht zukünftig als Datenträger nur noch Schlüssel für einzelne Mehrwertdienste (elektronische Patientenakte, Medikamentenhistorie u. a.), die separat von der Industrie angeboten werden?

- Ist die weitgehende Fixierung auf die eGK umsichtig genug oder sind datenschutzrechtliche Festlegungen in Bezug auf die eGK nicht auch auf andere Telematik-Anwendungen und die elektronische Verarbeitung von Patientendaten in Deutschland generell zu übertragen und durch den Gesetzgeber vorbeugend zu regeln? Die Entwicklungen außerhalb des Verfahrens der eGK sollten nicht aus dem Blick geraten. Große Firmen wie Microsoft, iSoft, Google, T-Systems u. v. a. haben den Medizin-Telematikbereich im Blick. Mit dem Projekt *elektronische Gesundheitskarte* läuft der Staat bei dem gegenwärtigen Veränderungstempo Gefahr, von parallelen Entwicklungen eingeholt zu werden.

- War jede gesetzgeberische Entscheidung, z. B. die, den Datenträger Papierrezept gegen den Datenträger eGK mit dem sog. *eRezept* auszutauschen, patienten- und anwenderfreundlich? Oder sind einige Bausteine der eGK doch noch einmal (gerade in Bezug auf alte und behinderte Menschen) auf den Prüfstand zu stellen? *Die Menschen stolpern nicht über Berge, sondern über Maulwurfshügel. (Konfuzius)*

Man hat sich mit diesem gewaltigen Projekt auf ein Gebiet gewagt, in dem es nicht wie bei der Autobahnmaut um die Erfassung von Gebühren oder wie bei *Elster* um eine schnelle Steuererklärung geht. Hier geht es buchstäblich um Leib und Leben von Menschen. Die oben gestellten Fragen sollten nüchtern, mit dem Mut, der Wahrheit ins Auge zu sehen, und der Absicht, Fehler notwendigerweise zu korrigieren, beantwortet werden. Nicht dem Profit der Industrie und den Erfolgsmeldungen der Politik gebührt dabei der Vorrang, sondern den Patienten.

10.2 Sozialwesen

10.2.1 Verfassungswidrigkeit der Einrichtung der SGB II-Arbeitsgemeinschaften

In meinem letzten Tätigkeitsbericht habe ich unter 10.2.1 über die Entwicklung der Datenschutzkontrollzuständigkeit für die SGB II-Arbeitsgemeinschaften (ARGEn) be-

richtet und den sächsischen Sonderweg beschrieben. An diesem hat sich nichts geändert, und er hat zumindest indirekt höchstrichterliche Bestätigung erfahren:

Am 20. Dezember 2007 hat das Bundesverfassungsgericht in seinem Urteil (Az.: 2 BvR 2433/04, 2 BvR 2434/04) zu den Verfassungsbeschwerden von elf Landkreisen (darunter weit überdurchschnittlich viele sächsische!) für Recht erkannt, dass die in § 44b SGB II vorgeschriebene Übertragung der den Landkreisen und kreisfreien Städten nach dem SGB II zukommenden Aufgaben auf die Arbeitsgemeinschaften und die einheitliche Aufgabenwahrnehmung von kommunalen Trägern und Bundesagentur für Arbeit in den Arbeitsgemeinschaften die kommunalen Gebietskörperschaften in ihrem Recht auf eigenverantwortliche Aufgabenerledigung verletzt und gegen die Kompetenzordnung des Grundgesetzes verstößt. Konkret hat das Gericht § 44b SGB II als mit Art. 28 Abs. 2 Satz 1 und 2 i. V. m. Art. 83 GG unvereinbar angesehen. Die Arbeitsgemeinschaften - so das Gericht weiter - seien als Gemeinschaftseinrichtung von BA und kommunalen Trägern nach der Kompetenzordnung des Grundgesetzes nicht vorgesehen. Zudem widerspreche die Einrichtung der Arbeitsgemeinschaften dem *verfassungsrechtlichen Grundsatz eigenverantwortlicher Aufgabenwahrnehmung*, der den zuständigen Verwaltungsträger verpflichtet, die Aufgaben grundsätzlich durch eigene Verwaltungseinrichtungen, also mit eigenem Personal, eigenen Sachmitteln und eigener Organisation, wahrzunehmen. Zur Begründung hat das Bundesverfassungsgericht unter anderem ausgeführt, dass die in § 44b SGB II geregelte „Mischverwaltung“ insbesondere auch zu Rechtsunsicherheiten beim Datenschutz führe; dies fußt auch auf Hinweisen, die ich dem Gericht unterbreitet habe.

Weil das Urteil eine grundlegende Umgestaltung erforderlich macht, hat das Gericht dem Gesetzgeber eine lange Frist zur Änderung der Konstruktion der Arbeitsgemeinschaften bis zum 31. Dezember 2010 gesetzt.

Das Bundesministerium für Arbeit und Soziales hat aus diesem Grund im Jahre 2008 ein Eckpunktepapier zur Neuordnung der Behörden im Bereich des SGB II vorgelegt, dem zufolge die SGB II-ARGEn in sogenannte „Kooperative Jobcenter“ umgewandelt werden sollten, die jedoch als Organisationseinheit der BA anzusehen sein und an denen sich die Kommunen auf der Grundlage freiwilliger Kooperationsverträge beteiligen können sollten. Dieses Eckpunktepapier hat es jedoch nicht bis zum Gesetzentwurf gebracht, vielmehr haben sich die Länder für eine Verfassungsänderung dahingehend ausgesprochen, dass in den Arbeitsgemeinschaften ausnahmsweise eine Mischverwaltung des Bundes und der Länder stattfinden könne. Dieser Vorschlag ist in einen Entwurf eines Gesetzes zur Regelung der gemeinsamen Aufgabenwahrnehmung in der Grundsicherung für Arbeitsuchende und in einem Entwurf eines Gesetzes zur Änderung des Grundgesetzes gemündet.

Das darin liegende Ansinnen, ein verfassungswidriges Gesetz durch Änderung des Grundgesetzes zu legitimieren, hat zum Teil heftige Kritik ausgelöst, darunter bei der Fraktion der Unionsparteien im Bundestag, wodurch zumindest bis zur Bundestagswahl im September 2009 das Einbringen des Regierungsentwurfs in das Gesetzgebungsverfahren blockiert sein dürfte.

Auf die weiteren Entwicklungen in dieser Frage kann man sehr gespannt sein.

10.2.2 Landes-Gesetz zur Förderung der Teilnahme von Kindern an Früherkennungsuntersuchungen

(A) Im Mai 2009 hat der Landtag als Artikel 1 *des Gesetzes zur Förderung der Teilnahme von Kindern an Früherkennungsuntersuchungen das Sächsische Kindergesundheits- und Kinderschutzgesetz* (SächsKiSchG, GVBl. S. 379) verabschiedet.

Es beruht auf der parlamentarischen Beratung des von der Staatsregierung im Zuge einer Welle gleichartiger Gesetzgebung anderer Bundesländer - als politischer Reaktion auf spektakuläre Fälle tödlich ausgegangener Kindesmisshandlung bzw. länger anhaltender misshandlungsartiger Vernachlässigung - erarbeiteten, unter der DS-Nummer 4/14409 im Januar 2009 im Landtag eingebrachten Gesetzentwurfes der Staatsregierung.

Der Regierungsentwurf hatte nicht sehr viel von dem aufgegriffen, was ich vorher, in zwei Besprechungen mit dem SMS und einer von mir um den Jahreswechsel abgegebenen 35seitigen Stellungnahme zu einem „Arbeitsentwurf“, an Kritik und Verbesserungsvorschlägen vorgebracht hatte.

(B) In Bezug auf die Sicherstellung der Teilnahme an den Früherkennungsuntersuchungen ist im Gesetz folgendes Verfahren vorgesehen:

Gemäß § 1 Abs. 4 SächsKiSchG sollen alle Kinder mit Wohnsitz im Freistaat Sachsen zur Förderung der gesundheitlichen Vorsorge und des gesunden Aufwachsens an den bis zum Alter von vier Jahren, und zwar auf der Grundlage des in § 26 Abs. 1 Satz 1 SGB V begründeten Leistungsanspruches gegenüber der gesetzlichen Krankenversicherung in Richtlinien des nach § 91 Abs. 1 Satz 1 SGB V gebildeten *Gemeinsamen Bundesausschusses*, vorgesehenen Früherkennungsuntersuchungen (U4 bis U8) teilnehmen. Zu diesem Zweck sollen Eltern, deren Kinder nicht an Früherkennungsuntersuchungen teilgenommen haben, von den Gesundheitsbehörden erinnert und zur Teilnahme aufgefordert werden (§ 1 Abs. 4 Satz 2 SächsKiSchG). Hierfür erhält die KV Sachsen nach § 2 Abs. 1 SächsKiSchG die Befugnis, regelmäßig die bei der SAKD gespeicherten Meldedaten der Kinder abzurufen, die ihrem Alter entsprechend für die

Durchführung einer Früherkennungsuntersuchung nach den Kinderrichtlinien des Bundesausschusses in Frage kommen. Daneben erhält die KV nach § 2 Abs. 2 SächsKiSchG von Ärzten, die bei einem Kind eine Früherkennungsuntersuchung U4 bis U8 durchgeführt haben, innerhalb von fünf Werktagen folgende Daten übermittelt: Familienname und Vornamen, Tag der Geburt, Geschlecht, gesetzliche Vertreter, gegenwärtige Anschrift sowie die Bezeichnung der durchgeführten Früherkennungsuntersuchung. Innerhalb einer Fünf-Tage-Frist führt die KV nun einen Datenabgleich zwischen den bei der SAKD abgeforderten Meldedaten und den ärztlicherseits mitgeteilten Daten durch und teilt dem jeweils zuständigen Gesundheitsamt unverzüglich mit, falls ein Kind nicht an einer für sein Alter vorgesehenen Früherkennungsuntersuchung teilgenommen hat (§ 1 Abs 3 SächsKiSchG).

Nach § 2 Abs. 4 Satz 1 SächsKiSchG erinnert das Gesundheitsamt den gesetzlichen Vertreter eines Kindes an die nicht durchgeführte Früherkennungsuntersuchung und belehrt über Toleranzgrenzen und den Zweck der Durchführung der Früherkennungsuntersuchungen. Hiernach erfolgt ein erneuter Datenabgleich mit der Folge, dem gesetzlichen Vertreter des Kindes eine gesundheitliche Aufklärung und Beratung durch das zuständige Gesundheitsamt anzubieten, falls ein Kind trotz der Erinnerung nicht an einer Früherkennungsuntersuchung teilgenommen hat (§ 2 Abs. 4 Satz 2 SächsKiSchG). Es werden die zur Durchführung einer Früherkennungsuntersuchung geeigneten Ärzte mitgeteilt oder die Untersuchung mit Einverständnis des gesetzlichen Vertreters durchgeführt (§ 2 Abs. 4 Satz 3 SächsKiSchG). Das Gesundheitsamt soll dem Jugendamt die gemäß § 2 Abs. 2 SächsKiSchG erhobenen Daten mitteilen, falls die Hilfsangebote des Gesundheitsamtes zur Durchführung einer der Früherkennungsuntersuchung vergleichbaren Untersuchung vom gesetzlichen Vertreter nicht wahrgenommen werden und darüber hinaus dem Gesundheitsamt gewichtige Anhaltspunkte für eine Kindeswohlgefährdung bekannt geworden sind (§ 2 Abs. 5 SächsKiSchG).

Dabei ist im Verlauf der parlamentarischen Beratung gegenüber dem Regierungsentwurf der Anwendungsbereich von den U3 bis U7a auf U4 bis U8 verschoben worden.

(C) Ich habe bis zuletzt den für die Beratung federführenden Ausschuss schriftlich wie mündlich beraten, wobei meine Kritik und meine Verbesserungsvorschläge zu Einzelregelungen letztlich auch in großem Umfang aufgegriffen worden sind. Unverändert bleibt es jedoch meinerseits bei einer verfassungsrechtlich begründeten Gesamtkritik an dem Gesetzesvorhaben, von der ich in den parlamentarischen Beratungen nie abgerückt bin (siehe hierzu Beschlussempfehlung und Bericht des ASGFFJ vom 8. Mai 2009, LT-DS 4/15418, Seite 7 ff., *abrufbar unter: http://edas.landtag.sachsen.de/*).

Diese grundlegenden verfassungsrechtlichen Einwände gegen das Gesamtvorhaben in seiner *Grundkonzeption* (Totalerfassung, Meldung der ca. 4 % Nichtteilnehmer an das Gesundheitsamt und der nach dessen Tätigwerden erwarteten rund 2 % Nichtteilnehmer an das Jugendamt) habe ich in meiner schriftlichen Stellungnahme zum Gesetzentwurf der Staatsregierung im letzten Abschnitt (dort unter [*4*]), dargelegt, wobei ich gerne eingeräumt habe, dass das in Sachsen gewählte Verfahren wegen der Einführung der Zwischenstufe der Tätigkeit des Gesundheitsamtes günstiger zu beurteilen ist als ähnliche Vorhaben anderer Länder.

Diese Kritik wird von der erwähnten Verschiebung auf den Bereich der Untersuchungen U4 bis U8 nicht wesentlich berührt, weswegen ich hier unverändert aus meiner Stellungnahme vom Januar 2009 zitieren darf:

„**(4.1) Gesetzeszwecke**

(**4.1.1**) Erklärter **Zweck** des Gesetzes ist (**A**) laut § 1 und der Begründung dazu die Erhöhung der Teilnahmerate an den U3 bis U7a von der derzeitigen Quote auf 100 %. Dazu wird ein Melde- und Abgleichssystem für alle Kinder bzw. deren Sorgeberechtigte eingeführt.

Dabei gehe ich nachfolgend von derjenigen *Zahlenangabe* aus, die das SMS bis Ende des Jahres 2008 zur Teilnahme an den Kinderfrüherkennungsuntersuchungen U1 bis U7 gemacht hat (vgl. Entwurf Stand 5.12.2008, Begründung, Allgemeines, 5. Absatz), nämlich *96 %* - eine Angabe, die auch laut Sächsischer Zeitung vom 29./30. November 2008 der Vorsitzende der Kassenärztlichen Vereinigung Sachsen, Klaus Heckmann, so gemacht hat. Dazu sehe ich mich berechtigt, weil eine Erläuterung des Umstandes, dass das SMS unter Nennung derselben - SMS-eigenen - Datenquelle die Angabe zur Nichtteilnehmerquote zwischen Ende Dezember 2008 und Anfang 2009 schlicht verdoppelt hat, mir nicht vorliegt.

Erst nach einer Überprüfung dieser Zahlenangabe wäre es sinnvoll, sich Gedanken darüber zu machen, inwieweit eine Nichtteilnahmequote von 8 % statt von 4 % eine veränderte verfassungsrechtliche Beurteilung nach sich ziehen könnte.

Dabei ist zu berücksichtigen, dass nicht erkennbar ist, dass die Einschätzung der Staatsregierung, wie hoch der Anteil derjenigen Kinder sei, für die Voraussetzungen einer Überprüfung durch das Jugendamt gemäß § 8a SGB VIII gegeben sind, ebenfalls gegenüber dem Dezember 2008 um 100 % oder jedenfalls signifikant gestiegen wäre. Immerhin gibt die Staatsregierung im Gesetzentwurf (nachstehend **E**; im Vorblatt S. 2 unten) eine sinkende Anzahl der in der Polizeistatistik für Sachsen angegebenen Fälle - so

darf man wohl interpretieren: - strafbarer Verletzung oder Gefährdung des Kindeswohles an.

Wie bereits in der *Einleitung* erläutert, gehe ich von der vom SMS bis Ende des Jahres 2008 angegebenen Teilnahmequote von 96 %, statt jetzt angegebener 92 %, aus.

Konkrete Angaben über Gesundheitsdefizite, die bei den bisher ferngebliebenen 4 % der Kinder bekanntgeworden wären, enthalten die Gesetzesmaterialien nicht.

Nicht ausdrücklich, sondern im Allgemeinen Teil der Begründung nur andeutungsweise und implizit als weiterer Zweck (**B**) des Gesetzes zu erkennen gegeben wird die Meldung der nach Intervention des Gesundheitsamtes verbleibenden (hartnäckigen) Nicht-Teilnahme-Fälle an das Jugendamt, die den Zweck hat, diesem ein Eingreifen wegen erklärten Verdachtes der Kindeswohlgefährdung im Rahmen von § 8a SGB VIII zu ermöglichen.

Mittel zur Erreichung des Zweckes A ist mittels des Melde- und Abgleichssystems die Einführung einer Art *Begründungslast* für die Nichtteilnahme an den Kinder-Untersuchungen […] Rechtsnachteile sind die Ansprache durch das Gesundheitsamt als erste Unannehmlichkeitsstufe und die Wahrscheinlichkeit von Ermittlungen des Jugendamtes als zu befürchtende zweite Unannehmlichkeitsstufe, also behördliche Erkundigungen wegen des erklärten behördlichen Verdachtes auf Kindeswohlgefährdung, wobei die Erkundigungen im Wesentlichen in einer Inaugenscheinnahme des Kindes und der Sorgeberechtigten, möglicherweise auch in der Befragung von Nachbarn bestehen: **B1** - Abschreckungswirkung der drohenden Jugendamtstätigkeit (zunächst bloße Ermittlungstätigkeit) zwecks Erhöhung der Teilnahmerate.

Neben dieser als Hilfs- oder Zwischenzweck dem Zweck A dienenden Möglichkeit eines Tätigwerdens des Jugendamtes (B1) steht unerklärt auch der Zweck **B2** - Erkenntnisgewinnungs-Nutzen eines tatsächlichen Tätigwerdens des Jugendamtes für dieses: Dass das Überprüfungsprogramm betreffend die Teilnahme an Kinderfrüherkennungsuntersuchungen (im Folgenden kurz „ÜP“) ermöglicht, dem Jugendamt Fälle bekanntwerden zu lassen, in denen es in Anwendung des § 8a SGB VIII eingreifen muss. Das sind nach der Eigenart des ÜP, also der Beschränkung der Überwachung auf die Zeitkorridore der Kinderuntersuchungen U3-U7a, die Fälle der *wiederholten Misshandlung* oder der *länger anhaltenden misshandlungsartigen Vernachlässigung*. Demgegenüber würden die Fälle, in denen einzelne Misshandlungen mit tödlicher Folge verübt werden oder eine kurzfristige misshandlungsartige Vernachlässigung zum Tode des Kindes führt, vom ÜP nicht erfasst.

Zugleich dient Zweck A dem Zweck B2 - über die Erlaubnis für die Kinderärzte, gemäß § 5 Satz 2 E den Jugendämtern Fälle von Kindeswohlgefährdung, deren Abstellung sie selbst nicht haben bewirken können (Satz 1 der Vorschrift), zu melden.

(**4.1.2**) Das ÜP soll also zwei unerwünschte *Verhaltensweisen aufdecken*:
Zum einen (Zweck A) die unverboten, also von Rechts wegen legal bleibende Nichtteilnahme an der Früherkennungsuntersuchung, um diese zu erschweren,
und zum anderen die - rechtswidrige - pflichtverletzende wiederholte Misshandlung oder anhaltende misshandlungsartige Vernachlässigung, die ein Einschreiten des Jugendamtes geboten sein lässt (Zweck B2).

(**4.2**) Zu diesem Zweck sollen - vereinfacht! - folgende informationellen **Grundrechtseingriffe** seitens Behörden stattfinden:

(**4.2.1**) Übersicht:

(a1) Nutzung und Übermittlung der Meldedaten aller 0-3jährigen Kinder und ihrer (vereinfacht im Sinne der verfassungsrechtlichen Terminologie:) Eltern durch die zentrale sächsische Meldebehörde (Kernmelderegister)
(a2) Speicherung dieser Daten bei der Kassenärztlichen Vereinigung Sachsen (KV)
(a3) Übermittlung aller Kinder (und der dazugehörigen Eltern) von 0-3 Jahren, die an den für das Lebensalter 4 Wochen bis 36 Monate vorgesehenen Untersuchungen teilgenommen haben, durch die sächsischen Ärzte an die sächsische KV

(b1) Übermittlung der Nichtteilnehmer, also nach dem bisherigen Stand (Nicht-Existenz des Gesetzes bzw. des ÜP) 4 % des Doppeljahrganges, durch die KV an das Gesundheitsamt
(b2) Datennutzung durch das Gesundheitsamt

(c1) Gegebenenfalls Datenübermittlung durch das Gesundheitsamt an das Jugendamt (vom SMS erwartete 1,5 % des Doppeljahrgangs der bis Zweijährigen, entsprechend zurzeit 1.000 Kindern, zusätzlich die zum dritten Jahrgang gehörenden)
(c2) Datennutzung und Datenerhebung durch das Jugendamt betreffend diese Fälle, d. h. nach dem derzeitigen Stand in durchschnittlich 75 Fällen je sächsisches Jugendamt (13) in den ersten beiden Jahrgängen, für die drei Jahrgänge mithin ca. 110 Kinder.

(**4.2.2**) Die Grundrechtseingriffe a1 bis a2 betreffen zu 96 % Fälle von Menschen, bei denen der Gesetzeszweck schon ohne diese Grundrechtseingriffe erreicht ist, beim Grundrechtseingriff a3 sind es 100 %.

Auch die Grundrechtseingriffe b1 und b2 betreffen einen Personenkreis, den noch nicht notwendig ein *konkreter Störerverdacht* trifft (zu diesem rechtlichen Gesichtspunkt vgl. BVerfGE 115, 320, 355).

(**4.3**) Somit stellt sich verfassungsrechtlich die Frage, inwieweit bzw. unter welchen Voraussetzungen eine solche einzelverdachtslose informationelle Totalerfassung verfassungsrechtlich zulässig und das heißt insbesondere ***verhältnismäßig*** ist.

(**4.3.1**) Konkret: Sind hier von Verfassungs wegen die Voraussetzungen dafür gegeben, dass mit den Grundrechtseingriffen a1-a3 96 % bis 100 % Betroffene hinsichtlich eines bestimmten Verhaltens erfasst werden dürfen, um eine Menge von 4 % individuell aufzuspüren, die sich aus Schein-Störern (U-Teilnahme, die lediglich nicht gemeldet ist) und „Schwach-Störern“ (keine U-Teilnahme, aber kein § 8a SGB VIII) und unbekannt vielen „Stark-Störern“ zusammensetzt, wovon den Vermutungen nach insgesamt etwa 35 % Schwach-Störer (bloße hartnäckige Nicht-Teilnehmer) oder aber möglicherweise Stark-Störer unterschiedlichen Schweregrades (= Fälle der Interventions-Maßnahmen nach § 8a SGB VIII, d. h. § 8a Abs. 1 S. 3, Abs. 3 und 4) sein sollen.

(**4.3.2**) Für die Prüfung der *Geeignetheit, Erforderlichkeit* und *Angemessenheit* der geplanten Grundrechtseingriffe im Hinblick auf den Gesetzeszweck kommt es auf die zu erwartenden **Wirkungen** des ÜP bzw. der Gesetzesanwendung an.

(**4.3.2.1**) Dabei kann unterstellt werden, dass (**W1**) die informationellen Eingriffe a1-a3 mit b1 und b2 und c1 und c2 zur Erreichung des Zieles (A) im Sinne einer *Anhebung in Richtung auf 100 % Teilnahme geeignet* sind. Es wird für die 4 %, die von Hause aus (d. h. ohne Gesetz bzw. ÜP) Nichtteilnehmer sind bzw. wären, Druck erzeugt, ihr Kind doch der Untersuchung zu unterziehen.

Die Schätzung des SMS, dass von den 4 %, die nicht von sich aus Früherkennungsuntersuchungsteilnehmer gewesen sind, ca. 65 % die Untersuchung aufgrund der Tätigkeit des Gesundheitsamtes durchführen werden, mag plausibel sein.

Erfolg wäre, dass in denjenigen Fällen, in denen die gesundheitliche Entwicklung des Kindes Maßnahmen erfordert, diese mit wesentlich erhöhter Wahrscheinlichkeit ergriffen würden.

Dazu, wie hoch die Quote dieser Fälle (d. h. der Anteil an den 65 % von 4 % des Doppeljahrgangs) sein wird und wie schwerwiegend der medizinische Interventionsbedarf ist, sind keine vom Gesetzgeber angestellten Schätzungs-Überlegungen erkennbar.

Das bedeutet: Über den tatsächlichen Wert der Verfolgung des Zweckes A für das Kindeswohl, also den praktischen Effekt von W1 hinsichtlich der Fall-Anzahl und Fall-Schwere, liegen für das Gesetzgebungsverfahren keine erkennbaren Vorstellungen vor.

(**4.3.2.2**) Genauso wenig ist erkennbar, wie hoch der Interventionsbedarf bei den nach Tätigwerden des Gesundheitsamtes verbleibenden Nichtteilnehmern (**W2**) sein würde. Dies gilt sowohl für den rein medizinischen, also ohne sonstige, d. h. misshandlungsartige Vernachlässigung, bestehenden Bedarf, in die gesundheitliche Entwicklung einzugreifen (Ziel A), als auch für den unter § 8a SGB VIII fallenden Bedarf an Einschreiten gegenüber länger dauernder misshandlungsartiger Vernachlässigung oder wiederholter Misshandlung (also die Fälle, die das Jugendamt kennen sollte, Ziel B).

Auch insoweit fehlt es an erkennbaren Vorstellungen des Gesetzgebers über den praktischen Wert der Wirkung, hier W2.

Zusätzlich fehlt es auch an erkennbaren Überlegungen des Gesetzgebers dazu, wie sich die Menge (Anzahl, Schwere) der dem Jugendamt gemeldeten Fälle zu derjenigen verhält, die das Jugendamt ohne die Meldung des Gesundheitsamtes schon kennt. Denn diejenigen Fälle, die das Jugendamt schon ohne das ÜP kennt, sind nicht Fälle der Erreichung des Zweckes B2.

Nicht einmal die *Anzahl* der Fälle der Altersgruppe 4 Wochen bis 24 Monate, die den Jugendämtern jeweils bekannt sind, im bloßen *Vergleich* zu den durchschnittlich 75 Fällen, mit deren Bekanntwerden der Gesetzentwurf nach den Angaben des SMS (außerhalb der schriftlichen Gesetzesbegründung) rechnet, ist somit auch nur grob geschätzt erkennbar; für die miteinbezogenen Kinder des dritten Jahrganges gilt Entsprechendes.

(**4.3.2.3**) Es mag sein, dass die Fälle schweren, in das Elternrecht stark eingreifenden nach § 8a SGB VIII berechtigten und gebotenen Einschreitens des Jugendamtes zu einem stark erhöhten Anteil unter die 4 % Nicht-Teilnehmer fallen. Mit der Richtigkeit einer solchen Feststellung wäre aber noch nicht die Erkenntnis verbunden, dass solche Fälle überhaupt erst noch (Geeignetheit) und überdies am grundrechtsschonendsten (Erforderlichkeit) gerade durch Heraus-Fahnden der 4 % des Doppeljahrganges oder auch Dreifachjahrganges, die nicht ohnehin an Kinderfrüherkennungsuntersuchungen teilnehmen, gefunden werden müssen.

Jedenfalls können die spektakulären, schlimmstens ausgegangenen Fälle von wiederholter Misshandlung bzw. anhaltender, misshandlungsartiger Vernachlässigung, die über die Medien der Öffentlichkeit bekannt geworden sind, nicht zur Begründung der Erforderlichkeit des Vorhabens herangezogen werden. Denn in diesen Fällen haben die

Jugendämter ausweislich der unbestrittenen Medienberichte immer Kenntnis davon gehabt, dass es sich um Fälle des § 8a SGB VIII gehandelt hat.

(4.3.2.4) Fazit:

Zur effektiven Gesundheitsförderungswirkung wie auch zur Kindeswohlgefährdungsverhinderungswirkung des Gesetzes liegen keine erkennbaren Vermutungen oder Schätzungen des Gesetzgebers vor.

Damit ist die *Geeignetheit* für Primärzwecke (Gesundheitsförderung, Kindeswohlgefährdungsverhinderung) noch nicht völlig ausgeschlossen, aber der vom Gesetzgeber erkennbar in keiner Weise auch nur vage eingeschätzte Eignungsgrad (Wirkungsgrad) erscheint als mutmaßlich sehr gering.

(**4.3.3**) Diese Zweifelhaftigkeit der Geeignetheit bzw. des Wirkungsgrades der geplanten informationellen Grundrechtseingriffe wird im Hinblick auf den unter dem medial verstärkten Druck der Öffentlichkeit politisch im Vordergrund stehenden Zweck B2 in folgender Hinsicht bestätigt:

(**4.3.3.1**) Angesichts des Umstandes, dass nach bisherigen bundesweiten Erkenntnissen staatliche Aktivitäten zugunsten des Kindeswohles eher durch eine zu schwache personelle Ausstattung der Jugendämter begrenzt werden, die es diesen nicht gestattet, in wünschenswertem Umfang den bereits vorliegenden Anhaltspunkten nachzugehen und, wie erwähnt, die bisher in der Öffentlichkeit bekannt gewordenen Fälle von Kindeswohlgefährdungen den jeweiligen Jugendämtern bereits bekannt waren, erscheint das Gesetzesvorhaben als im Hinblick auf die hauptsächliche Zielgruppe der Stark-Störer (B2) *insgesamt ungeeignet*: Es werden in mehr oder weniger geeigneter Weise Fälle gesucht, die dann nach den bisherigen Erfahrungen von den zuständigen Stellen nicht hinreichend bearbeitet (versorgt) werden können.

(**4.3.3.2**) Dabei kann auch nicht unberücksichtigt bleiben, dass der Gemeinsame Bundesausschuss die Einführung einer Reihenuntersuchung („Screening“) zur Früherkennung von Kindesmisshandlungen in die Kinderuntersuchungs-Richtlinien abgelehnt hat, da seiner Auffassung nach einem fraglichen Nutzen ein möglicherweise hoher Schaden entgegenstünde; denn eine solche gezielte Untersuchung auf Kindesmisshandlung hin würde die Einwilligung der Eltern verlangen, so dass unter Umständen bei der dafür relevanten Gruppe die Teilnahme zurückginge, weil die Untersuchung nicht mehr als Vorsorgeangebot, sondern als Kontrollinstrument wahrgenommen würde (Pressemitteilung des Gemeinsamen Bundesausschusses vom 14. September 2007).

Außerdem hat während der Anhörung im Hessischen Landtag zum Hessischen Kindergesundheitsschutzgesetz am 8. November 2007 der Vorsitzende des Unterausschusses Prävention des Gemeinsamen Bundesausschusses, *Metzinger*, diese Feststellung des Gemeinsamen Bundesausschusses noch dahin ergänzt, dass es seiner Meinung nach keine Belege dafür gebe, dass verbindliche Früherkennungsuntersuchungen eine wirksame Vorkehrung gegen Vernachlässigung oder Gewalt bei Kindern darstellen.

Seinerzeit hat der Präsident des Berufsverbandes der Kinder- und Jugendärzte, *Dr. Hartmann*, darauf hingewiesen, dass es sich bei den Kinderuntersuchungen um ein reines Krankheitsfrüherkennungsprogramm, nicht aber um ein eigentliches Präventionsprogramm handele, und er hat bekräftigt, dass zwischen den Vorsorgeuntersuchungen viel zu große Lücken bestünden, um kurzfristige Kindeswohlgefährdungsentwicklungen zu erfassen, und dass eine Beurteilung der sozialen und familiären Situation den Ärzten nicht möglich sei.

Das Vorstandsmitglied der Deutschen Gesellschaft gegen Kindesmisshandlung und -vernachlässigung *Herrmann* hält die Vorsorgeuntersuchung für kein geeignetes Erkennungsinstrument für die große Zahl der durch Misshandlung seelisch geschädigten Kinder; so hätten zum Beispiel sexuell missbrauchte Kinder zu 90 % keine nachweisbaren körperlichen Befunde.

Die mögliche Beeinträchtigung der Wirkungsmöglichkeit der Jugendämter durch Beeinträchtigung des Vertrauens in diese infolge einer stärker eingreifenden als helfenden Arbeit kommt hinzu.

Angesichts dessen erscheint auch die *Geeignetheit* des Gesetzesvorhabens bzw. des ÜP als sehr fraglich. Erwägungen des Gesetzgebers zur Geeignetheit, die sich mit diesen als bekannt gelten könnenden Äußerungen aus Gesetzgebungsverfahren (ich schließe mich hier dem an, was mein Kollege von Bose in Sachsen-Anhalt im Gesetzgebungsverfahren geltend gemacht hat), fehlen. Damit fehlen Ansätze und Überlegungen zur Rechtfertigung der geplanten Grundrechtseingriffe durch begründete Einschätzung ihrer Geeignetheit überhaupt, zumindest eine Einschätzung ihres Wirkungsausmaßes.

(**4.4**) Folgendes hat meiner Meinung nach demnach Grundlage der Beurteilung der Verhältnismäßigkeit des geplanten Informationssystems (ÜP) zu sein:

(**4.4.1**) Es handelt sich um eine *anlasslose* informationelle Totalerfassung, die erfassten Eltern (im Sinne von Art. 6 GG, also Sorgeberechtigten) haben zu 96 % keinen Anlass zu ihrer Erfassung gegeben - außer dadurch, Eltern eines Kleinkindes zu sein.

Auch die restlichen 4 % des Doppeljahrganges haben überwiegend auch nach Auffassung des Gesetzgebers keine Rechtsverletzung begangen, *gesichert* liegt bei ihnen nur ein leicht risikoerhöhendes Verhalten vor.

(**4.4.2**) Die Totalerfassung ist eine anlasslose *Überwachungsmaßnahme* im Schutzbereich von Art. 6 Abs. 2 Satz 1 GG.

Dass Art. 6 Abs. 2 Satz 2 GG anlasslose Total-Überwachungen, die es bisher nicht gegeben hat, in der vorliegenden Weise zulässt, erscheint als mehr als zweifelhaft. Der Vorschrift liegt ein Vertrauen in die Eltern als Ausgangs-Prinzip zugrunde.

Die Einschüchterungswirkung der im Gesetz vorgesehenen informationellen Eingriffe, die grundsätzlich geeignet ist, die Grundrechtsausübung zu beeinträchtigen (vgl. BVerfGE 115, 320, 354 unten und NJW 2008, 1516 lSp., Rdnr. 173), trifft hier auf das hochrangige Grundrecht der vor-staatlichen Gemeinschaft *Familie*, deren Antastung bekanntlich eine Kennzeichen unfreiheitlicher, totalitärer politischer Systeme gewesen ist, weswegen hier auch bei Grundrechtseingriffen gänzlich unideologischer Natur von Verfassungs wegen besondere Vorsicht geboten ist.

Die „Beobachtung“ als Ausübung des in Art. 6 Abs. 2 Satz 2 GG begründeten staatlichen „Wächteramtes“ greift in das Recht der Eltern aus Art. 6 Abs. 2 Satz 1 GG ein. Derartige Informationsbeschaffungseingriffe sind nur unter der Voraussetzung zulässig, *dass konkrete Anhaltspunkte für eine Kindeswohlbeeinträchtigung gegeben und* die Maßnahmen geeignet, erforderlich und angemessen sind zur Erlangung von Daten, deren die öffentliche Gewalt bedarf, um auf hinreichend gesicherter Erkenntnisgrundlage beurteilen zu können, ob und in welchem Maße die Voraussetzungen für ein Einschreiten in Ausübung des Wächteramtes vorliegen. Unzulässig sind namentlich informationelle Eingriffe im Sinne einer ‚mitlaufenden’ Erziehungskontrolle oder einer Befolgungskontrolle, denn trotz ihrer Pflichtbindung beruhen elterliche Befugnisse nicht auf staatlicher Konzession; elterliche Auskunfts-, Duldungs- oder Mitwirkungspflichten lassen sich nur ausnahmsweise, d. h. bei begründetem Verdacht einer Kindeswohlgefährdung rechtfertigen - so überzeugend Jestaedt in BK, Stand 1995, Rdnrn. 185 f. zu Art. 6 Abs. 2 und 3 GG.

Eine gegenüber der Zeit von vor 60 Jahren wesentlich verringerte Fähigkeit der Eltern, statt des Staates selbst für ein gesundes Aufwachsen ihrer Kinder zu sorgen, ist nicht dargetan. Überforderungssymtome, insbesondere im Bereich des *Gesetzesvollzuges*, zeigt im Übrigen auch allenthalben der Staat, nicht nur im Bereich der Jugendämter (zwei Beispiele nur: das im letzten Jahr vielfach beklagte Vollzugsdefizit bei der

Kontrolle der Datenverarbeitung im privaten Bereich und die erkennbar gewordene mangelnde Kontrolle der Finanzwirtschaft).

(**4.4.3**) Es handelt sich, anders als im Falle der Rasterfahndungsentscheidung des Bundesverfassungsgerichtes (Entsch. v. 4.4.2006, 1 BvR 518/02, E 115, 320, insbes. 354 ff., 360 ff.), eher wie im Falle der automatisierten Kfz-Kennzeichen-Erfassung (BVerfG Urt. v. 11.3.2008, 1 BvR 2074/05 u. 1254/07, NJW 2008, 1505), um eine anlasslose (BVerfG: „verdachtslose“) Totalerfassung, bei der statistisch gesichert permanent mit dem Vorhandensein einiger Treffer-Fälle als Fällen gegenwärtiger konkreter Gefahr (§ 8a SGB VIII-Fälle) zu rechnen ist.

Ähnlich wäre etwa die anlasslose Durchsuchung sämtlicher Kraftfahrzeuge oder Wohnungen auf Drogen, Sprengstoffe oder unerlaubten Waffenbesitz.

Ähnlichkeit besteht auch mit der beim BVerfG anhängigen Speicherung von Verbindungsdaten nach §§ 113a, 113b TKG: Durch einzelverdachtslose Totalerfassung bewirkte große Streubreite des informationellen Eingriffes mit dadurch statistisch gesichertem ‚dauerndem’ Vorkommen einzelner bzw. vereinzelter konkreter Verdachtsfälle (Gefahrenabwehr oder Strafverfolgung).

(**4.4.4**) Dabei gibt es jedoch, wie ausführlich dargelegt, keine Anhaltspunkte dafür, dass bzw. in welchem Maße schwerwiegende Fälle rechtswidrigen Elternverhaltens (wiederholte Misshandlung oder anhaltende misshandlungsartige Vernachlässigung) tatsächlich bei der mit dem Gesetzesvorhaben geplanten Schleppnetz-Fahndung gefunden werden, die der zuständigen Behörde (Jugendamt) nicht schon bekannt sind.

(**4.4.5**) Ferner ist nicht abschätzbar, wie hoch der Nutzen für Kinder in den Nicht-Teilnehmerfällen ist, bei denen eine wiederholte Misshandlung oder länger andauernde misshandlungsartige Vernachlässigung (Fall des § 8a SGB VIII) nicht vorliegt.

(**4.4.6**) Angesichts dessen sehe ich keine für eine verfassungsrechtliche Beurteilung erkennbare Rechtfertigung der geplanten Erfassungs- und Überwachungsmaßnahmen, so dass die vom Gesetz angeordnete Fahndung nach den 4 % Anteilen von Nichtteilnehmern nach den Maßstäben des Bundesverfassungsgerichts als eine *Ermittlung ins Blaue hinein* im Sinne der Rasterfahndungsentscheidung (E 115, 360 f. bzw. der Entscheidung zum automatisierten Abgleich von Autokennzeichen (NJW 2008, 1515 rSp.) anzusehen und somit zumindest *unverhältnismäßig im engeren Sinne (unangemessen)* und daher *verfassungswidrig* ist: Es fehlt an der erkennbaren für die Rechtfertigung einzelverdachtsloser informationeller Grundrechtseingriffe auch bei höchstem Gewicht der drohenden Rechtsgutbeeinträchtigung erforderlichen hinreichenden Wahrscheinlichkeit von deren *plausiblerweise gerade durch den Grundrechtseingriff abzuwendendem* Ein-

tritt (BVerfGE 115, 320, 361 und NJW 2008, 1515 rSp. - der kursive Einschub ist hier von mir ergänzt: Er bezieht in die vom Gericht formulierte Überlegung einen Gesichtspunkt ein, der anders als in den Fällen der automatisierten Kennzeichenerfassung wie auch der Nutzung auf Vorrat gespeicherter Telekommunikationsverbindungsdaten die besondere verfassungsrechtliche Problematik der hier vorliegenden Technik einer Art gestufter *Schleppnetzfahndung* deutlich macht, die eben anders als die beiden zum Vergleich genannten, vom Bundesverfassungsgericht geprüften Fallgestaltungen ohne Nutzung aus anderen Verarbeitungen stammender verdachtsbegründender Daten vor sich geht).“

Ich habe schließlich folgende *Alternativ-Vorschläge* unterbreitet, mit denen sich die verfassungsrechtliche Bedenklichkeit des Vorhabens meiner Auffassung nach auf folgende Weise hätte vermeiden lassen noch künftig vermeiden ließe:

„Der Nachweis der Teilnahme an den Kinderuntersuchungen könnte ohne verfassungsrechtliche Probleme zur Voraussetzung des Anspruches auf Landeserziehungsgeld gemacht werden (wie dies in Thüringen und in Bayern geschehen ist: Art. 2 Nr. 1 des Thüringer Gesetzes zur Weiterentwicklung des Kinderschutzes, LT-Drs: 4/4249, am 11.12.2008 beschlossen; Art. 1 Satz 1 Nr. 4 des Bayerischen Landeserziehungsgeldgesetzes vom 9. Juli 2007, GVBl. 442).

Denn dann wäre die Meldung von Antragstellern, die nicht den fortlaufenden Nachweis der Teilnahme an den Untersuchungen bringen, an die *Gesundheitsämter* berechtigt: Der Staat honoriert mit dem Landeserziehungsgeld die Leistung der Eltern, sich, abgesehen von finanziellen Aufwendungen für diese, um diese zu kümmern, sich ihnen zu widmen; also ist es legitim, wenn der Staat sich darüber unterrichtet, ob diese Leistung tatsächlich in gesundheitlicher Hinsicht erfolgreich (ordnungsgemäß) erbracht wird.

Man wäre nicht mehr im Bereich der Gefahrenabwehr, sondern dem der Überprüfung des Erfolges der Verwendung einer staatlichen Subvention.

Fachleute müssen beurteilen können, ob überdies mit einer solchen Verfahrensweise nicht gerade eine Teilmenge der Eltern (einkommensschwächere) erfasst würde, bei der gesundheitliche Fehlentwicklungen der Kleinkinder in signifikant überdurchschnittlichem Maße zu befürchten sind, so dass der informationelle Eingriff wesentlich gezielter wäre als im Falle des geplanten ÜP.

Falls praktische Erfahrungen das plausibel machen, wäre dann in der zweiten Stufe auch eine zusätzliche Einschaltung des Jugendamtes zulässig, weil die dann erfassten Fälle nahezu mit Sicherheit die Voraussetzungen des § 8a Abs. 1 SGB VIII erfüllten.

Nur zweierlei spräche *gegen* eine solche Lösung, die natürlich Eltern, die aus Gründen der Einkommenshöhe kein Landeserziehungsgeld bekommen, nicht erfasst:

(a) Bestimmte Eltern könnten bewusst von vornherein auf einen Antrag auf Landeserziehungsgeld verzichten, um sich unauffällig der Teilnahme ihres Kindes an den Kinderuntersuchungen zu entziehen. Dies wären dann wohl schon im Wesentlichen nicht nur Fälle des § 8a SGB VIII, sondern auch strafrechtlich relevante Fälle.

Diese sehr wenigen und zugleich sehr schwerwiegenden Fälle kalkulierter, schon krimineller oder übertrieben schamhafter Vernachlässigung würde man in Kauf nehmen - in der Annahme, dass sie wie bisher doch, soweit erforderlich, dem Jugendamt durch Beobachtungen aus dem sozialen Umfeld bekannt werden.

(b) Geltend gemacht werden könnte auch, dass der Staat den Teilnahmeverweigerern das Erziehungsgeld nicht entziehen dürfe, da sie es doch gerade für die Kinder brauchten, man also durch eine solche Maßnahme das Kindeswohl gefährdete.

Dieses Argument ist nicht stichhaltig:
Im Hinblick auf den Verhältnismäßigkeitsgrundsatz geht es im Verhältnis und im Vergleich zu der im Gesetzentwurf vorgesehenen Verfahrensweise verfassungsrechtlich nicht an, *alle* betroffenen Eltern mit dem Eingriff in ihr Grundrecht auf informationelle Selbstbestimmung zu belasten, weil die öffentliche Gewalt sich scheut, *sehr wenigen* das Erziehungsgeld zu verweigern bzw. das Gesundheitsamt auf sie ‚anzusetzen', obwohl man dadurch gezielt etwas für das Wohl der betreffenden sehr wenigen Kinder tun könnte.

Wenn der Freistaat Sachsen in dieser Angelegenheit rechtlich *risikofreudig* sein sollte (ohne Grundrechtsbelastung!), könnte er *zusätzlich* durch Landesgesetz für den Freistaat den Anspruch auf *Bundeselterngeld* von dem Nachweis der Teilnahme an den Kinderuntersuchungen abhängig machen.

Dieses Risiko einzugehen wäre vertretbar: Die Gesetzgebungszuständigkeit des Bundes für das BEEG ist, was das Elterngeld betrifft, nach den überzeugenden Ausführungen von Seiler in NVwZ 2007, 129-131 „mehr als zweifelhaft", der Bund würde es vermutlich kaum auf einen juristischen Konflikt ankommen lassen, mit Klagen von Eltern wäre kaum zu rechnen.

Eine Beschränkung auf das intervenierende Tätigwerden des Gesundheitsamtes, also der Verzicht auf eine Unterrichtung des Jugendamtes, würden den Mangel an Verhältnismäßigkeit mindern, eine Beschränkung auf ein bloßes *Einladungswesen* würde den Mangel meiner Auffassung nach beheben."

(D) Ob meine Kritik an dem Gesetz berechtigt ist, wird der Verfassungsgerichtshof in Leipzig oder auch das Bundesverfassungsgericht zu klären haben, sollten sich betroffene Eltern - wie in Rheinland-Pfalz in einem Fall im Hinblick auf ein dortiges ähnliches Gesetz aus dem Jahre 2008 (RP-GVBl. S. 52) geschehen - gegen das staatliche Überwachungsprogramm zur Wehr setzen und Verfassungsbeschwerde erheben.

Die Verfassungsbeschwerde an den Verfassungsgerichtshof Rheinland-Pfalz ist inzwischen gescheitert (Az: B 45/08). Die Begründung der Gerichtsentscheidung stützt sich zum einen in ausgeprägter Weise (unter B II 2 a bb [1], [4] β und b cc der Gründe, Umdruck S. 16, 23 bzw. 29 f.) auf ein im Jahr 2000 in die dortige Landesverfassung aufgenommenes besonderes Kinder-Recht, das Kindern „*besonderen* Schutz [des Staates] insbesondere vor körperlicher und seelischer Misshandlung und Vernachlässigung“ gewährt (Art. 24 RPVerf). Diese Vorschrift versteht das Gericht als Schaffung eines *gegenüber anderen hochrangigen Rechtsgütern überragenden Verfassungswertes* („Gemeinschaftsgutes“, a. a. O. S. 16 mit S. 23). Dies hat weder in der Sächsischen Verfassung noch im Grundgesetz ein Gegenstück. (Als Verschiebung gegenüber der Wertordnung des Grundgesetzes wäre dies eine Betrachtung wert.)

Zum anderen, und dies ist von allgemeinem datenschutzrechtlichem Interesse, lässt die Entscheidung jede Auseinandersetzung mit den vom Bundesverfassungsgericht bereits zur Frage der einzelverdachtslosen Totalerfassung (s. oben Abschnitt C unter 4.4.2 bis 4.4.6 meiner Stellungnahme) angestellten Überlegungen (vgl. zuletzt dazu etwa Hong NJW 2009, S. 1458, 1459 f.) fast so gut wie vollständig vermissen - bis auf die Feststellung, dass es sich nicht um eine Rasterfahndung handele (dazu oben Abschnitt C unter 4.4.3 meiner Stellungnahme). Das Gericht stellt im Grunde genommen nur darauf ab, dass die öffentliche Gewalt für den anerkannt guten Zweck möglichst frühzeitig Gefährdungen des Kindeswohles erkennen müsse (Umdruck S. 18, a. a. O. bb [2]); der Staat müsse sich zur angemessenen Erfüllung seiner Aufgaben vor dem Eintritt von Verletzungen des Kindeswohles Informationen verschaffen dürfen (a. a. O. S. 27, b aa).

Datenschutzrechtlich befremdlich ist dabei auch die *Ablehnung* der Beschränkung einer Fahndungsmaßnahme auf - offenbar - anerkannte Risikogruppen, d. h. Personenkreise mit, wie das Urteil annimmt, signifikant weniger Einzelverdachtslosigkeit (Umdruck S. 21, a. a. O. bb [3] der Gründe): Totalerfassung zur Vermeidung von ‚Stigmatisierung’. Folgerichtig wäre jede Rasterfahndung verfassungswidrig, weil sie per se in diesem Sinne *stigmatisiert*. Oder auch: Stammt der Gefährder oder Tatverdächtige nach den vorliegenden Erkenntnissen aus der Gruppe z. B. der jungen Männer mit Führerschein und bestimmter örtlicher Sprachfärbung, so muss die Fahndung in gleicher Weise auch Frauen und Greise bundesweit erfassen, damit eine *Stigmatisierung* vermieden

wird. (Eine verfassungsrechtliche Begründung dieses so verstandenen *Stigmatisierungsverbotes* gibt die gerichtliche Entscheidung nicht.)

So einfach wird man es sich im Hinblick auf einen Eingriff in das Grundrecht auf informationelle Selbstbestimmung zum Zweck der Gefahrenabwehr wohl nicht machen dürfen, sofern nicht für die Gefahrenabwehr im Hinblick auf Übergriffe oder Versäumnisse von Eltern gegenüber ihren Kindern andere Maßstäbe, nämlich weniger strenge Anforderungen, an die Voraussetzungen informationeller Grundrechtseingriffe gelten sollen als in sonstigen Bereichen, beispielsweise auch der Terrorismusabwehr.

(E) Abschließend zu einem Beispiel erfolgreicher datenschutzrechtlicher Arbeit in diesem Gesetzgebungsverfahren:

Zu dem mit dem Sächsischen Kindergesundheits- und Kinderschutzgesetz geschaffenen System der Überwachung der Teilnahme an den Kinder-Früherkennungsuntersuchungen gehört, wie eingangs gegen Ende des Abschnittes B erwähnt, der Versuch, über die auch nach Mahnung durch das Gesundheitsamt festzustellende Nicht-Teilnahme (das ist ungenau, vgl. dazu nachstehend am Ende) an einer Früherkennungsuntersuchung Fälle der Kindeswohlgefährdung ausfindig zu machen und dementsprechend das Jugendamt tätig werden zu lassen. Dabei muss sichergestellt sein, dass die Übermittlungserlaubnis für das Gesundheitsamt nicht an weniger strenge Voraussetzungen geknüpft ist als diejenigen, unter denen das Jugendamt gemäß § 8a SGB VIII derartige Daten entgegennehmen, d. h. erheben darf. Mit anderen Worten: Die Übermittlungserlaubnis des § 2 Abs. 5 Satz 1 SächsKiSchG ist an das Vorliegen der in § 8a SGB VIII für das Jugendamt bestimmten Erhebungsvoraussetzungen zu binden; andernfalls forderte der Landesgesetzgeber rechtswidrige Datenweitergaben durch die Gesundheitsämter heraus: Die Erlaubnis der Übermittlung vom Empfänger nicht rechtmäßig zu erhebender personenbezogener Daten wäre wegen Ungeeignetheit (als Verstoß gegen den Verhältnismäßigkeitsgrundsatz) *verfassungswidrig*. Das ist, nachdem ich darauf noch einmal in meiner Stellungnahme vom Januar 2009 gegenüber dem Gesetzentwurf der Staatsregierung (LT-DS 4/14409) nachdrücklich hingewiesen hatte, im parlamentarischen Verfahren dann erfreulicherweise dadurch vermieden worden, dass die ‚Meldung' (Übermittlung) des Falles durch das Gesundheitsamt an das Jugendamt in § 2 Abs. 5 Satz 1 SächsKiSchG an die Voraussetzung gebunden worden ist, dass dem Gesundheitsamt (sc. zusätzlich zur Nicht-Teilnahme an der Früherkennungsuntersuchung) *gewichtige Anhaltspunkte für die Gefährdung des Wohls des Kindes bekannt geworden sind*, also die Voraussetzung, die § 8a Abs. 1 Satz 1 SGB VIII aufstellt. Zudem verpflichtet und berechtigt das Gesetz das Gesundheitsamt nicht ausnahmslos zur Übermittlung, sondern nur im Wege einer *Soll*-Vorschrift, so dass es in begründeten Ausnahmefällen von der Datenübermittlung an das Jugendamt abzusehen hat, also auch

absehen darf. (Damit unterscheidet sich § 2 Abs. 5 Satz 1 SächsKiSchG wohltuend von seinem Gegenstück im oben in Abschnitt D erwähnten entsprechenden rheinland-pfälzischen Gesetz: Dessen § 9 Abs. 1 Satz 1 schreibt eine Übermittlung durch das Gesundheitsamt an das Jugendamt für alle Fälle vor, in denen trotz der Mahnung durch das Gesundheitsamt dieses eine Teilnahme an der Früherkennungsuntersuchung nicht hat feststellen können - in der genannten Entscheidung des dortigen Verfassungsgerichtshofes nicht problematisiert.)

Allerdings stellt sich unverändert die Frage, auf der Grundlage wie bzw. bei wem getroffener Feststellungen (Sachverhaltsermittlungen) das Gesundheitsamt die nach § 2 Abs. 5 Satz 1 SächsKiSchG stattfindende Prüfung der Übermittlungsvoraussetzung „gewichtige Anhaltspunkte für die Gefährdung des Wohls des Kindes“ durchführen soll. Es ist nach dem Gesetzeswortlaut ja ausgeschlossen, dass diese gewichtigen Anhaltspunkte ausschließlich in der dem Gesundheitsamt bekanntgewordenen Reaktion bzw. Nicht-Reaktion der gesetzlichen Vertreter bestehen dürfen. Konkreter: Das Gesetz versäumt es, eine Aussage darüber zu treffen, *in welcher Weise* das Gesundheitsamt anknüpfend an das nach Bundesrecht wie auch nach Landesrecht (auch nach Inkrafttreten des Gesetzes weiterhin) *erlaubte* Verhalten, sich dafür zu entscheiden, die freiwilligen Früherkennungsuntersuchungen *nicht* wahrzunehmen, einen Verdacht auf das Vorliegen einer Kindeswohlgefährdung im Sinne von § 8a SGB VIII gewinnen können soll.

Es muss in der Verwaltungspraxis darauf geachtet werden, dass das Gesetz nicht durch die von ihm ausgelöste (in Sachverhaltsfeststellungen bestehende) Verwaltungs*praxis* der Gesundheitsämter seiner faktischen Wirkung nach eine *Begründungslast*, genauer gesagt eine Last des *Äußerns dem Gesundheitsamt* (nach welchem Maßstab?) *einleuchtender Gründe* (vgl. Gesetzesbegründung zu Absatz 4: „Beweggründe“) mit der rechtlichen Folge einführt, dass ihre Nichterfüllung kraft nicht vom Gesetz bestimmter, aber aus seiner Anwendung im praktischen Ergebnis resultierender landesrechtlicher *Fiktion* den Tatbestand der Kindeswohlgefährdung im Sinne von § 8a Abs. 1 Satz 1 SGB VIII erfüllt.

Denn der Landesgesetzgeber kann nicht bestimmen, dass das Nicht-Äußern eines dem Gesundheitsamt einleuchtenden Grundes für eine Nichtteilnahme des Kindes an der Kinderuntersuchung den Tatbestand des § 8a Abs. 1 Satz 1 SGB VIII erfüllt. Es ist ja schon fraglich, ob typischerweise das Nicht-Äußern eines dem Gesundheitsamt einleuchtenden Grundes für eine Nicht-Teilnahme des Kindes an der Kinderfrüherkennungsuntersuchung das Vorliegen des anderen Tatbestandes (gewichtiger Anhaltspunkt einer Gefährdung des Kindeswohls) *indiziert*. Dementsprechende empirische Erkenntnisse sind im Gesetzgebungsverfahren nach meinem Kenntnisstand nicht mitgeteilt worden, es ist auch nicht einmal behauptet worden, dass es sie gebe. Deswegen muss

darauf geachtet werden, dass die Praxis der Anwendung des Gesetzes nicht auf einen in diese Richtung gehenden Automatismus hinausläuft. Dies umso mehr, als für die Gesundheitsämter natürlich die Verlockung groß ist, vorsorglich immer zu übermitteln, um die Möglichkeit auszuschließen, einmal einen Fall nicht dem Jugendamt zu melden, der später wegen spektakulärer Verletzung des Kindeswohls Aufsehen erregt.

Abgesehen davon muss § 2 Abs. 5 Satz 1 SächsKiSchG so ausgelegt werden, dass statt auf die (nicht) *durchgeführte* auf die nicht *gemeldete* Untersuchung abzustellen ist, die *nach Kenntnis des Gesundheitsamtes auch nicht durch eine gleichwertige Untersuchung ersetzt worden ist*.

10.2.3 Sozialdatenschutzrechtlicher Auskunftsanspruch, gerichtet auf Überlassung einer Kopie des amtsärztlichen Gutachtens im Zusammenhang mit der Bewilligung von Eingliederungshilfe

Die Eltern eines minderjährigen Kindes baten im Rahmen der Bewilligung ihres Antrags auf Eingliederungshilfe für heilpädagogische Förderung in einer Frühförderstelle (vgl. § 54 SGB XII) die zuständige Sozialhilfebehörde um Einsichtnahme in das vom Gesundheitsamt hierzu erstellte amtsärztliche Gutachten beziehungsweise um Überlassung einer Kopie davon. Die Eltern wandten sich an mich, nachdem ihnen die Sozialhilfebehörde auf Anfrage mitgeteilt hatte, dass sie nur einen Teil des Gutachtens zur Einsicht erhielten und Kopien überhaupt nicht überlassen werden dürften.

Ich habe der Sozialhilfebehörde Folgendes mitgeteilt: Einem Auskunftsbegehren nach § 83 SGB X ist regelmäßig durch Gewährung von Akteneinsicht zu entsprechen, da der Betroffene auf diese Weise zur Durchsetzung seines Rechtes auf informationelle Selbstbestimmung am zuverlässigsten erfahren kann, über welche Informationen eine öffentliche Stelle über seine Person verfügt. Das Gutachten des Gesundheitsamtes, welches für die Entscheidung über den Sozialleistungsantrag erstellt worden ist, ist selbstverständlich Bestandteil der bei der Sozialhilfebehörde zum Antragsteller geführten Sachakte. Dies schließt das Recht des Betroffenen mit ein, in entsprechendem Umfang auch Kopien aus der Akte und damit auch in Bezug auf das streitgegenständliche Gutachten überlassen zu bekommen oder fertigen zu können.

Das Sozialamt hat den betroffenen Eltern hierauf umgehend eine Ablichtung des vollständigen Gutachtens ausgehändigt.

Generell ist bei der Entscheidung über die Rechtmäßigkeit einer Auskunftsverweigerung durch die zuständige Behörde und der Überprüfung dieser Entscheidung durch mich nach § 83 Abs. 6 SGB X zu beachten, dass ich meine Entscheidung über die Auskunft *auch nicht faktisch* an die Stelle der Entscheidung der Behörde setzen darf

(deutlicher insoweit § 18 Abs. 6 Satz 4 SächsDSG): Ich darf nur eine Stellungnahme dazu abgeben, inwieweit die Auskunft in Erfüllung des datenschutzrechtlichen Auskunftsanspruches erteilt zu werden hat. Gegenüber der Behörde wird diese Stellungnahme oft in die Einzelheiten gehen; meine Mitteilung an den Betroffenen hingegen soll diesem zu einer Einschätzung seiner Rechtsposition dienlich sein, darf aber nicht so formuliert sein, dass der Betroffene daraus schon die von ihm angestrebten Informationen gewinnen kann. Letztlich ist der Betroffene daher auf den Rechtsweg verwiesen, wenn die Behörde an ihrer Ablehnung der Auskunftserteilung festhält.

10.2.4 Übermittlung von Sozialdaten zur Vollstreckung der Forderung auf Rückzahlung zu Unrecht erbrachter Leistungen

Der Datenschutzbeauftragte eines LRA hat die grundsätzliche Frage aufgeworfen, ob es zulässig sei, wenn eine für Sozialleistungen zuständige Stelle des LRA, z. B. die Sozialhilfebehörde, Sozialdaten an die Kreisfinanzverwaltung übermittelt, damit diese zu Unrecht gezahlte Leistungen zurückfordern kann.

Meines Erachtens ist eine solche Datenübermittlung insoweit zulässig, als es um die Schlussphase der Rückforderung, nämlich die Vollstreckung bestandskräftiger Rückforderungsbescheide der Sozialbehörde geht und die Kreisfinanzverwaltung für die Vollstreckung solcher Bescheide eine gesetzliche Zuständigkeit hat. Das ergibt sich aus Folgendem:

Gemäß § 69 Abs. 1 Nr. 1 SGB X darf eine Sozialbehörde Sozialdaten übermitteln, soweit dies zur Erfüllung der Zwecke erforderlich ist, für die die Daten erhoben worden sind oder soweit sie für die Erfüllung einer aus dem Sozialgesetzbuch selbst hervorgehenden gesetzlichen Aufgabe der Behörde erforderlich sind. Zur Aufgabe der Sozialleistungsträger oder genauer gesagt der Ausführung des jeweiligen Buches des SGB gehört auch die Rückforderung zu Unrecht gezahlter Leistungen (Hauck/Noftz, § 69 SGB X Rdnr. 14; v. Wulffen, § 69 SGB X Rdnr. 13). Soweit die Zuständigkeit für die Beitreibung dieser Forderung einer (sc. funktional) anderen Stelle als dem Sozialleistungsträger übertragen ist, also einer anderen Behörde, ist eine Übermittlung von Sozialdaten zur Erfüllung der gesetzlichen Aufgabe (Beitreibung der Forderung) erforderlich.

So ist es hier:
Die Zuständigkeit für die Vollstreckung regelt § 66 Abs. 3 SGB X, wonach die jeweiligen landesrechtlichen Vorschriften für das Verwaltungsvollstreckungsverfahren gelten. Damit öffnet sich das Sozialgesetzbuch wie etwa in § 81 Abs. 2 Satz 3 SGB X

Gesetzesinhalten außerhalb seiner selbst, und zwar anders als in § 71 SGB X in blanketthafter Weise.

Gemäß § 4 Abs. 1 Nr. 1 SächsVwVG sind Vollstreckungsbehörden bei Leistungsbescheiden die Finanzämter, es sei denn, es ist etwas anderes bestimmt, § 4 Abs. 4 SächsVwVG. Eine solche „andere“ Bestimmung findet sich in § 61 SächsLKrO i. V. m. § 86 SächsGemO. Danach ist für alle Kassengeschäfte der Landkreis zuständig. Zu dem Kassengeschäft gehören unter anderem die Annahme der Einzahlungen einschließlich Mahnung, Beitreibung und Einleitung der Zwangsvollstreckung. Die Einzelheiten regelt § 1 Abs. 1, 3 KomKVO, die gemäß § 45 auch auf die Landkreise anwendbar ist.

Für die Beitreibung der vollstreckbaren Forderung ist jedoch nicht erforderlich, dass die Sozialhilfebehörde den gesamten Rückforderungsbescheid, einschließlich der darin enthaltenen Sozialdaten, an die Kreisfinanzverwaltung übermittelt. Zur Übersendung der Zahlungsaufforderung an den Betroffenen reicht es aus, wenn auf den Rückforderungsbescheid der Sozialhilfebehörde Bezug genommen wird. Dafür ist lediglich, neben der genauen Bezeichnung der Stelle und deren Aktenzeichen, die Kenntnis des zurückzufordernden Betrages, des Tages des Bescheiderlasses sowie der Anschriftsdaten des Vollstreckungsschuldners und der sonstigen Daten nach § 4 Abs. 3 Satz 1 SächsVwVG erforderlich.

10.2.5 Übermittlung von Sozialdaten im Hinblick auf Ermittlungsverfahren wegen Verletzung der Unterhaltspflicht (§ 170 StGB) an Staatsanwaltschaft oder Polizei

Einer SGB II-Behörde gegenüber, die im Hinblick auf eine Dienstanweisung der BA und auf die Datenerwartungen der zuständigen Staatsanwaltschaft an mich die Frage herangetragen hat, nach welcher Vorschrift sie der Staatsanwaltschaft oder der Polizei Sozialdaten im Hinblick auf Ermittlungsverfahren wegen Verletzung der Unterhaltspflicht zur Verfügung stellen dürfe, habe ich unbeschadet der Zuständigkeit des BfDI (vgl. 13/10.2.1) folgenden Rechtsstandpunkt geäußert, gegen den Einwände von meinen Kollegen im Bund und in den Ländern nicht geltend gemacht worden sind (und bei dem ich davon ausgegangen bin, dass ungeachtet des § 51b Abs. 4 SGB II die §§ 67 ff. SGB X Anwendung finden):

Rechtsprechung und Literatur vertreten zu den in Frage kommenden Vorschriften des SGB X unterschiedliche Auffassungen. Die überwiegende Meinung (vgl. dazu Seidel in LPK-SGB X, § 74 Rdnr. 3) ist der Ansicht, dass eine solche Übermittlung *nicht* auf § 74 Satz 1 Nr. 1 Buchst. a SGB X gestützt werden kann; diese Vorschrift bestimmt, dass die Übermittlung von Sozialdaten zulässig ist, soweit die Daten erforderlich sind für die

Durchführung eines gerichtlichen Verfahrens oder eines Vollstreckungsverfahrens wegen eines gesetzlichen oder vertraglichen Unterhaltsanspruches oder eines an seiner Stelle getretenen Ersatzanspruches. Vielmehr soll nach dieser Auffassung allenfalls eine Übermittlung auf der Grundlage des § 73 Abs. 2 SGB X in Betracht kommen, wonach eine Übermittlung von Sozialdaten zur Durchführung eines Strafverfahrens wegen Straftaten zulässig ist, soweit die Übermittlung auf die Weitergabe des Namens, Vornamens, Geburtsortes, Geburtsdatums, Anschrift des Betroffenen sowie erbrachte oder demnächst zu erbringende Geldleistung beschränkt ist. Diese Übermittlungserlaubnis hilft den Strafverfolgungsbehörden in der Regel wenig weiter.

Eine einzelne Stimme in der Rechtsprechung (LG Berlin, Beschluss v. 14. April 2004, Az. 511 Qs 40/04) hat als Übermittlungserlaubnis die Regelung des § 73 Abs. 1 SGB X als einschlägig erachtet und die Verletzung der Unterhaltspflicht als eine Straftat von erheblicher Bedeutung angesehen; hier gibt es keine Beschränkung des Datensatzes, aber wie bei Absatz 2 ist die Übermittlung gemäß § 73 Abs. 3 SGB X vom Richter anzuordnen.

Die BA schließlich vertritt die Auffassung, dass die Übermittlung auf § 69 Abs. 1 Nr. 2 SGB X gestützt werden könne und eine richterliche Anordnung somit nicht erforderlich sei. Danach soll eine Übermittlung der Erkenntnisse über eine Unterhaltspflichtsverletzung dann zulässig sein, wenn die Übermittlung für die Durchführung eines mit der Erfüllung einer Aufgabe nach § 69 Abs. 1 Nr. 1 SGB X zusammenhängenden gerichtlichen Verfahrens einschließlich eines Strafverfahrens erforderlich ist. Nach Auffassung der BA gehört zur Aufgabe der SGB II-Behörden auch das Erstatten von Strafanzeigen, um die Zahlungsdisziplin der Unterhaltsverpflichteten zu wahren.

Ich habe mich der Rechtsauffassung eines Landgerichts (LG Stade, MDR 1981, S. 960 ff.) angeschlossen, wonach § 74 SGB X in Fällen der Offenbarung von Daten bei der Verletzung der Unterhaltspflichten als Spezialvorschrift gegenüber § 73 SGB X anzusehen ist, so dass doch, entgegen der zitierten überwiegenden Meinung, § 74 Satz 1 Nr. 1 Buchst. a SGB X auf eine Datenübermittlung an Strafverfolgungsbehörden wegen Verfahren nach § 170 StGB angewandt werden kann. Ich habe insbesondere die von der BA vertretene Auffassung abgelehnt, da die Übermittlungserlaubnis des § 69 Abs. 1 Nr. 2 SGB X nicht für Ermittlungsverfahren gilt und darüber hinaus inhaltlich auf Betrugsverfahren (Leistungsmissbrauch) und Angriffe auf Personal oder Eigentum des Leistungsträgers beschränkt ist (vgl. Seidel in LPK-SGB X, § 69 Rdnr. 6; v. Wulffen-Bieresborn, § 69 SGB X, Rdnr. 26).

10.2.6 Übermittlung von Sozialdaten auf Einwilligungsgrundlage

In einem Fall, in dem sich jemand von einem Sozialleistungsträger ungerecht behandelt fühlte und die Presse für seinen Fall interessiert sowie ihr „Vollmacht“ erteilt hatte, von der Behörde sämtliche Daten über seinen Fall zu erhalten, in dem die Voraussetzungen des § 69 Abs. 1 Nr. 3 SGB X (also der besonderen Erlaubnis zur Unterrichtung der Öffentlichkeit zum Zweck der Richtigstellung im Behördeninteresse) jedoch noch nicht erfüllt waren, habe ich dem betreffenden Sozialleistungsträger folgende Rechtsauffassung mitgeteilt:

Zwar erlaubt § 67b Abs. 1 Satz 1, letzter Fall, SGB X im Unterschied zu demjenigen, was § 67a Abs. 1 für die Datenerhebung vorschreibt, auch eine Verarbeitung und Nutzung auf Einwilligungsgrundlage. Unter diese Regelung fällt gemäß § 67 Abs. 6 Satz 1 SGB X auch das Übermitteln. Allerdings geht dem meiner Auffassung nach die Spezialvorschrift des § 67d, als allgemeine Vorschrift für alle Übermittlungserlaubnisse des SGB, vor. Nach diesem § 67d Abs. 1 ist *eine Übermittlung von Sozialdaten nur zulässig, soweit eine gesetzliche Übermittlungsbefugnis nach den §§ 68 bis 77 oder nach einer anderen Rechtsvorschrift in diesem Gesetzbuch vorliegt*.

Nach der zwingenden Regel des Vorranges der lex specialis, also der verdrängenden Wirkung der speziellen gegenüber der allgemeineren Vorschrift, muss dies auch im Verhältnis des § 67d Abs. 1 zu § 67b Abs. 1 SGB X gelten. Man könnte demgegenüber höchstens geltend machen, dass § 67b Abs. 1 mit der Formulierung *soweit die nachfolgenden Vorschriften … es erlauben … oder soweit der Betroffene eingewilligt hat* ausspreche, dass die verarbeitungserlaubende Wirkung der Einwilligung auch neben den dem § 67b folgenden Erlaubnissen gelten solle. Dem steht jedoch das „nur“ in § 67d Abs. 1 entgegen, das andere Erlaubtheitsgründe ausschließt.

Der Vollständigkeit halber sei angemerkt, dass sich in der Kommentarliteratur die gegenteilige Auffassung findet (Seidel in LPK-SGB X zu § 67d, Rdnr. 2), die jedoch nur oberflächlich mit dem begrifflichen Verhältnis von „Übermittlung“ und „Verarbeitung“ in Verbindung mit der Anwendbarkeit von § 67b Abs. 1 und 2 begründet wird (so auch Bieresborn in v. Wulffen zu § 67d Rdnr. 3). Eine Variante dieser Gegenmeinung bietet Rombach in Hauck/Noftz, Rdnr. 32 zu § 67d: Rombach sieht in der zweiten Tatbestandsvariante des § 67d Abs. 1 („*oder nach einer anderen Rechtsvorschrift in diesem Gesetzbuch*“) eine Rückverweisung auf § 67b Abs. 1. Aber auch diese Überlegung überzeugt mich nicht. Denn im 2. Kapitel des SGB X hat die Formulierung „oder nach einer anderen Rechtsvorschrift in diesem Gesetzbuch“ üblicherweise den Sinn einer Verweisung auf SGB-Bücher außerhalb des Zehnten Buches.

Zwar mag dieses Ergebnis im Hinblick auf eine ausschließlich vom Betroffenen selbst ausgehende Einwilligung (Spontaneinwilligung), also für den Fall eines ureigenen Übermittlungswunsches des Betroffenen, engherzig erscheinen. Jedoch hat der Betroffene ja seinen umfassenden datenschutzrechtlichen Auskunftsanspruch und in der Regel überdies den verwaltungsverfahrensrechtlichen Akteneinsichtsanspruch, §§ 83, 25 SGB X. Dadurch hat er die Möglichkeit, Dritten all die Auskünfte zur Verfügung zu stellen, die die Behörde ihrerseits durch Sozialdatenübermittlung den Dritten zur Verfügung stellen könnte, hat es aber bis zuletzt selbst in der Hand zu entscheiden, welche konkreten Daten er tatsächlich herausgeben will.

Im Hinblick auf die strenge Grundregel des Sozialdatenschutzes in § 35 Abs. 2 SGB I mitsamt der Bußgeldbewehrung in § 85 Abs. 2 Nr. 1 SGB X halte ich daher an der von mir seit längerem vertretenen strengeren Auffassung weiterhin fest. Sie scheint mir wohlbegründet: Die Behörde ist kein Auftragsempfänger („Vollmacht"), das Handeln auf Einwilligungsgrundlage muss ihr im Bereich ihrer eigentlichen Aufgabenerfüllung vom Gesetz erlaubt sein - wegen des Verfassungsgrundsatzes des *Vorbehaltes des Gesetzes*, vgl. 13/10.2.15 unter 4.3.

10.2.7 Datenschutz bei der Ausschreibung der Erbringung von Sozialleistungen durch freie Träger

Ein Jugendamt hat Leistungen zur Erbringung von Hilfen zur Erziehung (§§ 27 ff. SGB VIII, als sog. „integrierte, flexible Hilfen") unter freien Trägern zum Zweck der Vergabe entsprechender Aufträge ausgeschrieben. Dabei werden auch einzelne „Fälle" konkret ausgeschrieben, was zu der datenschutzrechtlichen Frage führt, wie konkret diese „Fälle" beschrieben werden dürfen.

Wie sich aus den mir zunächst vorgelegten Durchführungsbestimmungen einer städtischen „Grundsatzkommission" zur Vergabe derartiger Hilfen ergeben hatte, sollte das Jugendamt den freien Trägern nur folgende Angaben mitteilen: den Bedarf, die Erwartungen und die Zielsetzung mit zeitlichen Vorgaben zur Maßnahme sowie Alter und Geschlecht des potentiellen Leistungsempfängers.

Dies habe ich gegenüber dem Jugendamt folgendermaßen beurteilt: Derartige Angaben ermöglichen es dem jeweiligen freien Träger nicht, Rückschlüsse auf die Person des potentiellen Leistungsempfängers zu ziehen. Sie stellen deshalb auch keine Sozialdaten im Sinne des § 67 Abs. 1 Satz 1 SGB X dar, mit der Folge, dass ihre Bekanntgabe durch das Jugendamt an die freien Träger auch keiner gesetzlichen Erlaubnis bedarf.

In der konkreten Durchführung ist jedoch dann, wie ich wiederum durch einen Hinweis aus Fachkreisen erfahren habe, die Grenze zur Personenbeziehbarkeit in der Folgezeit

überschritten worden: In einer mir vorgelegten „Information zum Fall“, die Bestandteil der Ausschreibung war, waren nicht nur in dem dort vorgegebenen Freitextfeld „Festgestellter Hilfebedarf“ sehr genaue Angaben zu dem betreffenden Kind enthalten (Beispiel: „gewaltvolle Auseinandersetzung mit Bruder und gleichzeitig wichtige Bezugsperson“, „intensive Reaktion auf Körperkontakt“), sondern darüber hinaus wurden im Feld „Vorausgegangene Hilfen/Verlauf/Grund für Beendigung der Hilfen“ viele konkrete Angaben gemacht: Dort war nunmehr nicht nur aufgeführt, dass das Kind innerhalb eines bezeichneten Zeitraums in einem genannten Stadtteil vom „Allgemeinen Sozialdienst“ betreut worden war, sondern es waren zudem auch konkrete Aufenthaltszeiten (Datum Anfang und Ende) in einer wiederum genau bezeichneten Kinder- und Jugendpsychiatrie-Einrichtung sowie in anderen Einrichtungen aufgeführt.

Diese Informationen waren so konkret, dass sie für in der betreffenden Stadt in der Jugendhilfe Tätige Rückschlüsse auf den konkreten potenziellen Leistungsempfänger zugelassen haben, soweit er mit einem freien Träger bzw. jetzt bei diesem beschäftigten Personen bereits Kontakt hatte, mit der Folge, dass nunmehr personenbezogene Daten im Sinne des § 67 Abs. 1 Satz 1 SGB X übermittelt worden sind. (Auf dieses Problem hatte dabei, wie das Jugendamt dann zugab, - erfreulicherweise - auch schon der städtische Datenschutzbeauftragte hingewiesen.)

Es hätte somit für die Beibehaltung einer solchen Verfahrensweise einer gesetzlichen Rechtsgrundlage, und zwar wohlgemerkt im Sozialgesetzbuch, bedurft, die eine derartige Übermittlung personenbezogener Daten hätte rechtfertigen können; eine solche Rechtsgrundlage gibt es jedoch nicht.

Das betreffende Jugendamt hat daraufhin - wenn auch nicht gerade unumwunden - mir gegenüber eingeräumt, dass in dem aufgezeigten Fall die Detailliertheit der gemachten Angaben tatsächlich für die Ausschreibung bzw. Vergabe nicht erforderlich gewesen sei. Mit anderen Worten: Es sind in dem bekannt gewordenen Fall personenbezogene Daten im Sinne des § 67 Abs. 1 Satz 1 SGB X übermittelt worden, und dies ohne die hierfür erforderliche Rechtsgrundlage.

Laut Mitteilung des Jugendamts ist der Fall zum Anlass genommen worden, die betroffenen Mitarbeiter nochmals auf die Wahrung der Anonymität des Leistungsempfängers im Vergabeverfahren hinzuweisen. Seitdem haben mich keine weiteren Einwände gegen die Vorgehensweise dieses Jugendamts in derartigen Verfahren erreicht.

10.2.8 Grenzen der Prüfungsbefugnis und Prüfungsaufgabe des Sächsischen Datenschutzbeauftragten: Vorfragen von Verarbeitungserlaubnissen

Der Sächsische Datenschutzbeauftragte kontrolliert bei den öffentlichen Stellen die Einhaltung des Sächsischen Datenschutzgesetzes und anderer Vorschriften über den Datenschutz, § 27 Abs. 1 Satz 1 SächsDSG. Gemäß § 81 Abs. 2 Satz 2 und 3 SGB X kontrolliert er auch die Einhaltung der Regelungen über den Sozialdatenschutz nach dem Sozialgesetzbuch bei den öffentlichen Stellen der Länder, die Sozialleistungsträger sind oder sonst unter § 35 Abs. 1 SGB I fallen. Von der Kontrolle umfasst ist zunächst die Einhaltung der das Grundrecht der Betroffenen auf informationelle Selbstbestimmung unmittelbar schützenden Vorschriften, also das Vorliegen der notwendigen Verarbeitungserlaubnis, aber auch die Einhaltung präventiver Regelungen, wie etwa der Verpflichtung zu dem Datenschutz dienenden technischen und organisatorischen Maßnahmen, sowie der Vorschriften über Hilfs-Ansprüche wie insbesondere auf Löschung oder Auskunft.

Habe ich in diesem Zusammenhang auch zu prüfen und festzustellen, ob zwischen zwei miteinander zusammenlebenden Personen eine nicht-eheliche Lebensgemeinschaft besteht? Ich meine: Nein.

Hintergrund dieser Frage war folgender: Ein Petent und eine Petentin haben sich an mich gewandt und mir geschildert, eine SGB II-Behörde (Optionskommune, vgl. 13/10.2.1) teile regelmäßig ihre Sozialdaten dem jeweils anderen mit. So seien beide zu einem gemeinsamen Gespräch eingeladen worden, bei dem über Sozialdaten des jeweils anderen in beider Anwesenheit gesprochen wurde. Die beiden sahen darin einen Verstoß gegen den Sozialdatenschutz. Da beide unter gemeinsamer Adresse gemeldet waren, bat ich um Mitteilung, ob sie eine nicht-eheliche Lebensgemeinschaft bildeten. Diese Information benötigte ich, um den Sachverhalt datenschutzrechtlich prüfen zu können. *Besteht* nämlich eine solche nicht-eheliche Lebensgemeinschaft, so bilden deren Mitglieder eine Bedarfsgemeinschaft. Gemäß § 51b SGB II darf die SGB II-Behörde die erforderlichen personenbezogenen Daten aller Empfänger von Sozialleistungen, einschließlich aller Mitglieder der Bedarfsgemeinschaft erheben und verarbeiten. Da § 38 SGB II eine gesetzliche Vermutung regelt, wonach derjenige der Bedarfsgemeinschaft, der Leistungen beantragt hat, bevollmächtigt ist, Leistungen für die andere Person zu beantragen und entgegenzunehmen, darf eine SGB II-Behörde - im Rahmen ihrer Aufgabenerfüllung - diesem Vertreter auch Sozialdaten der Mitglieder der Bedarfsgemeinschaft mitteilen. Anders ausgedrückt: Von dieser Regelung notwendigerweise mitumfasst ist die Befugnis zur Übermittlung personenbezogener Daten der Personen der Bedarfsgemeinschaft, § 67d Abs. 1 SGB X i. V. m. § 38 SGB II.

Man kann das wohl auch so begründen: Kraft der Regelungen über die Bedarfsgemeinschaft im SGB II sind, soweit die Behörde davon auszugehen hat, dass ein Antragsteller (A) mit einer anderen Person (B) in Bedarfsgemeinschaft lebt, die für die Anwendung des SGB II erheblichen Daten beider Beteiligten Daten mit verstecktem (Beispiel: B hat ein Einkommen in Höhe X) oder offenem (Beispiel: B zahlt für A die Wohnungsmiete mit) *Doppelbezug* innerhalb eines durch die Rechtsordnung geschaffenen gemeinschaftlichen Rechtsverhältnisses mit einem Dritten (Leistungsträger): Solche Daten sind im Hinblick auf die Verarbeitung durch die SGB II-Behörde für jeden der beiden (A und B) immer eigene, es findet gar keine Übermittlung von Daten im Rechtssinne (§ 67 Abs. 6 Nr. 3 SGB X, in allen Datenschutzgesetzen aus zwingendem Grund nicht abweichend definiert) statt, weil die Daten nicht an einen *Dritten* weitergegeben werden.

Die Petenten versicherten mir wortreich, ohne abzustreiten ein „Paar“ zu sein, dass kein wechselseitiger Wille im Sinne des § 7 Abs. 3 Nr. 3 Buchst. c und Abs. 3a SGB II bestehe, Verantwortung füreinander zu tragen und füreinander einzustehen. Dabei stellte sich heraus, dass die SGB II-Behörde nach Befragung der Petenten und bei einem Hausbesuch zu der Feststellung gelangt war, dass zwischen den beiden eine nichteheliche Lebensgemeinschaft bestehen müsse. Ich habe mich an diese - nicht von offensichtlicher Willkürlichkeit getragene, plausible - Feststellung gebunden gesehen, da meine Kontrolltätigkeit nicht so weit gehen kann, dass ich selbst zu prüfen habe, ob eine nicht-eheliche Lebensgemeinschaft zwischen den Petenten besteht, denn: Nicht meiner Überprüfung unterliegen Schlussfolgerungen, die die Behörde in Anwendung des Gesetzes aus Feststellungen zu Sachverhalten zieht. Hat die Behörde wie im vorliegenden Falle konkrete Anhaltspunkte für das Vorliegen einer nicht-ehelichen Lebensgemeinschaft und ergeben sich aus dieser Annahme zusätzliche Befugnisse zur Datenerhebung - etwa Erhebung zu Vermögen und Einkommen des Partners - und zur Weitergabe an den anderen Beteiligten, kann und muss ich zwar diese Befugnisse, nicht aber die Feststellung zur nicht-ehelichen Lebensgemeinschaft kontrollieren. Dies gilt erst recht, wenn der Behörde ein sogenannter Beurteilungsspielraum eingeräumt ist, wovon bei der Feststellung einer nicht-ehelichen Lebensgemeinschaft auszugehen ist, vgl. LSG Nordrhein-Westfalen, Beschluss vom 27. Dezember 2006, Az.: L 1 B 36/06 AS ER, Rd.-Nr. 20, juris.

Kommt die SGB II-Behörde bei der Bearbeitung des Leistungsantrags nach dem SGB II zu dem Ergebnis, dass der Antragsteller mit einer weiteren Person in einem gemeinsamen Haushalt so zusammenlebt, dass der wechselseitige Wille anzunehmen ist, füreinander Verantwortung zu tragen und einzustehen, § 7 Abs. 3, lit. c SGB II, so fällt dies unter eine solche Feststellung von Sachverhalten. Zur Feststellung, ob eine nichteheliche Lebensgemeinschaft vorliegt, darf die SGB II-Behörde Ermittlungen anstellen.

Kommt sie dabei zu dem Ergebnis, dass die im Haushalt lebende Person zur Bedarfsgemeinschaft gehört, so kann ich dies nur beanstanden, wenn diese Beurteilung offensichtlich falsch ist und die darauf gegründete Datenerhebung oder -verarbeitung deshalb rechtsmissbräuchlich wäre.

Im konkreten Fall waren die Feststellungen der SGB II-Behörde nachvollziehbar und ganz offenbar nicht außerhalb des bei vernünftiger Betrachtungsweise Möglichen.

10.2.9 Übermittlung von Versichertendaten durch die Krankenkasse an Leistungserbringer, die Hilfsmittel liefern

Neue Versorgungsstrukturen in der Krankenversicherung haben zu folgender datenschutzrechtlichen Anfrage an mich geführt:

Eine große meiner Kontrollzuständigkeit unterliegende Krankenkasse hatte die Versorgung mit sog. Inkontinenzhilfen ab dem 1. Januar 2009 dahingehend umgestellt, dass jeweils ein bestimmtes (wohl jeweils gemäß § 127 Abs. 1 Satz 2 SGB V wohnortnahes) Unternehmen mit der Auslieferung der betreffenden Hilfsmittel beauftragt ist. Zu diesem Zweck waren seitens der Krankenkasse den betreffenden Unternehmen jeweils die Kontaktdaten der auf die betreffenden Hilfsmittel angewiesenen Versicherten übermittelt worden. Insgesamt waren hiervon nach Mitteilung der Krankenkasse insgesamt ca. 45.000 Versicherte betroffen.

Die Verfahrensumstellung ist auf das zum 1. April 2007 in Kraft getretene „Gesetz zur Stärkung des Wettbewerbs in der gesetzlichen Krankenversicherung (GKV-Wettbewerbsstärkungsgesetz - GKV-WSG)“ zurückzuführen. Danach werden die Versicherten grundsätzlich nur noch durch Vertragspartner der Krankenkassen mit Hilfsmitteln versorgt, und die Versicherten sind hiervon gemäß § 127 Abs. 5 SGB V in Kenntnis zu setzen.

Ich habe gegenüber der Krankenkasse folgende Rechtsauffassung vertreten:

Die im SGB V vorgesehene Informationspflicht berechtigt die Krankenkasse zwar, ihren Versicherten den jeweils für sie zuständigen Hilfsmittelerbringer mitzuteilen - mit der Möglichkeit für den Versicherten, sich sodann mit diesem in Verbindung zu setzen. Die Informationspflicht berechtigt die Krankenkasse jedoch nicht, dem betreffenden Leistungserbringer die Kontaktdaten des Versicherten zu übermitteln. Eine *Erforderlichkeit* dieser Datenübermittlung gemäß § 284 Abs 1 Satz 1 Nr. 4 SGB V i. V. m. § 284 Abs. 3 Satz 1 SGB V ist nicht erkennbar, zumal in Ausnahmefällen der Versicherte gemäß § 33 Abs. 6 Satz 3 SGB V auch einen anderen Leistungserbringer *wählen* kann,

wenn er ein berechtigtes Interesse daran begründen kann - gegebenenfalls mit der Folge der Mehrkostentragung durch den Versicherten.

Die Krankenkasse hat sich daraufhin für ihre Vorgehensweise auf einen vom SG Gießen und LSG Hessen entschiedenen Fall berufen, in dem die Gerichte unter Hinweis auf das Wirtschaftlichkeitsgebot die Weitergabe personenbezogener Daten von Versicherten im Zusammenhang mit der Organisation von Dialysefahrten für rechtmäßig erklärt haben. Ob diese Rechtsprechung auf den vorliegenden Fall anwendbar ist, ist sehr zweifelhaft: Wirtschaftlichkeitsgründe können die Datenverarbeitungsbefugnisse und insbesondere Datenübermittlungsbefugnisse der Krankenkassen nicht erweitern, wenn dies nicht im Gesetz vorgesehen ist - was nicht der Fall ist. Abgesehen davon sind Kostenersparnisgründe seitens der Krankenkasse hier gerade nicht zu erkennen, denn eventuelle Mehrkosten infolge der Inanspruchnahme eines anderen Leistungserbringers als des von der Krankenkasse angegebenen hat ja der Versicherte selbst und gerade nicht die Krankenkasse zu tragen.

Darüber hinaus habe ich die Krankenkasse aufgefordert, die betreffenden Vertragspartner zu verpflichten, für eine neutrale Verpackung bei der Auslieferung der Inkontinenzhilfen zu sorgen, die zudem auch sicherstellt, dass Dritte weder über den Aufdruck auf der Packung vom Inhalt der Packungen noch auf andere Weise vom Inhalt Kenntnis vermittelt bekommen.

Inzwischen sind auch andere Bundesländer mit dieser Problematik konfrontiert worden. Der Protest der Betroffenen hält sich wohl deswegen in Grenzen, weil Menschen, die Inkontinenz-Hilfsmittel benötigen, vielfach dement oder froh sind, dass ihnen die Mühe abgenommen worden ist, ihrerseits die Verbindung zu dem Lieferanten herzustellen. Das - und nur das - hat mich von einer Beanstandung absehen lassen.

Leider habe ich von der Datenweitergabe erst erfahren, als das Kind schon in den Brunnen gefallen war, sprich: die Krankenkasse bereits sämtliche Kontaktdaten an die beauftragten Liefer-Firmen weitergeleitet hatte. Im Hinblick auf den beachtlichen Umfang an Datenübermittlungen, die bei dieser Aktion vorgenommen worden sind, wäre es gerade hier wünschenswert gewesen, dass mich die Krankenkasse vorab zu Rate gezogen und mich um meine datenschutzrechtliche Bewertung gebeten hätte - so wie dies die vielen Jahre davor in solchen Fällen gute Übung gewesen ist.

10.2.10 Arztdaten, welche die Kassenärztliche Vereinigung zur Aufgabenerfüllung verarbeitet, sind Sozialdaten

An mich ist die Frage herangetragen worden, ob die KV der Staatsanwaltschaft für Ermittlungsverfahren Auskunft über Ärzte betreffende bei ihr gespeicherte Daten erteilen

muss. In einem Fall handelte es sich um Daten aus Notrufprotokollen des Kassenärztlichen Bereitschaftsdienstes, vgl. § 75 Abs. 1 Satz 2 SGB V, § 285 Abs. 1 Nr. 2 SGB V, im anderen um Ausbildungsdaten von Ärzten. Die KV hatte die Auskunft zunächst unter Hinweis auf § 73 SGB X mit der Begründung verweigert, es liege keine richterliche Anordnung vor. Die Staatsanwaltschaft hatte darauf erwidert, dass keine sozialdatenschutzrechtliche Auskunftsbeschränkung in Bezug auf die personenbezogenen Daten der Ärzte vorliege, insbesondere nicht nach § 73 SGB X, weil sie keine Versicherten- oder Patientendaten seien, und angekündigt, die Erwirkung richterlicher Durchsuchungs- und Beschlagnahmebeschlüsse prüfen zu wollen.

Die Kassenärztlichen Vereinigungen haben nicht nur die Sicherstellung der vertragsärztlichen Versorgung zur Aufgabe (§§ 72, 77 SGB V), sondern führen zugleich das Arztregister und prüfen die Voraussetzungen der Zulassung als Vertragsarzt - mit den dazugehörigen Verpflichtungen wie Weiterbildung etc. - (§§ 95 ff. SGB V). In diesem Aufgabenbereich werden personenbezogene Daten der Ärzte verarbeitet.

Gemäß § 67 Abs. 1 SGB X i. V. m. § 35 Abs. 1 Satz 4 SGB I i. V. m. § 77 Abs. 1 Satz 1 SGB V sind auch die personenbezogenen Daten von Ärzten, soweit es um ihre Speicherung oder sonstige Verarbeitung durch die KV geht, Sozialdaten im Sinne des § 35 Abs. 1 SGB I. Ihre Übermittlung unterfällt deswegen den Übermittlungsvorschriften des SGB X, so dass, weil andere Übermittlungserlaubnisse nicht in Frage kommen, in der Tat eine richterliche Anordnung nach § 73 SGB X erforderlich ist.

Dieses Ergebnis, dass Ärztedaten in der Verarbeitung durch die KV Sozialdaten sind, kann zusätzlich auf § 285 SGB V gestützt werden, der in Absatz 1 von Angaben über die persönlichen und sachlichen Verhältnisse der Ärzte spricht und in Absatz 3 Satz 1 und 3 diese Angaben dann als „Sozialdaten“ bezeichnet. Auch Waschule in Krauskopf, § 285 SGB V Rdnr. 3 und 7 unterscheidet zwischen den „Sozialdaten“ der Ärzte und denjenigen der Versicherten.

Dieser Auslegung könnte allerdings ein Beschluss des LG Heidelberg vom 26. April 2004 (Az.: 2 Qs 26/04) entgegengehalten werden, wonach die Datenverarbeitungsvorschriften des SGB X das Verhältnis der nach dem Sozialgesetzbuch Anspruchsberechtigten zu den Leistungsträgern, nicht aber das der Leistungsträger untereinander oder zu Leistungserbringern wie namentlich den Ärzten betreffen. Das Gericht hat § 73 Abs. 2 SGB X betreffend auf Ärzte bezogene Daten im Verhältnis zwischen KV und der Staatsanwaltschaft für nicht anwendbar gehalten und deshalb auf die Auskunftspflichten der Strafprozessordnung abgestellt (deren Erfüllung allerdings ebenfalls nicht behördlich, sondern allenfalls gerichtlich angeordnet werden kann).

Aus den aufgeführten Gründen ist das falsch:

Der von der Staatsanwaltschaft herangezogene § 161 StPO bietet nicht die nötige Grundlage als Übermittlungserlaubnis, da er unter dem Vorbehalt entgegenstehender anderer gesetzlicher Vorschriften steht und solche in Gestalt von §§ 67d Abs. 1, 68 Abs. 1 und 73 SGB X, § 35 Abs. 2 SGB I sowie § 285 Abs. 3 Satz 1 SGB V vorliegen.

Einwände gegen diese dem Gesetz unschwer zu entnehmende Auffassung habe ich auch aus dem Kreis meiner Kollegen nicht gehört.

Die Beschaffung der Ausbildungs-Daten bei der Ärztekammer, statt der KV, unterläge nicht den Vorschriften des Sozialdatenschutzes.

10.2.11 Anforderung von Betriebsunterlagen bei selbständiger Tätigkeit mit ALG II-Bezug

In 13/10.2.8 habe ich mich sehr grundlegend zur Zulässigkeit der Anforderung von Betriebsunterlagen des selbständigen Ehegatten eines ALG II-Empfängers geäußert.

Diese Ausführungen sind aus folgenden Gründen überholt: Nach § 9 SGB II hat die SGB II-Behörde zu prüfen, ob der Antragsteller hilfebedürftig ist. Dafür ist unter anderem auch zu prüfen, ob bestehendes Einkommen und Vermögen seinen Lebensunterhalt sichern kann. Wie das zu berücksichtigende Einkommen ermittelt wird, regelt § 11 SGB II i. V. m. § 3 der *Verordnung zur Berechnung von Einkommen sowie zur Nicht-Berücksichtigung von Einkommen und Vermögen bei Arbeitslosengeld II/Sozialgeld (ALG II-V)*. Diese Verordnung ist zum 1. Januar 2008 dahingehend geändert worden, dass nunmehr ein eigener Einkommensbegriff zur Berechnung des Einkommens aus selbständiger Arbeit, Gewerbebetrieb oder Land- und Forstwirtschaft entwickelt worden und die Ankopplung an die steuerrechtliche Einkommensermittlung entfallen ist. Nach dem neu gefassten § 3 ALG II-V ist die SGB II-Behörde berechtigt, eine Gegenüberstellung von voraussichtlichen Einnahmen und voraussichtlichen Ausgaben zu verlangen. Zur Plausibilisierung dieser Selbstprognose des Selbständigen kann dieser einen Nachweis über die tatsächlichen Einnahmen und Ausgaben der vorangegangenen sechs Monate, eine Einnahmenüberschussrechnung für das vorangegangene Kalenderjahr oder eine aktuelle betriebswirtschaftliche Auswertung vorlegen. Diese Datenerhebung ist zur Berechnung des aktuellen Einkommens des selbständig Tätigen für die Aufgabenerfüllung nach dem SGB II erforderlich.

10.2.12 Anforderung von Sozialversicherungsbuch und Führerschein durch die SGB II-Behörde

Darf die SGB II-Behörde verlangen, dass ein Antragsteller seinen Führerschein und seinen Sozialversicherungsausweis (im folgenden: „SV-Buch“) vorlegt, und darf eine Kopie davon zur Akte genommen werden?

Mit dem Anfertigen von Kopien von Sozialversicherungsausweisen der DDR durch eine Behörde habe ich mich bereits in 7/10.4 auseinandergesetzt. Die dort und auch die in 9/10.2.6 und 13/10.2.5 (Zulässigkeit der Anforderung von Kontoauszügen) aufgestellten Grundsätze gelten gleichermaßen für die Verarbeitung personenbezogener Daten nach dem SGB II.

Danach dürfen Unterlagen nur in dem für die Aufgabenerfüllung der Behörde erforderlichen Umfang angelegt und aufbewahrt werden. Das bedeutet, dass das Anfordern der Sozialversicherungsausweise nur dann zulässig ist, wenn die dort enthaltenen Daten für die Aufgabenerfüllung im konkreten Einzelfall erforderlich sind. Dies ist zu prüfen, bevor die Vorlage des SV-Buches verlangt wird. Kommt der Fallmanager zu dem Ergebnis, dass er die Einsicht in die Unterlagen benötigt, darf er unter Nennung des konkreten Grundes die Vorlage verlangen.

Die Ablichtung eines Teils des SV-Buches kommt nur in Betracht, wenn auf der Kopie nur die Angaben enthalten sind, die für die konkrete Fallbearbeitung erforderlich sind und die sowieso abzuschreiben wären. Sind noch weitere - nicht relevante personenbezogene Daten enthalten - darf keine Kopie angefertigt werden. Die notwendigen Daten sind dann abzuschreiben und es ist zu vermerken, dass das SV-Buch vorgelegen hat. Möglich ist auch eine Kopie mit Schwärzung der nicht relevanten Daten.

Etwas anderes gilt für den Führerschein. Für die Aufgabenerfüllung eines Fallmanagers ist es allenfalls erforderlich zu wissen, ob eine Fahrerlaubnis für welche Fahrzeugklasse vorliegt. Dies kann in der Akte vermerkt werden. Alle anderen personenbezogenen Daten aus dem Führerschein sind in gespeicherter Form nicht erforderlich für die Fallbearbeitung. Das Anfertigen von Ablichtungen ist daher nicht zulässig.

Auch hier gilt allerdings eine Ausnahme, auf die mich der Landkreis hingewiesen hat: Gemäß §§ 1 Abs. 2, 14 SGB II gehört auch die Unterstützung des Leistungsempfängers bei der Eingliederung in Arbeit zu den Aufgaben der SGB II-Behörde. Zu diesem Zweck soll der Landkreis gemäß § 16 Abs. 1 Satz 1 SGB II auch Leistungen zur Arbeitsvermittlung nach den §§ 35 ff. SGB III (also dem Gesetz zur Arbeitsförderung) erbringen. Zu diesen Vermittlungsleistungen gehört auch die Übersendung von Bewerbungsmappen an den Arbeitgeber-Sofortdienst, auf deren Grundlage sich potenzielle

Arbeitgeber ein erstes Bild von möglicherweise in Betracht kommenden Arbeitnehmern machen können. Die Bewerbungsmappe wird zusammen mit dem Arbeitssuchenden erstellt und mit den Bewerbungen anderer an den Arbeitgeber übermittelt. Ist für die Stelle ein Führerschein erforderlich, kann dies mit einer Führerscheinkopie nachgewiesen werden. Für diese Aufgabe des Landkreises erachte ich auch das Kopieren und das Speichern des Führerscheins in der Bewerbungsmappe (und auch nur dort!) als erforderlich und datenschutzrechtlich zulässig.

10.2.13 Befugnisse der SGB II-Behörde zu impliziten Mitteilungen an den Vermieter des Leistungsempfängers

Die Frage, inwieweit die SGB II-Behörde befugt ist, ausdrückliche oder stillschweigende Mitteilungen zum Leistungsbezug des Mieters an dessen Vermieter zu machen, hat sich in verschiedener Hinsicht gestellt:

(1) Das Sozialamt einer sächsischen Großstadt hat ‚seiner' SGB II-ARGE die Weisung erteilt, im Falle von Regelleistungskürzungen nach § 31 Abs. 1 bis 4 SGB II auch außerhalb von dessen Absatz 5, also auch für 25-jährige Leistungsempfänger, die Leistungen für Unterkunft und Heizung durch unmittelbare Zahlung an den Vermieter des Leistungsempfängers zu erbringen, und zwar in allen Fällen, ganz generell. Die ARGE-Leitung hatte dagegen rechtliche Bedenken, auch in datenschutzrechtlicher Hinsicht. Über den Datenschutzbeauftragten der betreffenden Stadt ist die Frage an mich weitergegeben worden. Ich habe der Stadt mitgeteilt, dass ich diese Weisung für aus folgenden Gründen (namentlich auch) datenschutzrechtlich unzulässig halte:

(1.1) Ausgangsüberlegung ist folgende:
Gemäß § 19 SGB II haben erwerbsfähige Hilfebedürftige bei Vorliegen der entsprechenden Voraussetzungen einen Anspruch auf ALG II zur Sicherung des Lebensunterhaltes einschließlich der angemessenen Kosten für Unterkunft und Heizung. Daraus ergibt sich zunächst der Grundsatz, dass die Leistungen dem Hilfebedürftigen persönlich erbracht werden müssen. Ausnahmsweise soll unter den Voraussetzungen des § 22 Abs. 4 SGB II die Leistung an den Vermieter als empfangsberechtigten Dritten erbracht werden.

Eine Direktzahlung an den Vermieter ist gemäß § 22 Abs. 4 SGB II nur zulässig, wenn die zweckentsprechende Verwendung durch den Hilfebedürftigen nicht sichergestellt ist; in diesem Fall hat die Direktauszahlung der Regelfall zu sein, nur in atypischen Fällen darf anders verfahren werden.

Aus der Formulierung dieser Vorschrift - „durch den Hilfebedürftigen" - folgt, dass ein Vorliegen der Voraussetzungen immer im konkreten Einzelfall zu prüfen ist.

Das entspricht auch den Intentionen des Gesetzgebers, der als Beispiel den Fall der Trunksucht oder des fortgesetzt unwirtschaftlichen Verhaltens genannt hat (BT-Drs. 15/1516, Seite 57 zu Absatz 3, jetzt 4). Daraus ergibt sich, dass eine zweckentsprechende Verwendung erst dann nicht sichergestellt ist, wenn aufgrund mehrmaligen entsprechenden Geschehens die Gefahr weiterer zweckwidriger Mittelverwendung besteht. Eine abstrakte Gefahr reicht deshalb nicht.

Begründet wird dies auch mit der Überlegung, dass eine Zahlung an Dritte die Gefahr einer Entmündigung des Hilfebedürftigen in sich birgt und insbesondere dem Grundsatz der Förderung der Eigenverantwortung des besonderen Zieles des SGB II (vgl. § 1 Abs. 1 Satz 1) zuwiderläuft; vgl. zum ganzen Lang in Eicher/Spellbrink, Rdnrn. 97 f. zu § 22 SGB II.

(1.2) Die von den beteiligten Stellen aufgeworfene *Frage* war nun, ob Pflichtverletzungen des Hilfebedürftigen, die die Tatbestände des § 31 Abs. 1 oder Abs. 4 SGB II erfüllen (um Absatz 2 der Vorschrift ging es wohl nicht!), per se den in § 22 Abs. 4 SGB II normierten Regelfall darstellten, wie das Sozialamt offenbar gemeint hat, das überdies im Falle des § 22 Abs. 4 SGB II offenbar atypische Ausnahmefälle gar nicht vorgesehen wissen wollte.

Diese Frage ist jedoch aufgrund des Umkehrschlusses zu verneinen, der sich aus § 31 Abs. 5 Satz 1, 2. Halbsatz SGB II zwingend ergibt: Aus dieser Vorschrift ist zu folgern, dass bei unter 25-Jährigen die Erfüllung der Tatbestände des § 31 Abs. 1 oder 4 SGB II mit der Erfüllung des Tatbestandes des § 22 Abs. 4 SGB II in der rechtlichen Wirkung (sc. für die Zahlung der Kosten für Unterkunft und Heizung) gleichgestellt wird. Daraus folgt, dass dies für über 25-Jährige gerade nicht gelten soll. Nichtsdestoweniger ergibt sich aus der Vorschrift zugleich aber auch, dass die Pflichtverletzungen nach Absatz 1 und die nach Absatz 4 des § 31 SGB II einen Grad an Übereinstimmung mit dem besonderen Unzuverlässigkeitstatbestand des § 22 Abs. 4 haben, der im Rahmen der Anwendung dieser Vorschrift auch bei den über 25-Jährigen zu berücksichtigen ist. Das bedeutet, dass in vielen, vielleicht sogar der Mehrzahl der Fälle, aber eben nicht in allen oder auch nur in so gut wie allen Fällen von Pflichtverletzungen nach § 31 Abs. 1 oder Abs. 4 der Regelfall des § 22 Abs. 4 SGB II gegeben ist.

(1.3) Dabei wird man den Grad der Absenkung des Arbeitslosengeldes II als Umstand anzusehen haben, der objektiv die Gefährdung der zweckentsprechenden Verwendung, im Sinne des § 22 Abs. 4 erhöht, und insoweit wohl begrenzt schematisieren dürfen - nur begrenzt freilich, weil § 22 Abs. 4 eine (Subsumption und) Ermessensausübung im Einzelfall verlangt.

Im Hinblick auf eine dem Gesetzgeber verfassungsrechtlich zuzugestehende typisierende Betrachtungsweise wird man aus der gesetzlichen Regelung wohl folgern können, in welchem Maße in den Fällen des § 31 Abs. 1 oder Abs. 4 *bei über 25-Jährigen* die Direktzahlung an den Vermieter als angemessen anzusehen ist: § 22 Abs. 4 ist ein Regel-Tatbestand für ca. 90 bis 95 % der Fälle, in denen sein Tatbestand erfüllt ist; der Unterschied zu § 31 Abs. 5 SGB II - der, wie gezeigt, darin besteht, dass diese Vorschrift für die Fälle des Absatzes 1 oder Absatzes 4 dieses § 31 gerade nicht die Regel-Rechtsfolgeanordnung des § 22 Abs. 4 ausspricht - dürfte eine Beschränkung auf ca. 65 bis 75 % als Obergrenze bedeuten.

(1.4) Eine generelle Festlegung auf eine Ermessensausübung im Sinne des § 22 Abs. 4 SGB II oder gar auf eine ermessensgebrauchslose Anordnung der Direktzahlung an den Vermieter in der vom Sozialamt der Stadt verlangten Weise wäre daher unzulässig. Aus denselben Gründen gälte dies auch für die damit notwendig verbundene Übermittlung personenbezogener Daten an den Vermieter des Betroffenen. Eine Übermittlung auf der Grundlage von § 67d Abs. 1 SGB X i. V. m. § 22 Abs. 4 SGB II (im Sinne einer implizit die mit der Direktzahlung notwendig verbundene Datenübermittlung erlaubenden Rechtsvorschrift) setzt - eben außerhalb des § 31 Abs. 5 Satz 1, 2. Halbsatz, also bei über 25-jährigen Leistungsempfängern - das Vorliegen aller Tatbestandsmerkmale des § 22 Abs. 4 SGB II voraus.

(1.5) Für eine Einwilligungslösung ist kein Raum.

Einwände gegen meine Auffassung haben weder das SMS noch meine Kollegen in den anderen Bundesländern oder im Bund geltend gemacht, auch nicht das Sozialamt der betreffenden sächsischen Großstadt.

(2) Eine Optionskommune hat angefragt, inwieweit eine Mitteilung der SGB II-Behörde an die Vermieter von Leistungsempfängern darüber zulässig wäre, dass sie dem betreffenden Mieter als Hilfsbedürftigem (Leistungsempfänger) nunmehr für Kosten der Unterkunft keine bzw. nur noch verminderte Zahlungen leiste.

Datenschutzrechtlich handelte es sich bei einer solchen Mitteilung um eine Übermittlung personenbezogener Daten, die gemäß § 67d Abs. 1 SGB X nur aufgrund konkreter gesetzlicher Übermittlungsvorschriften zulässig wäre. Eine solche gesetzliche Grundlage für die hier infrage stehende Übermittlung ist nicht vorhanden. Eine Mitteilung an den Vermieter über die Absenkung oder den Wegfall von Leistungen nach dem SGB II durch die Behörde wäre somit unzulässig.

Gegen einen Hinweis an den Leistungsempfänger, dass dieser seinen Vermieter informieren *könne*, ist datenschutzrechtlich nichts einzuwenden.

Im Falle der Direktzahlung von Kosten für Unterkunft und Heizung durch die Behörde an den Vermieter gemäß § 22 Abs. 4 oder § 31 Abs. 5 Satz 1 2. Halbs. SGB II (oben 1) gilt natürlich anderes: Insoweit ergibt sich die Übermittlungsbefugnis der Behörde als Bestandteil der mit der Befugnis zur Direktzahlung verbundenen Übermittlungsbefugnis; diese muss sich selbstverständlich auch auf eine Verringerung oder Einstellung der Zahlung erstrecken.

(3) Zu den Leistungen für Unterkunft und Heizung nach § 22 SGB II gehört auch, dass gemäß Absatz 3 Satz 1 der Vorschrift die SGB II-Behörde eine bei einem Umzug des Leistungsempfängers anfallende Mietkaution (im Regelfall als Darlehen, Satz 3) übernehmen kann. Einer Petentin war eine solche Leistung zugesichert worden, allerdings mit dem Hinweis, man werde die Kaution unmittelbar an den Vermieter überweisen. Das nun wollte die Petentin auf gar keinen Fall, denn der Vermieter würde ja so erfahren, dass sie Leistungen nach dem SGB II bezog. Nachdem die Behörde ihren diesbezüglichen *Widerspruch* (mit der haarsträubenden Begründung, eine Direktzahlung sei auch bei Nichtvorliegen der Voraussetzungen des § 22 Abs. 4 SGB II zulässig, wenn auch eben nicht obligatorisch, und der Absatz 4 des § 22 SGB II beziehe sich nicht auf den Absatz 3) als unbegründet zurückgewiesen hatte, hatte die Petentin sich an mich gewandt.

Die von der Behörde, der ARGE einer sächsischen Großstadt - nicht der von oben (1) - angekündigte Verfahrensweise hätte einen klaren Datenschutzverstoß dargestellt: Dabei ist der Behörde offenbar klar gewesen, dass mit der Direktüberweisung der Kaution an den Vermieter eine Übermittlung von Sozialdaten verbunden sein würde (nämlich des Datums, dass der Mieter Sozialleistungen bezieht). Die Übermittlung würde nach § 67d Abs. 1 SGB X nur zulässig sein, wenn sie von einer gesetzlichen Übermittlungsbefugnis gedeckt sein würde (vgl. oben 10.2.6). Als gesetzliche Übermittlungsbefugnis kam nur § 69 Abs. 1 Nr. 1 SGB X in Betracht, wonach Sozialdaten übermittelt werden dürfen, soweit dies zur Erfüllung einer gesetzlichen Aufgabe der übermittelnden Stelle, hier also der betreffenden SGB II-ARGE, erforderlich ist. Was hier zur Erfüllung der Aufgabe der Behörde zu tun war, bestimmte sich nach § 22 Abs. 4 SGB II: Die Kaution als Leistung für Unterkunft durfte nur dann unmittelbar an den Vermieter gezahlt werden, wenn die zweckentsprechende Verwendung durch den Bedürftigen nicht sichergestellt sein würde. Etwa, wenn die konkrete Gefahr bestünde, dass der Hilfeempfänger die Kaution anderweitig verbrauchte und nicht an den Vermieter weiterleitete. Das bedeutete aber auch, dass die Direktzahlung und die mit ihr notwendig einhergehende implizite Übermittlung nur auf Grund Prüfung des Einzelfalles und ausgeübten Ermessens zulässig sein würde, s. oben (1). Da bei der Petentin keine Gefahr einer zweckwidrigen Verwendung erkennbar war - sie hatte namentlich ihren Mietzins bisher immer

pünktlich gezahlt - gab es auch keinen Grund, die Kaution unmittelbar an den Vermieter zu überweisen.

Die Petentin hat daraufhin von der ARGE einen Abhilfebescheid erhalten, und die Arbeitsanweisung der Stadt (als des kommunalen Trägers), in deren Befolgung die Behörde ihre falsche Entscheidung getroffen hatte, hat der Sozialdezernent datenschutzrechtlich nachbessern lassen.

Wie im Falle (1) hätte man von dem wirklich großen Verwaltungsträger eigentlich von vornherein zutreffende zentrale Anweisungen für die Rechtsanwendung erwarten müssen.

10.2.14 Datenerhebung durch die SGB II-Behörde betreffend Mietverträge unter Verwandten

Eine Petentin hat mich um Prüfung gebeten, ob sie gegenüber der SGB II-Behörde Angaben zu ihrem Vermieter machen müsse und ob diese Angaben von der Behörde verwendet werden dürften. Ferner wollte sie wissen, ob die SGB II-Behörde Auskünfte vom Vermieter zur Aufteilung der Wohnflächen des Hauses sowie eine Mietbescheinigung verlangen darf. Ich habe dazu wie folgt Stellung genommen:

Ein Sozialleistungsträger darf gemäß § 67a Abs. 1 Satz 1 SGB X nur die Daten erheben, die zur Erfüllung seiner Aufgaben erforderlich sind. Gemäß Absatz 2 der Vorschrift sind die Sozialdaten beim Betroffenen zu erheben. Dieser wiederum ist verpflichtet, all die Tatsachen anzugeben, die für die von ihm beantragte Sozialleistung erheblich sind. Er hat innerhalb des danach Erforderlichen (§ 35 Abs. 2 und § 37 Satz 3 SGB I!) auf Verlangen des Leistungsträgers Beweisurkunden vorzulegen oder ihrer Vorlage zuzustimmen; diese Mitwirkungspflichten ergeben sich aus § 60 Abs. 1 SGB I.

Gemäß § 22 Abs. 1 SGB II übernimmt die SGB II-Behörde die Kosten für Unterkunft und Heizung in der Höhe der tatsächlichen Aufwendungen, soweit diese angemessen sind. Zum Nachweis der angefallenen Kosten genügt in der Regel die Vorlage des Mietvertrages (auch ohne Angabe des Vermieters) und der Nachweis der regelmäßigen Mietzahlungen an den Vermieter - etwa durch Vorlage entsprechender Kontoauszüge. Weitere Angaben darüber hinaus sind für die Aufgabenerfüllung der Behörde nicht erforderlich.

Etwas anderes gilt in den Fällen, in denen der Mietvertrag zwischen Angehörigen geschlossen worden ist. Um einen Missbrauch auszuschließen, hat die Rechtsprechung der Sozialgerichte in Anlehnung an die ständige Rechtsprechung des Bundesfinanzhofes den Grundsatz aufgestellt, dass diese Verträge der Gewährung von Leistungen zur

Grundsicherung nur dann zugrunde zulegen sind, wenn sie bürgerlich-rechtlich wirksam sind und wenn sie außerdem sowohl in ihrer Gestaltung als auch in der Durchführung des Vereinbarten dem zwischen Fremden Üblichen entsprechen (sog. Fremdvergleich), vgl. etwa LSG Baden-Württemberg, Urteil vom 14. März 2008, L 8 AS 5912/06, Rdnr. 23 bei juris. Danach liegt schon ein unwirksamer Mietvertrag vor, wenn die überlassene Mietsache so ausgestaltet ist, dass ein Fremder das Mietverhältnis nicht eingehen würde. Dies ist etwa der Fall, wenn eine Familie von sechs Personen eine Vier-Raum-Wohnung bewohnt und behauptet, mit der einen erwachsenen Tochter ein zur Mitbenutzung des gesamten Wohnraums berechtigendes Untermietverhältnis begründet zu haben (ein nach § 117 Abs. 1 BGB nichtiges Scheingeschäft, so überzeugend LSG Baden-Württemberg, Urteil vom 15. September 2006, Az.: L 8 AS 5071/ 05 mit nicht ganz klarer Unterscheidung zwischen aus Fremdvergleich sich ergebender sozialrechtlicher Unbeachtlichkeit und - nicht durch ihn begründeter - schon rein zivilrechtlicher Unwirksamkeit, Rdnrn. 39 f. bei juris)

Hat die SGB II-Behörde Anhaltspunkte dafür, dass ein Mietvertrag zwischen Angehörigen geschlossen worden ist, hat sie zur rechtmäßigen Prüfung eines Anspruches auf Leistungen für Kosten für Unterkunft und Heizung auch zu ermitteln, ob dies der Fall ist und ob ein wirksamer Mietvertrag vorliegt, sowie insbesondere auch die Daten zu erheben, die einen Fremdvergleich ermöglichen.

Die SGB II-Behörde hatte insoweit zu ermitteln versucht, ob es sich bei der Wohneinheit der Petentin um eine eigene in sich abgeschlossene Wohneinheit handelte. Diese Datenerhebung war für die Aufgabenerfüllung erforderlich und deshalb zulässig. Nachdem die Petentin die ihr angebotenen Termine zur Klärung der Tatsachen nicht wahrgenommen und auch einen Hausbesuch abgelehnt hatte, hat die SGB II-Behörde von der Petentin eine vom Vermieter ausgefüllte Mietbescheinigung mit einer Skizze der Räumlichkeiten und Angaben zu den Nutzungsbefugnissen verlangen dürfen.

10.2.15 Datenerhebung betreffend erwachsene Kinder von Sozialhilfeempfängern

Die erwachsenen Kinder einer erwerbsunfähigen Frau, die übergangsweise Leistungen der Sozialhilfe nach dem SGB XII erhalten hat, haben sich an mich gewandt und um Prüfung gebeten, ob ihre Weigerung, der Sozialhilfebehörde Auskunft über ihre „persönlichen und wirtschaftlichen Verhältnisse“, wie es geheißen hatte, zu erteilen, nicht doch rechtens (gewesen) sei. Außerdem haben sie sich heftig darüber beschwert, dass die Sozialhilfebehörde sich nach dieser Weigerung von ihren Arbeitgebern Auskünfte über das Arbeitsentgelt besorgt und dazu zunächst Auskünfte beim Rentenversiche-

rungsträger über bestehende Arbeitsverhältnisse eingeholt hatte, und das auch noch hinter ihrem Rücken.

Diese Vorgehensweise der Sozialhilfebehörde ist datenschutzrechtlich einwandfrei gewesen:

(1) (Versuchte) Erhebung der Sozialhilfebehörde bei den Kindern:

Da gemäß § 2 Abs. 1 SGB XII Sozialhilfe nur zu gewähren ist, wenn der Antragsteller sich nicht selbst helfen kann oder Leistungen von Angehörigen erhält, und gemäß Absatz 2 dieser Vorschrift die Verpflichtungen Unterhaltspflichtiger durch die Leistung von Sozialhilfe nicht entfallen - sog. „*Nachrang der Sozialhilfe*“ -, ist das Sozialamt verpflichtet, eventuelle Ansprüche des Antragstellers bzw. Leistungsempfängers gegen Unterhaltsverpflichtete zu prüfen.

Gemäß § 117 Abs. 1 Satz 1 und 2 SGB XII haben daher Unterhaltspflichtige über ihre Einkommensverhältnisse Auskunft zu geben. Kinder sind ihren Eltern gemäß §§ 1601, 1602 Abs. 1 BGB zum Unterhalt verpflichtet, wenn die Eltern außerstande sind, sich selbst zu unterhalten. Die seitens der Sozialhilfebehörde angestrebte Erhebung von Angaben zu Einkünften und Vermögen der Kinder war somit für die Aufgabenerfüllung der Sozialbehörde erforderlich und daher gemäß § 67a Abs. 1 SGB X rechtmäßig.

Die Kinder hatten die Auskunft verweigert und auf die bereits beantragte Erwerbsunfähigkeitsrente der Mutter verwiesen. Solange dieser Bescheid jedoch nicht vorlag, die Mutter aber bereits Sozialleistungen erhielt, durfte die Behörde von ihnen Auskunft verlangen.

Dazu war sie zusätzlich auch gemäß § 94 Abs. 1 Satz 1 SGB XII befugt: Danach gehen Unterhaltsansprüche der leistungsberechtigten Person auf die Sozialleistungsbehörde über, soweit diese bereits Leistungen erbracht hat, aber Unterhaltsansprüche bestanden haben. Geltend machen darf (kann) die Sozialhilfebehörde nach § 94 Abs. 4 Satz 1 SGB XII nur, soweit sie die Erbringung von Leistungen den Unterhaltsverpflichteten *mitgeteilt hat*. Vor allem muss sie natürlich feststellen, inwieweit in Anbetracht der Höhe des Einkommens bzw. Vermögens der Unterhaltsverpflichteten überhaupt ein Unterhaltsanspruch bestanden hat, der hat übergehen können. Dazu kann sie den (gemäß § 94 Abs. 1 Satz 1 SGB XII) mitübergegangenen Auskunftsanspruch des Unterhaltsberechtigten aus § 1605 Abs. 1 BGB gegen die Kinder geltend machen. (Auf § 1605 BGB hatte sich die Behörde auch gegenüber den Kindern berufen.)

(2) Nachdem die Kinder die Auskunft verweigert hatten, hat die Sozialhilfebehörde zudem den Rentenversicherungsträger und die Arbeitgeber der Kinder um Auskunft er-

suchen dürfen, also die Daten, die sie von den möglichen Unterhalts- und damit Rückgriffsschuldnern nicht bekommen hatte, bei Dritten erheben dürfen. Das ergibt sich im Einzelnen aus Folgendem:

(2.1) Die Sozialhilfebehörde darf gemäß § 67a Abs. 2 Satz 2 Nr. 2 Buchst. a SGB X i. V. m. § 117 Abs. 4 SGB XII vom Arbeitgeber eines Unterhaltspflichtigen Auskunft über Arbeitsentgelt und andere in der letztgenannten Vorschrift genannte Angaben verlangen und damit Daten ohne Mitwirkung des Unterhaltspflichtigen bei Dritten erheben, wenn eine Datenerhebung beim Betroffenen - etwa wegen dessen Auskunftsverweigerung und damit Verstoßes gegen die Auskunftspflicht aus § 117 Abs. 1 Satz 1 SGB XII - keinen Erfolg gehabt hat und es deshalb von vornherein feststeht (vgl. ansatzweise von Wulffen/Bieresborn Rdnr. 9, Rombach in Hauck/Noftz Rdnr. 96, jeweils zu § 67a SGB X), dass überwiegende schutzwürdige Interessen des Betroffenen, die der Datenerhebung bei einem Dritten entgegenstehen, nicht bestehen.

(2.2) Wenn die Auskunft des Dritten, nämlich des Arbeitgebers, - wie hier - für die Aufgabenerfüllung des Sozialamtes erforderlich war, das Sozialamt aufgrund der Auskunftsverweigerung der primär Auskunftspflichtigen (Kinder) jedoch noch nicht einmal Kenntnis über den Arbeitgeber haben konnte, hat es im Rahmen der Aufgabenerfüllung gelegen, diesen zunächst zu ermitteln. Aus diesem Grund ist es datenschutzrechtlich zulässig gewesen, den Rentenversicherungsträger um Mitteilung des Arbeitgebers zu ersuchen. Die Erhebungsbefugnis folgt aus § 67a Abs. 2 Satz 2 Nr. 1 SGB X: Die zwangsweise Durchsetzung der Auskunftspflicht der Kinder wäre ein unverhältnismäßiger Aufwand gewesen (Voraussetzung nach *Buchst. b* der Vorschrift; vgl. von Wulffen/Bieresborn Rdnr. 8 zu § 67a, a. E.). Da die Erhebung der Besorgung der Angaben gedient hat, zu deren Beibringung die Betroffenen selbst verpflichtet gewesen sind, hat von vornherein festgestanden, dass ein schutzwürdiges Interesse der Betroffenen, das der Erhebung beim Dritten entgegengestanden hätte, ausgeschlossen war (Voraussetzung nach *Buchst. c* der Vorschrift).

Schließlich hat der Rentenversicherungsträger diese Auskunft auf der Grundlage des § 69 Abs. 1 Satz 1, 3. Fall SGB X für die Erfüllung einer Aufgabe der Sozialhilfebehörde erteilen dürfen (Voraussetzung für die Erlaubtheit der Erhebung seitens der Sozialhilfebehörde nach *Buchst. a* des § 67a Abs. 2 Satz 2 Nr. 1 SGB X).

(2.3) Auch die mit der Anfrage beim Rentenversicherungsträger verbundene Übermittlung der Tatsache, dass Erstattungsansprüche gegen die betreffenden Kinder geprüft wurden, ist zulässig gewesen: Gemäß § 69 Abs. 1 Nr. 1 SGB X dürfen Sozialdaten einem anderen Leistungsträger für Sozialleistungen übermittelt werden, wenn dies zur Erfüllung einer gesetzlichen Aufgabe der übermittelnden Stelle erforderlich ist. Das

Sozialamt ist ebenso Leistungsträger im Sinne des § 35 SGB I wie der Rentenversicherungsträger, vgl. § 35 Abs. 1 i. V. m. §§ 28 und 23 SGB I; die Geltendmachung und Durchsetzung von Erstattungsansprüchen des Sozialleistungsträgers gehört zu seinen gesetzlichen Aufgaben.

(2.4) Die Sozialhilfebehörde hatte die Auskünfte auch ‚heimlich', also ohne Benachrichtigung der Betroffenen (Kinder) einholen dürfen, wie sich aus § 67a Abs. 5 Satz 1 (Fall oben 2.2) und Satz 2 *Nr. 3* SGB I i. V. m. § 117 Abs. 4 SGB XII (Fall oben 2.1) ergibt; dies ist datenschutzrechtlich *logisch*: Jeder, der einem Sozialhilfeempfänger gegenüber dem Grunde nach unterhaltspflichtig ist, kann, wie gezeigt, dem Gesetz - eben § 67a Abs. 2 Satz 2 Nr. 2 SGB I i. V. m. § 117 Abs. 4 SGB XII - entnehmen, dass die Sozialhilfebehörde Angaben über das Arbeitsentgelt beim Arbeitgeber in Erfahrung bringen kann und zu bringen hat und daher höchstwahrscheinlich auch wird, wenn er selbst die Auskunft verweigert hat, zu der er verpflichtet gewesen ist.

10.2.16 Die Beteiligung der sächsischen Jugendämter an „ISIS"

Die „Einrichtung eines **I**nformations**s**ystems zur **I**ntensivüberwachung besonders rückfallgefährdeter **S**exualstraftäter" ist Gegenstand einer gemeinsamen Verwaltungsvorschrift (kurz: VwV ISIS) von SMI, SMS und SMJus, die federführend von letzterem erarbeitet worden und am 1. September 2008 in Kraft getreten ist (SächsABl. 2008 Nr. 33 S. 1058). Das Informationssystem soll zum Zweck der Risikobeherrschung die Beobachtung und namentlich den Informationsfluss zwischen den beteiligten Stellen betreffend haftentlassene rückfallgefährdete Sexualstraftäter besser organisieren.

Die VwV ISIS enthält hierfür in Abschnitt V 8 eine an die Jugendämter gerichtete Anweisung zur Übermittlung personenbezogener Daten, die irreführenderweise den Eindruck erweckt, dass die Jugendämter unter den von der Vorschrift genannten Voraussetzungen in größerem oder zumindest nicht unbeträchtlichem Ausmaß zu der betreffenden Datenübermittlung befugt seien.

Die betreffende Regelung lautet wie folgt:

„*V*
Informationsübermittlung
……..
8
Ist ein Proband in das Informationssystem ISIS aufgenommen, informieren das Jugendamt und der soziale Dienst der Justiz die Strafvollstreckungsbehörde insbesondere über Erkenntnisse betreffend das soziale und familiäre Umfeld des Probanden, soweit dies gesetzlich zulässig ist."

„Proband“ ist dabei gemäß Abschnitt II der VwV vereinfacht ausgedrückt ein rückfallgefährdeter Sexualstraftäter.

Das SMJus hat zuletzt die dem Jugendamt für die Befolgung dieser Anweisung zu Gebote stehende Übermittlungserlaubnis vor allem in § 463a Abs. 1 Satz 1 StPO gesehen, es hat aber außerdem auch zu bedenken gegeben, ob nicht zusätzlich § 8a Abs. 4 Satz 2 SGB VIII eine ausreichende Ermächtigungsgrundlage darstelle.

Beides trifft *nicht* zu.

1) Im Falle des § 463a Abs. 1 Satz 1 StPO ist dies unschwer zu erkennen:

Gemäß § 35 Abs. 2 SGB I ist eine Verarbeitung (i. w. S.) von Sozialdaten *ausschließlich* aufgrund einer im SGB X vorgesehenen Erlaubnis zulässig, die, wie § 67d Abs. 1 SGB X speziell für Übermittlungen bestimmt, auch in einem anderen Buch des Sozialgesetzbuches, nicht jedoch in einer außerhalb des Sozialgesetzbuches stehenden Rechtsvorschrift begründet sein kann (so zuletzt auch Urteil des BSG vom 10. Dezember 2008, Az. B 6 KA 37/07 R, bei juris unter Rdnr. 33, m. w. N.). § 71 Abs. 1 Satz 1, vor Nr. 1, SGB X, mit seiner ausdrücklichen Erlaubnis, Sozialdaten zum Zweck der Erfüllung außerhalb des Sozialgesetzbuchs begründeter gesetzlicher Mitteilungspflichten zu übermitteln, macht diese Rechtslage mehr als deutlich.

§ 71 SGB X verweist in seinem *abschließenden* Aufzählungskatalog (so ausdrücklich auch die Begründung zu § 68 [= § 71 n. F.], siehe BT-Drs. 8/4022 Seite 85) indes nicht auf die entsprechende Strafprozessvorschrift. Mit anderen Worten: Angesichts von § 67d Abs. 1 SGB X ist es unzweifelhaft, dass der Katalog des § 71 Abs. 1 Satz 1 zwingend einen Umkehrschluss begründet: Dort nicht aufgeführte Mitteilungspflichten aus anderen Gesetzen begründen keine Übermittlungsbefugnis für unter § 35 Abs. 1 Satz 1 SGB I fallende Stellen wie etwa die Jugendämter. Eine gegenteilige Rechtsauffassung ist nicht vertretbar.

Damit scheidet § 463a Abs. 1 Satz 1 StPO als Übermittlungserlaubnis für das Jugendamt im Anwendungsbereich des Abschnittes V 8 der VwV vollständig aus.

2) § 8a Abs. 4 Satz 2 SGB VIII ist hingegen auf den ersten Blick gut geeignet, den gegenteiligen Eindruck zu erwecken, also denjenigen, als eine Übermittlungsbefugnis für die Jugendämter in Frage zu kommen, die Abschnitt V 8 der VwV voraussetzt.

Bei näherem Hinsehen stellt sich heraus, dass das Gegenteil der Fall ist. Denn:

§ 8a Abs. 4 Satz 2 SGB VIII erlaubt die Datenweitergabe durch das Jugendamt (ausschließlich) an *die anderen zur Abwendung der Gefährdung zuständigen Stellen*. Diese Wendung bezieht sich auf Satz 1 der Vorschrift, in dem als *zur Abwendung der Gefährdung* möglicherweise einzuschaltende zuständige Stellen ausschließlich *sonstige (SGB)-Leistungsträger* (also neben dem Jugendamt), *die Einrichtungen der Gesundheitshilfe und die Polizei* genannt werden.

Daraus folgt, dass in Satz 2 wegen des „*die anderen*“ nur solche Stellen als Datenempfänger (Empfänger einer Information über die Gefahr) in Betracht kommen, die in Satz 1 als (neben dem Jugendamt für die Abwehr der Gefahr) zuständig genannt sind, also nicht die Staatsanwaltschaft und nicht die Strafvollstreckungsbehörde.

Anders ausgedrückt: Der Anwendungsbereich des § 8a Abs. 4 Satz 2 SGB VIII geht, was die Frage der Übermittlungsbefugnis der Jugendämter an Dritte betrifft, nicht über die in § 8a Abs. 4 Satz 1 SGB VIII explizit genannten Stellen hinaus. § 8a Abs. 4 Satz 2 SGB VIII berechtigt das Jugendamt unter den dort genannten Voraussetzungen (namentlich dass die dort genannten Personen nicht selbst tätig werden) im Unterschied zu § 8a Abs. 4 Satz 1 SGB VIII nur zusätzlich, die betreffenden Stellen eigenständig, das heißt *selbst einzuschalten* - und nicht nur wie in den Fällen des § 8a Abs. 4 Satz 1 SGB VIII auf deren Einschaltung *hinzuwirken*. Ich halte den Wortlaut des § 8a Abs. 4 SGB VIII für insoweit eindeutig. Zudem weist übrigens auch die Gesetzesbegründung zu § 8a Abs. 4 SGB VIII die Polizei als geeignete Institutionen zur Abwehr einer Gefährdung aus, die Staatsanwaltschaft wird hingegen nicht erwähnt (BR-DS 586/04 S. 53, 54).

Der Wortlaut der Vorschrift ist unter dem Gesichtspunkt der Beschränkung auf das zur Gefahrenabwehr Tunliche auch sehr sinnvoll. Allerdings erschließt sich dieser Sinn der Vorschrift nur bei genauem Hinsehen.

Die einzige im Anwendungsbereich des Abschnitts V 8 der VwV für die Jugendämter in Frage kommende Befugnis zu einer (unter Abschnitt V 8 der VwV fallenden) Übermittlung an die Strafvollstreckungsbehörde ist § 71 Abs. 1 Satz 1 Nr. 1 SGB X i. V. m § 138 Abs. 1 StGB. Allerdings kommt neben oder statt der Polizei die Strafvollstreckungsbehörde als Übermittlungsempfänger nur in Frage, wenn die Ausführung des „Vorhabens“ noch nicht nah bevorsteht. Hinzu kommt, dass § 138 Abs. 1 StGB keine Sexualdelikte als solche erfasst, sondern in dem hier einschlägigen Bereich nur Mord, Totschlag, Menschenhandel und Menschenraub, und dass es sich um die Kenntnis von einem „Vorhaben“ handeln muss, so dass die Kenntnis einer allgemeinen Rückfallneigung des Probanden nicht für die Erlaubtheit der Übermittlung ausreicht.

Meiner aus dieser Rechtslage, also der nur in extrem seltenen Fällen bestehenden Befugnis der Jugendämter zur Übermittlung an die Strafvollstreckungsbehörde, gefolgerten Empfehlung, die diesbezügliche Übermittlungs-Anweisung in Abschnitt V 8 der VwV wegzulassen oder jedenfalls die Jugendämter ausdrücklich auf § 71 Abs. 1 Satz 1 Nr. 1 SGB X i. V. m. § 138 StGB als die allein in Betracht kommende Übermittlungserlaubnis hinzuweisen, ist man seitens der zuständigen Staatsministerien nicht gefolgt.

Ich habe daraufhin die sächsischen Jugendämter gemäß § 30 Abs. 4 SächsDSG beratend und empfehlend auf diese mögliche irreführende Wirkung aufmerksam gemacht (das Schreiben vom 9. Oktober 2008, Az.: 2-6920.7.6.1/1 ist nachstehend unter 16.2.1 abgedruckt), die dieser Abschnitt der Verwaltungsvorschrift auf die Jugendämter haben kann - damit die Verwaltungsvorschrift nicht insoweit unrechtmäßigen Datenübermittlungen Vorschub leistet. Zu dieser Unterrichtung über meine Rechtsauffassung bestand umso mehr Anlass, als es bereits vor dem Erlass der Verwaltungsvorschrift in ähnlich gelagerten Fällen im Hinblick auf an sächsische Jugendämter gerichtete Übermittlungsanforderungen seitens Strafverfolgungsbehörden oder Strafgerichten erhebliche datenschutzrechtliche Probleme gegeben hatte. Auch ist zu besorgen, dass die dem SMJus unterstehenden Strafvollstreckungsbehörden dessen Rechtsstandpunkt den Jugendämtern gegenüber geltend machen werden.

Das SMJus hat mich an der Erarbeitung der VwV ISIS rechtzeitig beteiligt, es hat jedoch leider die oben dargelegten und von mir wiederholt auch schriftlich geäußerten sozialdatenschutzrechtlichen Überlegungen nicht übernommen. (Das SMS ist in der Frage nicht in Erscheinung getreten.)

10.2.17 Der Einsatz von Jugendlichen als Testkäufern

Fälle sog. Koma-Saufens als Folge der unzulässigen Abgabe von Alkohol an Jugendliche, die bundesweit für Aufregung sorgten, hatten im Berichtszeitraum auch einen sächsischen Landkreis dazu bewogen, eine „Projektgruppe“ bei von diesen durchgeführten Testkäufen durch Jugendliche zu unterstützen.

(1) Koordiniert wurde die Arbeit der „Projektgruppe“ vom Kinderschutzbund, woraus der von mir zur Erteilung von Auskünften (§ 27 Abs. 1, § 28 Abs. 1 SächsDSG) aufgeforderte Landkreis zunächst meine angeblich fehlende Kontrollzuständigkeit herzuleiten versucht hat. Da der Landkreis jedoch selbst eingeräumt hat, dass die Testeinkäufe „unter Einbeziehung des Ordnungsamtes der zuständigen Kommune durchgeführt“ würden, mithin also doch unter Beteiligung einer öffentlichen Stelle, und außerdem mit ‚moralischer’ Unterstützung des LRA, war meine Zuständigkeit selbstverständlich gegeben.

Der weitere Einwand des LRA, ihm seien die persönlichen Daten der ‚erfolgreich' als Testkäufer tätig gewordenen Jugendlichen, insbesondere auch deren Name nicht bekannt, die Anzeigen an das LRA enthielten keine Daten der Jugendlichen, konnte aus verfahrensrechtlichen Gründen nicht einleuchten. Vielmehr war davon auszugehen, dass die Daten der betroffenen Jugendlichen, die als sogenannte Testkäufer eingesetzt wurden, dem LRA, insoweit es die für das Bußgeldverfahren nach § 28 Abs. 4 JuSchG zuständige Stelle ist, im Einzelfall (eines ‚erfolgreichen' Testkaufes) durchaus bekannt waren. Der betreffende Jugendliche ist in einem zu erlassenden Bußgeldbescheid als Zeuge unter Angabe seines vollen Namens und seiner Adresse zu benennen und hat in einer anschließenden Hauptverhandlung im Falle eines Einspruches gegen den Bußgeldbescheid gegebenenfalls mit einer öffentlichen Zeugenvernehmung zu rechnen. Denn bekanntlich ist der Einsatz von V-Leuten als Beweismittel, also von Personen, die Ermittlungsbehörden Informationen über Straftaten verschaffen und deren Identität von der Behörde geheimgehalten werden darf, verfahrensrechtlich beschränkt auf die Aufklärung und Bekämpfung der *schweren und der organisierten Kriminalität*, einschließlich des Rauschgifthandels; dem Einsatz anonymer Gewährsleute sind rechtsstaatliche Grenzen gesetzt: vgl. im Einzelnen Karlsruher Kommentar zur StPO, Rdnrn. 54 f. vor § 48. Dass es sich bei einem anlässlich eines derartigen Testkaufs gegebenenfalls erfolgenden Verstoß gegen die Jugendschutzbestimmungen um eine derartige Straftat von erheblicher Bedeutung handelt, ist nicht ersichtlich; so handelt es sich bei der vorsätzlichen wie auch der fahrlässigen Abgabe alkoholischer Getränke und Tabakwaren an Kinder nach geltendem Recht lediglich um eine Ordnungswidrigkeit (§ 28 Abs. 1 Nrn. 10 und 12 JuSchG).

Daraus war zu folgern, dass das LRA als Ganzes (Öffentlichkeitsarbeit und Mitarbeit von Jugendamt und Ordnungsamt in der „Projektgruppe") und Ordnungsämter durch Datenentgegennahme bei der konkreten Durchführung der Aktionen an der Verarbeitung personenbezogener Daten der Verkaufsstelleninhaber und wohl eben auch der jugendlichen Testkäufer beteiligt waren.

(2) In inhaltlicher Hinsicht bin ich zu folgendem rechtlichen Ergebnis gekommen:

Soweit der Landkreis für die Zulässigkeit derartiger Testeinkäufer auf die Beurteilung der Tätigkeit von Lockspitzeln („agent provocateur") im Strafrecht - unter dem Gesichtspunkt der Auswirkung auf die Strafzumessung für den Täter (vgl. Tröndle/Fischer, Rdnrn. 67 f. zu § 46) bzw. die Strafbarkeit des Lockspitzels unter dem Gesichtspunkt der Anstiftung (a. a. O. Rdnrn. 8 f. zu § 26) - verwiesen hat, so hat dies noch nicht die Frage der Erlaubtheit der durch die Organisierung der Tätigkeit von Lockspitzeln behördlicherseits stattfindenden mittelbaren Datenerhebungs-Tätigkeit beantwortet. Überdies dürfte - wie beim verdeckt ermittelnden Polizeibeamten - eine entsprechende Tat-

provokation durch den als Testkäufer auftretenden Jugendlichen darüber hinaus auch nur dann strafrechtlich ungefährlich sein, wenn bereits zureichende tatsächliche Anhaltspunkte für den Verdacht (entspr. §§ 152, 160 StPO) bestehen, der Täter sei an einer begangenen Tat beteiligt oder zu einer zukünftigen Tat bereit (Tröndle/Fischer, StGB Kommentar, 54. Auflage, § 46 Rdnr. 68). Dass der Einsatz der betroffenen Jugendlichen auf derartige Personen hat beschränkt sein sollen, ist nicht erkennbar gewesen. Deswegen bedürften Datenerhebungen durch Behörden mittels zu Gesetzesverstößen anregender minderjähriger Privater (Verwaltungshelfer?) einer besonderen gesetzlichen Erlaubnis - und die fehlt, was das betroffene LRA auch selbst eingeräumt hat.

Der Einsatz von Jugendlichen im Rahmen derartiger Testeinkäufe durch den Staat findet im Hinblick auf zu verarbeitende Daten der Jugendlichen auch nicht seine Rechtfertigung darin, dass der Einsatz der Jugendlichen nur mit deren Einverständniserklärung sowie einer Einverständniserklärung der Sorgeberechtigten durchgeführt wird. Kraft des verfassungsrechtlichen Grundsatzes des Vorbehaltes des Gesetzes dürfen Träger öffentlicher Gewalt - sei es also das Jugendamt oder das Ordnungsamt oder eine sonstige Stelle (sc. im funktionalen Sinne) innerhalb des LRA - Aufgaben oder vermeintliche Aufgaben nicht mithilfe einer lediglich durch Einwilligung der Betroffenen gerechtfertigten Verarbeitung personenbezogener Daten erledigen. Anders ausgedrückt: Die Träger öffentlicher Gewalt dürfen nicht dort, wo ihnen keine Aufgaben bzw. Befugnisse zur Verarbeitung personenbezogener Daten bzw. zu einer Verarbeitung mittels außergewöhnlicher, insbesondere heimlicher und damit in das Grundrecht auf informationelle Selbstbestimmung besonders eingreifender, Methoden vom Gesetz zugewiesen sind, Aufgaben an sich ziehen oder Ziele verfolgen und sich die nötigen rechtlichen Grundlagen für die Verarbeitung der dafür erforderlichen personenbezogenen Daten durch Einholung von Einwilligungen beschaffen (vgl. zum Einwilligungsgesichtspunkt schon 13/10.2.15 unter 4.3, zum Einsatz außergewöhnlich intensiver Erhebungsmethoden OVG Hamburg 21. März 2007 - 3 Bs 396/05, NJW 2008, 96 = DuD 2007, 931).

Dass es derzeit an einer Rechtsgrundlage gefehlt hat, hat auch der seinerzeit vom Bundesfamilienministerium vorgelegte Entwurf zur Änderung des Jugendschutzgesetzes gezeigt, der wohl den Einsatz von entsprechenden Testkäufern zwischen 14 und 18 Jahren erstmalig vorgesehen hatte, dann allerdings plötzlich nicht weiter verfolgt worden ist, wie der Presse entnommen werden konnte.

(3) Soweit der Landkreis die Rechtmäßigkeit der Erhebung und Verarbeitung personenbezogener Daten im Rahmen der betreffenden Testeinkäufe unter Einsatz von Jugendlichen mir gegenüber schließlich ganz schlicht mit wohltuenden Auswirkungen auf Jugendliche zu rechtfertigen versucht hat, ändert dies an der bestehenden Rechtslage

nichts. Dieser Umstand kann nur eine entsprechende Änderung der derzeit gültigen Rechtsvorschriften begründen, er macht jedoch die Änderung keinesfalls entbehrlich.

Im Ergebnis ist Seitens des Landkreises von dem Einsatz jugendlicher Testkäufer schließlich Abstand genommen worden. Es deutet aber einiges darauf hin, dass das Thema mich weiter beschäftigen wird - und nicht nur mich: Die bei mir eingegangenen Stellungnahmen meiner Kollegen in den anderen Bundesländern, unter denen ich meine oben dargelegte Rechtsauffassung zu Diskussion gestellt habe, sind allesamt zustimmender Natur. Das von mir ebenfalls angeschriebene SMS hat sich mir gegenüber nicht geäußert.

10.2.18 Übermittlung von Sozialdaten durch Jugendämter im Falle von Landtagspetitionen

Wenn sich jemand mit einer Bitte oder Beschwerde an den Landtag wendet (Art. 35 SächsVerf, § 1 SächsPetAG), ist der für die Bearbeitung einer solchen Petition zuständige Ausschuss im Landtag unter anderem berechtigt, Auskünfte einzuholen und sich insbesondere auch Akten zur Einsicht vorlegen zu lassen, wobei die Anforderung der Akten gemäß § 5 Abs. 3 Satz 1 SächsPetAG über die zuständige oberste Behörde des Freistaates zu erfolgen hat.

In diesem Zusammenhang habe ich im Jahre 2008 die Anfrage des Datenschutzbeauftragten einer Kreisfreien Stadt zu beantworten gehabt, ob auch ein Jugendamt Sozialdaten an den Petitionsausschuss des Sächsischen Landtages oder an das SMS übermitteln dürfe.

Hierzu habe ich folgende Rechtsauffassung vertreten:

(1) Während die Übermittlung von Sozialdaten *eines Petenten* durch einen Sozialleistungsträger an den Petitionsausschuss von manchen bereits deshalb für zulässig erachtet wird, weil der Petent mit seiner Eingabe implizit (stillschweigend) einen Antrag auf umfassende Sachaufklärung verbunden und somit in die Übermittlung eingewilligt habe (25. TB LfD Hessen unter. 6.2; 2. TB ThLfD unter. 3.1; 15. TB BfDI unter 9.2.4), erachte ich diese Datenübermittlung für auf der Grundlage der §§ 67d Abs. 1 i. V. m. 69 Abs. 5 und 67c Abs. 3 Satz 1 SGB X zulässig (10/10.2.6. für den Fall der Übermittlung durch die Sozialhilfebehörde über das SMS an den Petitionsausschuss). Danach dürfen Stellen, deren Aufgaben in der Wahrnehmung von Aufsichts-, Kontroll- oder Disziplinarbefugnissen bestehen, die zur Erfüllung ihrer Aufgaben erforderlichen Sozialdaten übermittelt werden. Im Schrifttum sind der Bundesbeauftragte und die Landesbeauftragten für den Datenschutz als derartige Kontrollbehörden anerkannt (Hauck/Noftz SGB X, § 69 Rdnr. 51). Auch der Petitionsausschuss des Landtages nimmt Aufsichts-

und Kontrollbefugnisse auf normenklarer Rechtsgrundlage, auch gegenüber den Jugendämtern, wahr (Art. 35 SächsVerf, § 21 GO LT, SächsPetAG). Es ist daher kein einleuchtender Grund ersichtlich, weshalb nicht auch der Petitionsausschuss eine Kontrollbehörde im Sinne der §§ 69 Abs. 5 i. V. m. 67c Abs. 3 Satz 1 SGB X sein und die Datenübermittlung nicht auf diese Vorschriften gestützt werden können sollte (siehe hierzu 10/10.2.6).

Auf eine *Einwilligung* im Sinne von § 67b Abs. 1 und 2 SGB X als Rechtsgrundlage für die Datenübermittlung kommt es angesichts dessen nicht an. Die gesetzliche Erlaubnis der Aktenübersendung an den Petitionsausschuss umfasst auch Daten Dritter, soweit diese Daten zur Erfüllung der Kontrollaufgaben erforderlich sind, unabhängig von einer zusätzlichen Einwilligung der betroffenen Dritten (s. unten 5 und 6).

(2) Allerdings habe ich eine Übermittlung von Sozialdaten durch ein *Jugendamt* an das *SMS* zur Vorlage an den Petitionsausschuss für unzulässig gehalten, weil die Rechtslage folgende war:

Das SMS nimmt insoweit keine Aufsichtsbefugnisse gegenüber dem kommunalen Träger des Jugendamtes wahr. Die Aufgabe der öffentlichen Jugendhilfe erfüllt der örtliche Träger nach § 69 SGB VIII als Selbstverwaltungsaufgabe. Folglich unterliegt der örtliche Träger auch nicht der Fachaufsicht, etwa ausgeübt durch das Landesjugendamt bzw. das SMS, sondern lediglich der Rechtsaufsicht nach den kommunalverfassungsrechtlichen Vorschriften. Das Landesjugendamt bzw. das SMS ist also keinesfalls übergeordnete Behörde im aufsichtsrechtlichen Sinne, vielmehr unterliegt das Jugendamt der Aufsicht durch das Regierungspräsidium (heute: Landesdirektion) sowie durch das SMI nach § 113 SächsGemO und § 65 SächsLKrO (vgl. Kunkel SGB VIII, 3. Aufl., § 69 Rdnr. 2a).

Meine Rechtsauffassung ist vom Sächsischen Landesamt für Familie und Soziales geteilt worden, das sich folglich nur für die Beratung der Jugendämter zuständig, nicht jedoch als Rechts- oder gar Fachaufsichtsbehörde der Jugendämter gesehen hat.

Der Petitionsausschuss hat daher auch nicht über das SMS bzw. das Landesjugendamt Akten oder Auskünfte eines Jugendamtes anfordern können, da gemäß § 5 Abs. 3 SächsPetAG die Anforderung über die zuständige oberste Behörde des Freistaates zu erfolgen hat und, vor allem, das Jugendamt nach §§ 67d Abs. 1, 69 Abs. 5 SGB X Sozialdaten nur an für es auch zuständige Aufsichtsstellen übermitteln darf. Die zuständige oberste Behörde ist aus den dargelegten Gründen jedoch das SMI, nicht jedoch das SMS gewesen.

So wird auch die Anforderung der Akten eines Amtsvormundes durch einen Petitionsausschuss über die oberste Landesjugendbehörde im Hinblick auf § 68 Abs. 1 Satz 2 SGB VIII als unzulässig angesehen, da auch nach dieser Vorschrift Sozialdaten für Zwecke der Aufsicht und Kontrolle nur von den für den Amtsvormund zuständigen Stellen genutzt werden dürfen. Nach § 1837 Abs. 2 BGB untersteht der Amtsvormund aber nur der Aufsicht des Vormundschaftsgerichtes bzw. des Landesjustizministeriums. Nur über diese Stellen kann der Petitionsausschuss daher in zulässiger Weise die Vorlage von Akten oder Stellungnahmen verlangen, da der Amtsvormund auch nur diesen gegenüber zur Übermittlung von Sozialdaten berechtigt ist (Gutachten des Deutschen Instituts für Vormundschaftswesen vom 24. November 1997, in: Der Amtsvormund 1998, 101 f.).

(3) Aus den genannten Gründen habe ich den Petitionsausschuss gebeten sicherzustellen, dass von einer Anforderung von Akten sowie Auskünften eines Jugendamts beim SMS wie auch von einer Datenübermittlung durch das Jugendamt an den Petitionsausschuss über das SMS abgesehen wird. Die Anforderung von Akten oder entsprechenden Auskünften bei den Jugendämtern seitens des Petitionsausschusses hat gemäß § 5 Abs. 3 SächsPetAG über das SMI zu erfolgen. Die erforderliche Befugnis zur Datenübermittlung der Jugendämter an das SMI zur Weiterleitung durch diese an den Petitionsausschuss ergibt sich, wie bereits genannt, aus §§ 69 Abs. 5 i. V. m. 67c Abs. 3 Satz 1 SGB X.

(4) Nur zur Klarstellung habe ich dabei darauf hingewiesen, dass dies so nur für das *Jugendamt*, nicht aber für die *Sozialhilfebehörde* gilt, gegenüber der das SMS Aufsichtsbefugnisse ausübt, so dass die Datenübermittlung durch diese über das SMS an den Petitionsausschuss stattzufinden hat (siehe 10/10.2.6).

(5) Die Datenübermittlung an den Petitionsausschuss hat sich aufgrund des Verhältnismäßigkeitsgrundsatzes unter dem Gesichtspunkt der Erforderlichkeit auf den zur Erfüllung der Aufgaben der Kontrollbehörde notwendigen Umfang zu beschränken. Da die Kontrollbefugnisse des Petitionsausschusses aber nur dann effektiv wahrgenommen werden können, wenn er sich über den an ihn herangetragenen Einzelfall umfassend, namentlich anhand der vollständigen Behördenakte, informieren kann, ist die Erforderlichkeit weit auszulegen (vgl. 9/10.2.9, S. 147 Mitte).

Im besonderen Sinne von § 65 SGB VIII „anvertraute“ Sozialdaten dürfen dem Petitionsausschuss allerdings nur unter den strengen Erlaubnistatbestandsvoraussetzungen des Absatzes 1 dieser Vorschrift weitergegeben werden. Dies wird auch durch die Verweisung in Absatz 2 auf § 35 Abs. 3 SGB I (Auskunftsverweigerungsrecht) deutlich. Anvertraute Daten in dem von § 65 SGB VIII gemeinten Sinne sind aber nur aus-

drücklich besonders und ganz persönlich einem bestimmten Mitarbeiter des Jugendamtes anvertraute Daten, die dieser deshalb auch gesondert, getrennt von der Sachakte, zu speichern hat (9/10.2.9) und die auch innerhalb der Behörde niemand anderem (Vorgesetztem, Urlaubsvertreter, Nachfolger) zur Verfügung stehen. Für die Weitergabe solcher Daten kann keinesfalls eine konkludente Einwilligung genügen, eine solche ist bereits als Grundlage für die Übermittlung sonstiger personenbezogener Daten zweifelhaft. Vielmehr bedarf es hierfür einer ausdrücklichen und informierten Einwilligung (so auch der BfDI für die Übermittlung sensibler Personalunterlagen an den Petitionsausschuss, 15. TB BfDI unter 9.2.4.)

(6) Darüber hinaus lässt auch § 67d Abs. 3 SGB X die Übermittlung zusätzlicher, nämlich für sich genommen nicht erforderlicher Sozialdaten sowohl des Petenten als auch Dritter unter besonderen Voraussetzungen zu. Andererseits enthält § 64 Abs. 2 SGB VIII eine Einschränkung der Befugnis zur Übermittlung von Sozialdaten nach § 69 SGB X insoweit, als der Erfolg einer zu gewährenden Leistung durch die Übermittlung in Frage gestellt wäre.

(7) Die Sächsische Staatsregierung hatte ausweislich ihrer Stellungnahme zu meinem 9. Tätigkeitsbericht, LT-DS 3/5765, meiner dort unter 10.2.9 bereits vertretenen Rechtsauffassung, wonach die Jugendämter der Rechtsaufsicht (als Teil der allgemeinen Kommunalaufsicht) der RP - und damit implizit auch des SMI, nicht jedoch des SMS – unterliegen, seinerzeit nicht widersprochen, nunmehr sind jedoch seitens des SMI hiergegen Bedenken geltend gemacht worden: Den Einwand, das SMS sei aufgrund des geltenden *Ressortprinzips* und einer daraus resultierenden Berechtigung zu fachrechtlicher Zuarbeit zu einer entsprechenden Verarbeitung personenbezogener Daten befugt, halte ich für unzutreffend: Ressortprinzip und Abgrenzung der Geschäftsbereiche wirken zunächst nur im Innenverhältnis zwischen den Organisationseinheiten der Staatsregierung (vgl. die Rechtsgrundlage für die Geschäftsbereichsverteilung in Art. 59 Abs. 3 SächsVerf, der im Abschnitt „Die Staatsregierung“ steht!). Die Außenwirkung gegenüber den Kommunen, die gemäß Art. 28 Abs. 1 GG, Art. 82 Abs. 2 SächsVerf ihre Aufgaben „im Rahmen [nur !!] der Gesetze“ eigenverantwortlich erfüllen, und gegenüber den Einzelnen (Grundrechtsträger) bedarf dagegen einer gesetzlichen Regelung.

Letzteres betrifft den Umgang mit personenbezogenen (Sozial-)Daten: Die Staatsregierung bzw. ein Staatsministerium (gleich welches) ist gegenüber einer Kommune in deren Eigenschaft als unterer Verwaltungsbehörde eine andere Behörde (im organisatorischen und erst recht im datenschutzrechtlich maßgeblichen funktionalen Sinne), so dass es für Datenweitergaben zwischen ihnen schon deshalb, also unabhängig von dem Umstand der rechtlichen Selbstständigkeit der Kommune gegenüber dem Staat, einer

(verfassungsgemäßen) formellgesetzlichen Ermächtigung bedarf, welche hier unstreitig nicht besteht.

(8) Letztlich ist es bei dem Ergebnis geblieben: Es bedarf einer gesetzlichen Erlaubnis für das SMS, für die Zwecke einer fachgesetzlichen Bewertung von das Handeln der Jugendämter betreffenden Einzeleingaben (Petitionen) personenbezogene Daten zu verarbeiten, wobei sich diese Befugnis nicht aus der Rechtsaufsicht ergeben kann, da diese nicht beim SMS, sondern ausschließlich beim SMI liegt. Die sich aus gesetzlichen Vorschriften ergebende auch *instanzielle* Zuständigkeit der Behörde ist Voraussetzung einer zulässigen Verarbeitung personenbezogener Daten: BVerwG 9. März 2005 - 6 C 3/04, NJW 2005, 2330 = DVBl. 2005, 1234 = DöV 2005, 873 - vielfach auch als Teil der sachlichen Zuständigkeit angesehen, vgl. Kopp/Ramsauer Rdnr. 5a zu § 3 VwVfG.

Auch mein Bayerischer Amtskollege ist - für eine insoweit gleiche Rechtslage in Bayern - seinerzeit zu dem Ergebnis gekommen, dass es keine Quasi-(Fach- oder Rechts-)Aufsicht des Sozialministeriums hinsichtlich einzelner Jugendhilfevorgänge mit entsprechender Datenerhebungsbefugnis gibt - wie dies aber gerade bei der Einzelbearbeitung von Petitionen erforderlich ist (19. TB des Bayerischen Datenschutzbeauftragten, LT-DS 14/5438, dort unter 4.6.1).

(9) Dem von der SK vorgeschlagenen Lösungsweg der Einholung einer Einwilligung des Petenten (und auch anderer Betroffener?) bin ich als *genereller Lösung* entgegentreten: Bei einer Petition, die ein Betroffener an den Sächsischen Landtag richtet, handelt es sich nicht lediglich um die Möglichkeit, außerhalb eines gerichtlichen Verfahrens dem Landtag beziehungsweise dessen Petitionsausschuss seine Belange vorzutragen, wodurch diese letztlich veranlasst werden sollen, das Petitum ganz oder zumindest teilweise für berechtigt zu erklären und den zuständigen Behörden entsprechende Empfehlungen zu geben. Es handelt sich vielmehr, was die Wirkung des Verfahrens betrifft, immer auch um die Überprüfung behördlichen Handelns seitens des Staatsministeriums in einem konkreten Einzelfall. Dieses hoheitliche Handeln der öffentlichen Gewalt bedarf auch einer entsprechenden gesetzlichen Grundlage. Denn kraft des verfassungsrechtlichen Grundsatzes des Vorbehaltes des Gesetzes dürfen Träger öffentlicher Gewalt nicht flächendeckend, in großem Stil Aufgaben oder vermeintliche Aufgaben mit Hilfe einer lediglich durch Einwilligung der Betroffenen gerechtfertigten Verarbeitung personenbezogener Daten erledigen. Anders ausgedrückt: Träger öffentlicher Gewalt dürfen nicht dort, wo ihnen keine Aufgaben bzw. 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 (siehe 13/10.2.15, unter 4.3; vgl. jetzt auch Menzel in DuD 2008, 401).

Ich habe jedoch zugegeben, bis zur Verabschiedung einer gesetzlichen Grundlage eine solche Verfahrensweise übergangsweise mitzutragen, unter der Voraussetzung, dass in jedem Einzelfall die Einholung einer Einwilligung geprüft werden müsste. Für Fälle, in denen neben dem Petenten noch andere Betroffene beteiligt sind, kann dies regelmäßig nicht in Betracht kommen, da mit der notwendig einzuholenden Einwilligung die unzulässige Offenbarung des Vorliegens einer Petition an Dritte verbunden wäre. Diese Vorgehensweise kommt deshalb wohl ausschließlich für solche Fälle in Betracht, bei denen der Petent sich gegen das Vorgehen einer Behörde in seinem Fall beschwert, ohne dass Dritte betroffen sind.

(10) Ich habe schließlich einen Vorschlag für eine entsprechende gesetzliche Regelung erarbeitet, die in Form und Inhalt an Art. 14 des Bayerischen Gesetzes zur Ausführung der Sozialgesetze (Bay AGSG) vom 8. Dezember 2006 angelehnt war. Die Staatsregierung ist erfreulicherweise meinem Lösungsvorschlag vollumfänglich gefolgt und hat diesen - als Ergänzung zum SächsLJHG - in den Entwurf eines „Gesetzes zur Förderung der Teilnahme von Kindern an Früherkennungsuntersuchungen“, LT-DS 4/14409, dort als Artikel 2, übernommen. Diese Vorschrift ist auch im Mai 2009 vom Landtag verabschiedet worden (GVBl. 2009, 379, 380). Damit haben sich meine hartnäckigen Bemühungen gelohnt und es ist eine für alle Beteiligten befriedigende datenschutzgerechte Lösung gefunden worden.

10.2.19 Datenerhebung betreffend Tagespflegepersonen

Ich habe im Berichtszeitraum einige Jugendämter hinsichtlich der Datenerhebung bei Tagespflegepersonen (sog. Tagesmütter und -väter) kontrolliert und festgestellt, dass in einigen Fällen Daten erhoben wurden, die für die Aufgabenerfüllung des Jugendamtes nicht erforderlich waren.

Wie § 61 SGB VIII deutlich macht, ist die Erforderlichkeit zur Aufgabenerfüllung Voraussetzung für eine zulässige Datenerhebung. Dem Jugendamt obliegen nach § 43 SGB VIII die Erteilung einer Erlaubnis zur Kindertagespflege sowie die laufenden Geldleistungen zu deren Förderung nach § 23 SGB VIII. Beide Vorschriften setzen (lediglich) die „Geeignetheit“ der Tagespflegeperson voraus. Dieses Tatbestandsmerkmal ist dem Gesetz zufolge bei einer Person gegeben, wenn sie sich durch ihre Persönlichkeit, Sachkompetenz und Bereitschaft zur Zusammenarbeit mit Eltern und anderen Tagespflegepersonen auszeichnet, siehe dazu § 23 Abs. 3 Satz 1, § 43 Abs. 2 Satz 2 Nr. 1 SGB VIII.

Zur Beurteilung dieser gesetzlichen Voraussetzungen, die bei einer Person vorliegen müssen, ist in der Regel unter anderem das Erheben folgender Daten zulässig:

- tabellarischer Lebenslauf bzw. Vorstellung der Person;
- Konzeption der Tätigkeiten;
- behördliches Führungszeugnis;
- Gesundheitszeugnis, d. h. Bescheinigung des Hausarztes nach § 34 Abs. 1 Nr. 1-20 IfSG;
- Nachweis über die pädagogische Ausbildung gemäß § 3 SächsQualiVO und
- Nachweis über Erste-Hilfe-Kurs.

Bei einem Jugendamt habe ich feststellen müssen, dass alle Tagespflegepersonen darüber hinaus eine „Schufa"-Auskunft sowie eine Unbedenklichkeitsbescheinigung der Stadtfinanzkasse vorlegen mussten.

Die Frage nach der finanziellen Situation der Tagespflegeperson fällt jedoch weder unter das Merkmal der „Sachkompetenz" noch unter das der „Kooperationsbereitschaft". Auch die „Persönlichkeit" einer Tagespflegeperson wird unter dem für das Jugendhilferecht maßgeblichen Gesichtspunkt (Verwaltungszweck) des Schutzes vor Gefahren für das Wohl des Kindes (§ 1 Abs. 3 Nr. 3 SGB VIII) sowie für die Förderung seiner Entwicklung (§ 1 Abs. 1 SGB VIII) nicht durch die wirtschaftliche Situation der Tagesmutter, sondern durch ihr Interesse und ihre Befähigung im Umgang mit Kindern und ihre diesbezügliche Zuverlässigkeit - etwa durch ein Führungszeugnis - bestimmt. Über diese Voraussetzungen kann weder eine Schufa-Auskunft noch eine Unbedenklichkeitsbescheinigung der Stadtfinanzkasse Auskunft geben.

Bei einem anderen Jugendamt habe ich feststellen müssen, dass neben den Angaben zur Tagespflegeperson auch der Ehegatte oder sonstige Lebensgefährte seinen Namen, Geburtsdatum, Geburtsort, Anschrift der Hauptwohnung, Staatsangehörigkeit, Konfession, Schulabschluss, erlernten Beruf, Telefonnummer und Mailadressen angeben musste. Auf meine Nachfrage teilte das Jugendamt mit, es handele sich bei dieser Auskunft um Angaben, die der Ehegatte oder sonstige Lebensgefährte freiwillig machen könne. Allerdings war das aus dem Formular nicht ersichtlich. Begründet wurde die Erhebung zudem damit, dass die Ehe- oder Lebenspartner kurzfristig und punktuell die Ersatzbetreuung für die Kinder in der Tagespflege übernähmen und so eine kurzfristige Erlaubniserteilung für die Ersatztagespflege möglich sei. Die Rechtsgrundlage dafür liege in § 62 Abs. 4 SGB VIII.

Auch diese Erhebung personenbezogener Daten habe ich für unzulässig erachtet. Die Prüfung der Geeignetheit der Tagespflegepersonen im Sinne des § 43 Abs. 2 SGB VIII stellen insoweit nicht auf die Eigenschaften des Ehegatten bzw. sonstigen Lebensgefährten der Tagespflegeperson ab, wenn dieser selbst keinen Antrag auf Zulassung als Tagespflegeperson oder Ersatztagespflegeperson gestellt hat. Auf der Grundlage des

§ 62 Abs. 1 SGB VIII dürfen diese Daten nicht erhoben werden. Aber auch eine Datenerhebung auf der Grundlage einer Einwilligung des Betroffenen wäre unzulässig. Denn solange eine gesetzliche Aufgabe des Sozialleistungsträgers eine Datenerhebung nicht erforderlich macht, kann diese auch nicht auf die Einwilligung des Betroffenen gestützt werden. Dies ergibt sich für den Sozialdatenschutz aus § 67b Abs. 2 SGB X, der die Einwilligung des Betroffenen ausdrücklich nur für die Verarbeitung oder Nutzung von Sozialdaten vorsieht, während § 67a Abs. 1 Satz 1 (Satz 3 und 4 ist eine besondere Fallgruppe) SGB X dies für die Erhebung gerade nicht als Erlaubnisgrund vorsieht. Auch auf § 62 Abs. 4 SGB VIII hat sich das Amt bei dieser Datenerhebung nicht stützen können: Entgegen der Auffassung des Jugendamtes begründet diese Regelung keine Befugnis zur Datenerhebung im Umfeld des Leistungsberechtigten, sondern stellt eine Spezialvorschrift zur Datenerhebung *bei Dritten*, insbesondere gerade bei Leistungsberechtigten, dar.

Ich habe dem Jugendamt ferner mitgeteilt, dass die Erhebung des Datums „Konfession" der Tagespflegeperson ebenfalls nicht für die Aufgabenerfüllung im Sinne des § 43 Abs. 2 SGB VIII erforderlich ist. Auf den Einwand des Jugendamtes hin, dass manche Eltern eine konfessionsangehörige Tagespflegeperson wünschten, habe ich erwidert, dass die Tagespflegeperson die Angabe ihrer Konfession freiwillig machen könne, dass dies jedoch auf den Erhebungsbögen des Jugendamtes nicht ohne Hinweis auf die Freiwilligkeit abgefragt werden dürfe.

Beide Jugendämter sind meinen Anregungen gefolgt und haben die unzulässigen Fragen in den Erhebungsbögen entfernt.

10.2.20 Datenschutzrechtliche Folgen von Fehlern bei der Gutachterbestellung nach § 200 Abs. 2 SGB VII

Eine Petentin hat sich über ihren Rechtsanwalt an mich gewandt, weil sie im Zusammenhang mit einem Verfahren betreffend die Zuerkennung einer Unfallrente vom Unfallversicherungsträger vergeblich die Löschung bestimmter ärztlicher Gutachten und gutachterlicher Stellungnahmen von Ärzten begehrt hatte, über die dieser verfügte. Der Unfallversicherungsträger hatte die Zahlung einer Rente unter Hinweis auf mehrere medizinische Gutachten, welche die Schwere der Beeinträchtigung zum Gegenstand hatten, abgelehnt. Die Petentin hatte gegen den Ablehnungsbescheid Klage vor dem Sozialgericht erhoben und unter anderem geltend gemacht, dass die dem Bescheid zugrunde liegenden ärztlichen Gutachten nicht richtig seien.

Gemäß § 84 Abs. 2 SGB X sind Sozialdaten zu löschen, wenn ihre Speicherung unzulässig ist oder wenn ihre Kenntnis für die verantwortliche Stelle zur rechtmäßigen Er-

füllung der in ihrer Zuständigkeit liegenden Aufgaben nicht mehr erforderlich ist und kein Grund zu der Annahme besteht, dass durch die Löschung schutzwürdige Interessen des Betroffenen beeinträchtigt werden.

Da ich bei meiner Prüfung festgestellt habe, dass zwei der von der Petentin genannten ärztlichen Gutachten nicht Grundlage des Ablehnungsbescheides geworden waren, habe ich den Unfallversicherungsträger aufgefordert, diese beiden zu löschen, da angesichts dessen die Aufbewahrung der Gutachten nicht mehr für die Aufgabenerfüllung des Unfallversicherungsträgers für das Verfahren vor dem LSG erforderlich war. Da sich die zu löschenden Daten auch in der bei dem LSG vorliegenden Behördenakte befanden, musste dieses gemäß § 84 Abs. 5 SGB X von der Tatsache der Löschung benachrichtigt werden.

Ein weiteres Gutachten war deshalb zu löschen, weil es unter Verstoß gegen § 200 Abs. 2 SGB VII zustande gekommen war.

Gemäß § 200 Abs. 2 SGB VII sind dem Versicherten vor Erteilung eines Gutachtenauftrags mehrere Gutachter zur Auswahl zu benennen. Solche medizinischen Gutachten kann der Unfallversicherungsträger zur Prüfung der Leistungsvoraussetzungen in Auftrag geben.

Nach der Rechtsprechung des BSG liegt ein Gutachten im Sinne dieser Vorschrift vor, wenn es als „Gutachten“ angefordert oder sonst wie als solches bezeichnet, erstellt, übersandt oder abgerechnet worden ist. Unabhängig von der rein äußerlichen Bezeichnung ist von einem Gutachten dann auszugehen, wenn es vornehmlich eine eigenständige Bewertung der verfahrensentscheidenden Tatsachenfragen, z. B. des umstrittenen Ursachenzusammenhangs enthält. Setzt sich die schriftliche Äußerung des Arztes allerdings im Wesentlichen mit den eingehenden Gerichtsgutachten auseinander, insbesondere im Hinblick auf deren Schlüssigkeit, Überzeugungskraft oder Beurteilungsgrundlage, ist es nur eine beratende Stellungnahme, für die die Voraussetzungen des § 200 Abs. 2 SGB VII nicht gelten. Diese Regelung ist im Übrigen auch auf solche Gutachten anzuwenden, die der Unfallversicherungsträger während eines Gerichtsverfahrens einholt (siehe zu alledem BSG, Urteil vom 5. Februar 2008, Az.: B 2 U 8/07, juris-Rdnrn. 26 ff.).

Obwohl in dem der Eingabe zugrundeliegenden Fall die funktionelle Leistungsfähigkeit der Patientin hatte begutachtet werden sollen, waren dieser keine Gutachter zur Auswahl benannt worden.

Der Verstoß gegen das Gebot der Benennung mehrerer Gutachter zur Auswahl führt zu einem Anspruch auf Löschung der erhobenen Daten. Bei der Regelung des § 200 Abs. 2

SGB VII handelt es sich bereits wegen ihrer systematischen Stellung im Achten Kapitel des SGB VII um eine datenschutzrechtliche Vorschrift. Dem steht auch nicht die Rechtsprechung des LSG Nordrhein-Westfalen entgegen. Zwar kommt dieses mit der herrschenden Meinung in der Literatur zu dem Ergebnis, dass § 200 Abs. 2 SGB VII lediglich die Rechte des Versicherten stärken und die Transparenz des Verfahrens verbessern soll (LSG NRW Urteil vom 14. Juli 2004, Az: L 17O 106/02, juris-Rdnr. 27). Gleichwohl geht das Gericht nicht so weit, einen Verstoß gegen das Gebot, mehrere Gutachter zur Auswahl zu benennen, als folgenlos anzusehen. Gerade eben die genannten Ziele würden ja dann verfehlt, wenn ein unter solchen Umständen zustande gekommenes Gutachten im weiteren Verfahren verwendet werden könnte. Selbst wenn man jedoch der Norm die datenschutzrechtliche Bedeutung abspräche, so folgte doch die Unzulässigkeit der Speicherung der in dem Gutachten enthaltenen Sozialdaten zumindest aus einem Verstoß gegen Verwaltungsverfahrensrecht.

Zu diesem Ergebnis ist nunmehr auch das BSG gekommen. Es hat festgestellt, dass Verstöße gegen § 200 Abs. 2 SGB VII ein Beweisverwertungsverbot nach sich ziehen (BSG a. a. O. Rdnrn. 50 ff.).

Ich habe den Unfallversicherungsträger aufgefordert, die betreffenden Gutachten zu löschen (vernichten). Weil das der Unfallversicherungsträger abgelehnt hat, habe ich der Petentin empfohlen, über den Löschungsantrag in dem anhängigen gerichtlichen Verfahren entscheiden zu lassen. Die gerichtliche Entscheidung würde dann maßgebend sein.

10.2.21 Forschung durch SGB-Behörden?

Das Jugendamt einer sächsischen Großstadt wollte unter dem Titel „Biographische Erfahrungen von Problemjugendlichen“ zu Jugendlichen, *die ein mehrfaches oder besonders intensives abweichendes Verhalten zeigen bzw. bei denen mehrfach durchgeführte Jugendhilfemaßnahmen bisher ohne ‚Erfolg’ geblieben sind, vor allem zu der Frage, wie solche ‚Maßnahmen’ von den Jugendlichen erlebt worden sind und erlebt werden*, eine „empirische Studie“ durchführen. Dazu sollten „fallführende“ Jugendamts-Bedienstete einer von einer Verwaltungsfachhochschule an die Stadtverwaltung ‚ausgeliehenen’ Dozentin geeignete Fälle mitteilen, deren Akten untersucht werden sollten, und auf dieser Grundlage sollte, soweit die Betreffenden damit einverstanden sein würden, die Dozentin mit den Jugendlichen und deren Sorgeberechtigten sog. narrative Interviews durchführen, bei denen die Probanden aus dem Stegreif ihre ganze Lebensgeschichte erzählen sollten, was auf Tonband aufgezeichnet werden sollte. Als Ergebnis dieser Untersuchung sollten dem Jugendamt allgemeine Schlussfolgerungen zur Wirkung von Jugendhilfemaßnahmen und davon abzuleitende Empfehlungen zur Verfü-

gung gestellt werden. (Im „Anhang der Studie“ sollten biografische Daten und Informationen in anonymisierter Form einem kleinen Kreis ausgewählter Personen zur Nachvollziehbarkeit und wissenschaftlichen Überprüfbarkeit des Ablaufes der Untersuchung zur Kenntnis gegeben werden; Interview-Inhalte sollten nur auf ausdrücklichen Wunsch des betreffenden Jugendlichen den ihm betreuenden Jugendamts-Bediensteten zur Nutzung im Jugendhilfeverfahren übermittelt werden.)

Die Jugendhilfebehörde hat mir gegenüber als Rechtsgrundlage § 62 Abs. 1 und 2 SGB VIII i. V. m. § 65 Abs. 1 Nr. 1 SGB VIII angegeben und erklärt, aufgrund ihrer gesetzlichen Aufgaben sei es für sie *unerlässlich und zwingend erforderlich, neben der Kenntnis aktuellen Fehlverhaltens grundlegende Informationen über Umstände, Lebensumfeld, soziale Einrichtungen und Rahmenbedingungen, in denen Kinder und Jugendliche aufwachsen und die Folgen für ihre jeweils individuelle Entwicklung haben, zu erlangen; es sei ureigenste Aufgabe der Jugendhilfe, vorhandene bis dato teilweise unkoordinierte Hilfeleistungen in ihrem Zuständigkeitsbereich auf die jeweilige Wirksamkeit zu überprüfen*, um diese Leistungen verbessern zu können. Durch die Abordnung der Dozentin sei die einmalige Möglichkeit gegeben, sich als Verwaltung selbst mit der eigenen Aufgabenerledigung intensiver zu befassen und in Art einer *Selbstevaluation* das eigene Handeln zu überprüfen, um Empfehlungen für Verbesserungen zu erlangen - *nur so könne das Jugendamt dem bundesgesetzlichen Auftrag der Planungs- und Gesamtverantwortung (§§ 79 f. SGB VIII) nachkommen*.

Aus den nachfolgend dargelegten Gründen bin ich zu der Auffassung gekommen, dass die im Rahmen des Vorhabens vorgesehene Verarbeitung personenbezogener Daten unzulässig wäre.

Nachdem ich dem Jugendamt mitgeteilt hatte, dass das Sozialrecht keine Forschung durch Sozialleistungsträger vorsehe, dass aber genau das dasjenige sei, was das Jugendamt durch die betreffende Wissenschaftlerin als seine Bedienstete bzw. die Wissenschaftlerin als Bedienstete des Jugendamtes vorhabe, hat es sich mit der von mir dafür gegebenen Begründung - nämlich dass aus § 75 Abs. 1 SGB X im Umkehrschluss folge, dass diese Regelung nur für die Übermittlung, nicht aber für die Erhebung personenbezogener Daten zu Forschungszwecken gilt und dass überdies keine Vorschrift in SGB VIII erkennbar sei, die über § 67a Abs. 1 Satz 1 hinaus die Datenerhebung auf Einwilligungsgrundlage vorsieht und dass überdies die rechtliche Freiwilligkeit einer Einwilligung nicht gesichert sei, weil die Leistungsempfänger, gerade als schon durch „abweichendes Verhalten“ Aufgefallene keineswegs sicher sein könnten, dass eine fehlende Teilnahmebereitschaft nicht auf das Verhalten der ihren Fall bearbeitenden Sachbearbeiter nachteilige Auswirkungen habe - nicht überzeugen lassen, sondern mir

weitere Erwägungen unterbreitet, die die Zulässigkeit des Vorhabens begründen sollten. Diese Erwägungen waren jedoch nicht stichhaltig:

(1) Zunächst kamen die vom Jugendamt genannten Vorschriften § 62 Abs. 1 und 2 und § 65 Abs. 1 Nr. 1 SGB VIII aus folgenden Gründen als Rechtsgrundlage nicht in Betracht:

(1.1) Die geplanten Datenerhebungen wären nicht zur Erfüllung einer dem Jugendamt gesetzlich übertragenen Aufgabe erforderlich gewesen, die Durchführung personenbezogener Erhebungen zu Forschungs- oder Planungszwecken ist gerade keine dem Jugendamt gesetzlich zugewiesene Aufgabe im Sinne des *§ 62 Abs. 1 SGB VIII* i. V. m. §§ 1, 2 SGB VIII, § 52 SGB VIII. Dies gilt auch dann, wenn Gegenstand der Erhebungen von der Tätigkeit des Jugendamtes beeinflusste oder beeinflussbare Sachverhalten sind bzw. das Forschungsergebnis Auswirkungen auf die weitere Arbeit des Jugendamts haben kann oder sogar ganz sicher haben wird. Dies wird nachstehend unter 2 bis 4 näher ausgeführt.

(1.2) Der Hinweis des Jugendamtes auf die Regelung des *§ 65 SGB VIII* ist von vornherein fehlgegangen: Es handelt sich bei dieser Vorschrift um eine Beschränkung der von Hause aus bestehenden *Weitergabe*befugnis, nicht jedoch um eine Daten*erhebungs*befugnis. Mithin kann diese Vorschrift nicht als Befugnis für eine Datenerhebung, auch nicht für eine auf Einwilligungsgrundlage, herangezogen werden. Die Vorschrift besagt nicht etwa, dass das Jugendamt oder einzelne Jugendamtsbedienstete alle personenbezogenen Daten erheben dürfen, die Jugendliche ihm freiwillig ‚anvertrauen'. Zum richtigen Verständnis des § 65 SGB VIII vorsorglich folgende Erläuterung: Die Vorschrift verlangt für die Gewährleistung einer - *über* die ohnehin schon im Normalfall bestehende vertrauensvolle ‚persönliche' Beziehung des „Klienten" zu dem oder den für ihn zuständigen Bediensteten des Jugendamts hinausgehenden - im Einzelfall gesteigerten besonderen Vertrauensbeziehung (die ja wesentliche Inhalte der Beziehung, nämlich Erkenntnisse des Behördenbediensteten, der ‚normalen' Behördennutzbarkeit entzieht), dass es sich um besonders ihm persönlich *anvertraute* Sozialdaten handelt. Die Anforderungen des § 65 SGB VIII sind insoweit erheblich: „Anvertraut" im Sinne dieser Regelung sind die Informationen (Sozialdaten) nur, wenn die Mitteilung „unter dem Siegel der Verschwiegenheit" gegenüber Kollegen und Vorgesetzten erfolgt oder aber derjenige, der die Informationen preisgibt, gegenüber dem betreffenden einzelnen Jugendamtsbediensteten im Sinne einer subjektiven Zweckbindung von dessen Verschwiegenheit (auch) innerhalb der Behörde ausgeht *und* dies ausdrücklich zu erkennen gegeben wird oder aus dem Zusammenhang erkennbar ist. Als Folge dessen sind die einem bestimmten Bediensteten des Jugendamtes in dem von § 65 SGB VIII gemeinten Sinne anvertrauten Daten dann auch *gesondert*, also insbesondere nicht in eine gewöhn-

lichen Behördenakte, zu speichern (siehe hierzu schon 9/10.2.9) und stehen dem Jugendamt als Ganzem nicht zur Verfügung.

(2) Das Vorhaben wäre auch nicht aufgrund anderer Vorschriften als Verwaltungsvollzug auf der Grundlage des SGB VIII anzusehen gewesen. Die vom Jugendamt genannte „Überprüfung der Nachhaltigkeit", „zukünftiges Steuern von Leistungsangeboten" sowie „Selbstevaluation" sind den Aufgabenkatalogen des SGB VIII als eigenständige Aufgaben der Jugendämter nicht zu entnehmen. ‚Ungeschriebene' Aufgaben (das Jugendamt hat von „ureigensten" gesprochen) können keine Grundlage für Grundrechtseingriffe sein, wie nachstehend unter 3 und 4 deutlich wird. Das Vorhaben war nur im Hinblick auf die dem Sozialgesetzbuch zu entnehmenden den laufenden Verwaltungsvollzug (Erbringung der im Gesetz vorgesehene Leistungen im Einzelfall, also für einzelne Kinder und Jugendliche) ergänzenden Aufgaben „*Forschung*" und „*Planung*" zu beurteilen.

(3) Das Vorhaben wäre in sozialdatenschutzrechtlicher Hinsicht wohl am ehesten als *Forschungsvorhaben* anzusehen gewesen.

(3.1) Inwieweit eine *Nutzung* der bei dem Jugendamt bereits aus der Erfüllung seiner Aufgaben nach dem SGB VIII vorliegenden personenbezogenen Daten für die Zwecke des Vorhabens, insbesondere für die Auswahl der Probanden, durch § 67c Abs. 2 Nr. 3 SGB X erlaubt gewesen wäre, hat hier dahingestellt bleiben können. Das heißt, es konnte die Frage dahingestellt bleiben, ob Eigenforschung der Sozialleistungsträger - betreffend ihr Handeln bzw. die Bedingungen ihres Handelns - nur bei ausdrücklicher diesbezüglicher gesetzlicher Aufgabenzuweisung, wie z. B. in § 287 SGB V (nur Datennutzung!) oder §§ 282 f. SGB III, oder aber aufgrund *§ 67c Abs. 2 Nr. 3, Abs. 5, § 67b Abs. 3 SGB X* generell, d. h. auch ohne besondere Erwähnung in dem betreffenden Buch des SGB, als (Annex-)Aufgabe der Behörde anzusehen ist - womit die Stellen nach § 35 SGB I gegenüber anderen Behörden im Sinne weitergehender Datenverarbeitungsbefugnisse privilegiert wären! Diese Frage hat hier deswegen nicht beantwortet zu werden brauchen, weil es an der zusätzlich nötigen Datenerhebungsbefugnis gefehlt hat:

(3.2) Für die einen wesentlichen Teil des Forschungsvorhabens ausmachende Befragung der Probanden, also Erhebung personenbezogener Daten durch eine unter § 35 Abs. 1 SGB I fallende Stelle, mithin für eine unter § 67a SGB X fallende *Datenerhebung*, hat es nicht die nötige eindeutige gesetzliche Grundlage gegeben:

Zwar wird in den bereits genannten drei Vorschriften des SGB X (§ 67c Abs. 2 Nr. 3 und Abs. 5, § 67b Abs. 3 SGB X) vorausgesetzt, dass *Eigen*-Forschung, sofern sie das

eigene Handeln der Behörde oder dessen Voraussetzungen bzw. Bedingungen zum Forschungsgegenstand hat, Aufgabe unter § 35 SGB I fallender Stellen sein kann - oder sogar ist (die Befugnis zur Eigenforschung bejaht von v. Wulffen/Bieresborn Rdnrn. 2, 5 und 11 zu § 75, ferner Seidel im LPK Rdnr. 5 zu § 75 SGB X unter Hinweis auf § 67c Abs. 2 Nr. 3 SGB X; implizit genauso Rombach in Hauck/Noftz Rdnrn. 10 und 16 zu § 75 SGB X).

Dies mag vielleicht sogar zur Folge haben, dass ein Sozialleistungsträger zu Forschungszwecken Sozialdaten bei einem anderen Sozialleistungsträger *erheben* darf (§ 67a Abs. 2 Nr. 1; so wohl vorausgesetzt von v. Wulffen/Bieresborn, wenn er Rdnr. 11 zu § 75 SGB X diese Vorschrift auch auf Eigenforschung angewandt wissen will). Aber diejenige Daten-*Erhebung*, die tatsächlich gerade zu Forschungszwecken hätte erfolgen und beim Betroffenen selbst hätte stattfinden sollen, also die Befragung über die normale Aufgabenerfüllung (vorliegend nach dem Katalog des § 2 SGB VIII) hinaus, wäre eine in klassischer Weise auf *Einwilligungsgrundlage* erfolgende *Erhebung gewesen*: Der *Proband* hätte Fragen beantworten sollen, die dem zu betreuenden „*Klienten*“ nicht gestellt worden wären, jedenfalls mangels Erforderlichkeit für die Erbringung der Sozialleistungen im Einzelfall nicht hätten gestellt werden dürfen.

Die Datenerhebung auf Einwilligungsgrundlage sieht das Gesetz (in § 67a Abs. 1 SGB X) aber eben gerade nicht vor, weswegen sie nach § 35 Abs. 2 SGB I unzulässig wäre. (Unklar von Wulffen/Bieresborn Rdnr. 14 zu § 67c SGB X: Die Befugnis zur Erhebung von Sozialdaten zu Forschungszwecken [sc. durch Sozialleistungsträger] richtet sich nach § 67a SGB X).

Den Vorschriften über den Sozialdatenschutz bzw. über die Verarbeitung personenbezogener Daten im Besonderen wie den Aufgabenzuweisungen des Sozialgesetzbuches insgesamt ist nicht mit der vom Verfassungsgrundsatz des *Vorbehaltes des Gesetzes* in der Ausprägung des Gebotes der Bestimmtheit und Klarheit von Rechtsvorschriften verlangten Deutlichkeit zu entnehmen, dass die wissenschaftliche Erforschung des eigenen Handelns und seiner Voraussetzungen generell Aufgabe der unter § 35 SGB I fallenden Stellen wäre. Zwar setzt Seidel in LPK Rdnr. 6 zu § 67b SGB X, zusammen mit Rombach in Hauck/Noftz Rdnr. 81 zu § 67b SGB X, auf der Grundlage der diesbezüglichen Gesetzesbegründung (BT-Drs.: 12/5187 S. 37) voraus, dass eine *Erhebung* stattfinden soll („Anfrage“), er übersieht dabei aber, dass die aus § 4a Abs. 2 BDSG übernommene (Seidel a. a. O.) Vorschrift *in § 67b SGB X* (anders als in § 4a BDSG!) im Wesentlichen nur das Speichern, Nutzen und Übermitteln, jedenfalls aber nicht das Erheben betrifft.

Die einzige Erwähnung einer *Erhebung* zu Forschungszwecken im Sozialgesetzbuch, nämlich in § 67c Abs. 5 Satz 1 SGB X, ist allem Anschein nach eine unbedachte Übernahme der Formulierung aus § 40 Abs. 1 BDSG (vgl. von Wulffen/Bieresborn Rdnr. 14 und Seidel in LPK Rdnr. 9, jeweils zu § 67c SGB X), die, außerhalb des zweiten und dritten Abschnittes des Bundesdatenschutzgesetzes stehend, auf die Verarbeitung *durch Forschungseinrichtungen* (eben gleich welcher Rechtsform!) zugeschnitten ist (vgl. Gola/ Schomerus Rdnr. 1 zu § 40 BDSG).

(4) Das Vorhaben hat sich auch nicht unter die „Planung“ im Sinne des § 80 Abs. 1 SGB VIII subsumieren lassen:

Diese Planungs-Zwecke sind im Sinne des allgemeinen Verständnisses von Planung im Sozialgesetzbuch vornehmlich als Bedarfs- und Bereitstellungsplanung (Seidel in LPK Rdnr. 6 zu § 75 SGB X) zu verstehen.

Eine *Erhebung* von Sozialdaten eigens zu Planungszwecken (also zusätzlich zum Verwaltungsvollzug im Einzelfall) setzt zwar § 67c Abs. 5 SGB X voraus, im SGB VIII gibt es jedoch keine speziellen Anhaltspunkte (in den §§ 62, 64 Abs. 3) dafür. Die Erwähnung der „Wünsche, Bedürfnisse und Interessen der jungen Menschen“ in § 80 Abs. 1 Nr. 2 SGB VIII wird zwar in der Literatur vielleicht ansatzweise implizit als Befugnis zur Erhebung von Sozialdaten zu diesem Zweck durch den Leistungsträger verstanden (Wabnitz in LPK Rdnr. 15 zu § 80, weniger deutlich Frankfurter Kommentar Rdnr. 13 zu § 80 SGB VIII), aber ohne die Frage zu erörtern, inwieweit die als Mittel der Beschaffung von diesbezüglichen Erkenntnissen erwähnte *Befragung* tatsächlich *personenbezogen* stattfinden soll bzw. darf.

Eine Aufgabenzuweisung, die erkennen ließe, dass die Aufgabe mittels personenbezogener Informationen zu erfüllen ist, fehlt im Gesetz. Daher kann auch insoweit, also wie bei der Forschung, dem Gesetz nicht mit der aus verfassungsrechtlichen Gründen für eine Eingriffsermächtigung nötigen Klarheit entnommen werden, dass - kraft der an die Aufgabenzuweisung anknüpfenden Eingriffsermächtigungen § 62 Abs. 1 SGB VIII, § 67a SGB X - eine Befugnis besteht, zum Zweck der Erfüllung dieser Aufgabe personenbezogene Daten zu erheben und damit in das Grundrecht auf informationelle Selbstbestimmung einzugreifen.

Meiner Aufforderung, von der Durchführung entsprechender Befragungen Abstand zu nehmen, ist die Kommune nach meinem Kenntnisstand gefolgt. Das SMS hat gegen meine Rechtsauffassung keine Einwände erhoben.

10.3 Lebensmittelüberwachung und Veterinärwesen

In diesem Jahr nicht belegt.

10.4 Rehabilitierungsgesetze

In diesem Jahr nicht belegt.

11 Landwirtschaft, Ernährung und Forsten

In diesem Jahr nicht belegt.

12 Umwelt und Landesentwicklung

12.1 Verwendung von Luftbildaufnahmen zur Beitragsbemessung von Abwassergebühren

Städte und Abwasserzweckverbände sind gehalten, die durch das Sächsische Kommunalabgabengesetz geforderte getrennte Gebührenerhebung für Schmutz- und Niederschlagswasser vorzunehmen. Um die Höhe des Entwässerungsentgeltes zu bestimmen, werden durch die kommunalen Unternehmen zunehmend eigene Luftbildaufnahmen von den dem Anschluss- und Benutzungszwang unterliegenden Grundstücken angefertigt. Fragen von Grundstückseigentümern nach der Zulässigkeit dieser Datenerhebung erreichen mich immer wieder.

Der durch die kommunalen Unternehmen hergestellte Personenbezug der Luftbildaufnahme eines dem Anschluss- und Benutzungszwang unterliegenden Grundstücks mit den dazugehörigen Gebäuden dient der dortigen Aufgabenerfüllung und ist nach § 12 Abs. 1 SächsDSG zulässig.

In 9/12 habe ich mich zu der allgemeinen Thematik geäußert (Anmerkung: Der im Beitrag genannte § 11 SächsDSG entspricht inhaltlich dem § 12 SächsDSG der heute geltenden novellierten Fassung des Gesetzes). Die von mir dort vertretene Auffassung ist zwischenzeitlich durch weitere Gerichtsentscheidungen gestützt worden und entspricht der herrschenden Meinung der Datenschutzbeauftragten in Deutschland.

Unabhängig davon ist eine gesetzliche Landesregelung zur Verarbeitung personenbezogener Daten, die bei der Erhebung und Nutzung von Geodaten auf verschiedenen Fachgebieten entstehen können, zur Erhöhung der Rechtssicherheit und der Transparenz der Datenverarbeitung erforderlich. Auf Bundesebene sind entsprechende europarechtliche Vorgaben zur Schaffung einer Geodateninfrastruktur durch das Gesetz über den Zugang zu digitalen Geodaten bereits erfolgt. In Sachsen wird ein Gesetz über das Geoinformationswesen vorbereitet.

13 Wissenschaft und Kunst

13.1 Veröffentlichung von „Dozentenplänen“ im Internet

Im Berichtszeitraum erreichte mich eine Anfrage eines Universitätsprofessors, inwieweit Hochschulen sog. „Dozentenpläne“, nämlich *dozentenbezogene* Übersichten über den Titel, die Zeit und den Raum der Lehrveranstaltung, im Internet veröffentlichen dürfen.

Ich bin zu dem Ergebnis gelangt, dass eine solche Veröffentlichung unzulässig ist. Als Rechtsgrundlage für die Verarbeitung personenbezogener Daten der Dozenten nicht in Betracht kam die Regelung des § 106 Abs. 3 Satz 1 SächsHG in der bis zum 31. Dezember 2008 geltenden Fassung. Danach war die Verarbeitung personenbezogener Daten des Hochschulpersonals nur erlaubt, wenn sie zur Beurteilung des Studienangebots und der Lehr- und Forschungstätigkeit verarbeitet worden sind. Darunter fiel jedoch nur die *amtliche* Beurteilung, also durch die Hochschule selbst. Dafür war jedoch eine Veröffentlichung der Dozentenpläne im Internet nicht erforderlich. Es reichte für eine solche Beurteilung vollkommen aus, dass die Dozenten ihre Stundenpläne den hochschulintern Verantwortlichen mitteilen.

Ebenfalls nicht als Rechtsgrundlage in Betracht kommt § 37 Abs. 2 Nr. 2 SächsDSG, dessen Anwendung neben § 106 Abs. 3 SächsHG (a. F.) meiner Auffassung nach nicht vollständig ausgeschlossen ist. Danach ist eine Veröffentlichung der Daten von Beschäftigten öffentlicher Stellen nur zulässig, wenn diese für die Unterrichtung der Allgemeinheit oder der anderen Beschäftigten erforderlich ist und ihr keine schutzwürdigen Interessen des Betroffenen entgegenstehen. Bei einer Veröffentlichung von Dozentenplänen fehlt es bereits an der Erforderlichkeit der Unterrichtung der Allgemeinheit oder der anderen Dozenten. Die Allgemeinheit - und damit vor allem die interessierte Studentenschaft - muss nicht im Interesse der Funktionsfähigkeit des Hochschulbetriebes erfahren können, wie viele Lehrveranstaltungen bzw. „Stunden“ ein Dozent hält; sie muss sich vielmehr lediglich darüber unterrichten können, zu welchem Gegenstand welche Veranstaltungen wann wo von welchem Dozenten angeboten werden. Diesem Interesse entsprechend werden die Vorlesungsverzeichnisse seit je her thematisch geordnet veröffentlicht. Der Student stellt sich seinen Stundenplan so zusammen, wie er ihn für ein ordnungsgemäßes Studium benötigt oder aus anderen Gründen wählt (sofern ihm nicht ohnehin alles vorgegeben ist). Die Kenntnis, wie viele Stunden jeder einzelne Dozent im Semester hält, muss ihm im Interesse eines ordentlichen Lehrangebotes der Hochschule nicht verschafft werden.

Gleiches gilt für die Kollegen der Lehrkräfte: Für deren Semesterplanung ist ebenfalls nur die Kenntnis des Inhalts der Lehrveranstaltungen der anderen Kollegen erforderlich.

Nur so kann das Angebot aufeinander abgestimmt werden, damit es nicht zu Themen- oder Zeitüberschneidungen kommt. Die Kenntnis, in welchem Umfang die anderen Kollegen lehren, ist für diese Abstimmung nicht erforderlich. Abgesehen davon bedarf es für die Bedürfnisse der Dozentenschaft nicht einer jedermann zugänglichen Veröffentlichung.

Als Rechtsgrundlage für die Veröffentlichung der Dozentenpläne käme grundsätzlich auch § 37 Abs. 2 Satz 1 SächsDSG in Betracht: Dazu müssten alle Dozenten in die Internet-Veröffentlichung der sie betreffenden Daten eingewilligt haben. Die - notwendige - Freiwilligkeit einer solchen Einwilligung wäre jedoch sehr zweifelhaft, und es fehlte an einer Aufgabe der Hochschule, für deren Erfüllung die Veröffentlichung nützlich wäre (vgl. 13/10.2.15 unter 4.3).

Im Übrigen ist die Veröffentlichung der Dozentenpläne im Internet auch nach dem neuen, seit dem 1. Januar 2009 geltenden Sächsischen Hochschulgesetzes nicht zulässig. Die Verarbeitung personenbezogener Daten ist nunmehr in § 14 SächsHSG geregelt. Gemäß § 14 Abs. 2 SächsHSG sind die Mitglieder und Angehörigen der Hochschulen verpflichtet, ihre personenbezogenen Daten anzugeben, soweit diese zur Erfüllung der Aufgaben nach Absatz 1 erforderlich sind. Danach dürfen diese personenbezogenen Daten für den Zugang zum Studium und die Durchführung des Studiums, die Zulassung zu Prüfungen, zur Promotion oder Habilitation, die Evaluation von Forschung und Lehre nach § 9, die Feststellung der Leistung ihrer Mitglieder und Angehörigen, die Erfüllung von Weisungsaufgaben oder Aufgaben der akademischen Selbstverwaltung, die Entwicklungsplanung, Leistungsbewertungen für die hochschulinterne Mittelvergabe und Steuerung, den Abschluss von Zielvereinbarungen, die Kontaktpflege mit ehemaligen Mitgliedern oder die Umsetzung des Gleichstellungszieles verarbeitet werden. Auch für diese Aufgaben ist jedoch eine Veröffentlichung der Dozentenpläne im Internet nicht erforderlich.

Das SMWK hat meine Auffassung in Bezug auf § 106 Abs. 3 Satz 1 SächsHG (a. F.) geteilt.

13.2 Beteiligung von Hochschulbediensteten an der Durchführung einer Umfrage einer gewerkschaftlichen Hochschulgruppe

Eine gewerkschaftliche Hochschulgruppe hatte begonnen, eine Umfrage zu den Arbeitsbedingungen studentischer Hilfskräfte an der Hochschule durchzuführen. Die Umfrage sollte unter Beteiligung von Stellen der Hochschule vonstatten gehen: So waren zunächst die Fragebögen mit einem Begleitschreiben an Dekanate verschickt worden. Diese waren gebeten worden, die Fragebögen über die Hauspost an die jeweiligen Insti-

tute und Lehrstühle weiterzuleiten, damit diese den Fragebogen entsprechend der Anzahl der dort beschäftigten Hilfskräfte vervielfältigen und verteilen könnten. Die ausgefüllten Fragebögen sollten die befragten Hilfskräfte über den Studentenrat, per E-Mail unmittelbar an die Hochschulgruppe oder aber auch über die Hauspost direkt an eine namentlich benannte Hochschulbedienstete an ihrem Arbeitsplatz in einer bestimmten Fakultät („an die Fakultät“ hieß es wörtlich in den Erläuterungen zum Rücklauf) zurückleiten können, die sie alle inhaltlich auswerten sollte. An vier Fakultäten war bereits damit angefangen worden (in den Dekanaten hatte man der Umfrage wohlwollend gegenüber gestanden), als der Datenschutzbeauftragte der Hochschule davon erfuhr und Einwände erhob, und zwar mit Recht. Denn diese unter Nutzung von Hochschuleinrichtungen, genauer gesagt *unter Beteiligung von Bediensteten der Hochschule* durchgeführte Umfrage war, was die Beteiligung der Hochschule, also das Handeln der Hochschule betrifft, datenschutzrechtlich unzulässig (und damit mittelbar auch insoweit, als die Hochschulgruppe selbst tätig gewesen ist, was nicht in meine Zuständigkeit nach § 27 Abs. 1 Satz 1 i. V. m. § 2 SächsDSG fällt):

Die Datensammlung war nicht frei von Personenbezug im datenschutzrechtlichen Sinn. Zwar wurden im Fragebogen keine Namen erhoben, aber über die Angaben zu den Merkmalen „Studiengang“ und „Alter“ sowie die angegebenen Merkmalsausprägungen zu anderen Erhebungsmerkmalen hat unter Heranziehung in den betreffenden Kreisen von Hochschulbediensteten und sonstigen Hochschulangehörigen durchaus erwartbaren Zusatzwissens ein Personenbezug hergestellt werden können. Das Entgegennehmen und Weiterleiten unverschlossener ausgefüllter Fragebögen durch Bedienstete der Hochschule (Sekretariate) war datenschutzrechtlich daher als eine Verarbeitung personenbezogener Daten durch eine öffentliche Stelle anzusehen. Dies galt insbesondere aber auch für diejenige Bedienstete, bei der die Fragebögen haben bzw. hätten abgegeben werden können und die sie auswerten sollte.

Eine solche Verarbeitung personenbezogener Daten konnte auf keine gesetzliche Grundlage gestützt werden. Weder § 106 Abs. 3 SächsHG (a. F.) noch § 37 SächsDSG enthält eine solche Erlaubnis. Mangels einer solchen Erlaubnis hat die Erhebung nicht rechtmäßig durchgeführt werden können. Die Freiwilligkeit der Datenhingabe hat daran nichts ändern können - auch dann nicht, wenn die Befragten über die Risiken einer Erkennbarkeit ihrer Person aufgeklärt worden wären. Die Durchführung von Primär-Statistiken ist den Hochschulen im Sächsischen Statistikgesetz (vgl. § 2 Abs. 1) nicht erlaubt, auch nicht auf freiwilliger Grundlage (Argument für letzteres: § 6 Abs. 3 Satz 1, Abs. 6 Satz 2 SächsStatG).

Eine Umfrage der Hochschulgruppe ohne Beteiligung universitärer Stellen, also ohne zutun von Hochschulbediensteten, wäre demgegenüber datenschutzrechtlich zulässig gewesen.

Der Kanzler der Hochschule hat meinem Wunsch entsprechend den Vorgang zum Anlass genommen, die Fakultäten - denn an diese hatte sich die Hochschulgruppe unmittelbar gewandt - auf die Rechtslage hinzuweisen.

13.3 Gewährung von Einsicht in Gerichtsakten zu Forschungszwecken

Im Berichtszeitraum wurde ich um die Abgabe datenschutzrechtlicher Stellungnahmen hinsichtlich der Einsichtsgewährung in Gerichtsakten zu Forschungszwecken gebeten. Ich habe mich insoweit geäußert, als im Einzelfall meine Kontrollzuständigkeit betroffen war, was sich wiederum aus den Regelungen der jeweils einschlägigen Prozessordnung ergibt: So wird, soweit ersichtlich, einhellig die Auffassung vertreten, die Entscheidung über die Gewährung von Akteneinsicht nach *§ 34 FGG* sei auch im Hinblick auf nicht am Verfahren Beteiligte ein Akt der Rechtsprechung und falle nicht in die Befugnis der Justizverwaltungsbehörde (statt vieler: OLG Hamm, Beschluss vom 19. Januar 2004, FG Prax 2004, 141), mit der Folge, dass insoweit die Entscheidung über die Gewährung von Akteneinsicht gemäß § 27 Abs. 4 SächsDSG nicht der Kontrollzuständigkeit des Sächsischen Datenschutzbeauftragten unterliegt. Hingegen besteht eine solche bei der Gewährung von Akteneinsicht nach *§ 299 Abs. 2 ZPO* (oder, erst recht, nach *§ 36 Abs. 1 SächsDSG*), also an Personen, die nicht verfahrensbeteiligt sind, weil es sich insoweit um Justizverwaltungsangelegenheiten handelt.

Soweit es sich bei den Verfahren, die für Forschungszwecke herangezogen werden sollen, um sogenannte Verbundverfahren handelt, also zum Teil die Zivilprozessordnung anwendbar ist, gilt Folgendes:

Maßgebliche Ermächtigungsgrundlage für eine Übermittlung personenbezogener Daten durch Gewährung von Einsicht in die Verfahrensakten zugunsten eines Forschungsvorhabens ist, entgegen der in der Literatur zum Teil vertretenen gegensätzlichen Auffassungen nicht § 299 Abs. 2 ZPO: Die von mir in 8/5.8.2 unter 1-3 angestellten Überlegungen sind weiterhin gültig. Unverändert gilt auch (a. a. O. unter 4), dass § 299 Abs. 2 ZPO (eben im Unterschied zu § 34 FGG, wenn man die oben genannten h. M. zu dieser Vorschrift zugrunde legt) der ergänzenden Anwendung solcher Vorschriften aus den allgemeinen Datenschutzgesetzen, welche speziell die Erlaubnis einer Datenübermittlung *zu Forschungszwecken* aussprechen, nicht entgegensteht. Maßgebliche Vorschrift

dafür ist seit der Novellierung im Jahr 2003 § 36 Abs. 1 SächsDSG, der nicht mehr zwischen der Übermittlung an öffentliche und an private Stellen unterscheidet.

Eine Nutzung der in den Gerichtsakten vorhandenen personenbezogenen Daten durch vollständige Beseitigung des Personenbezuges dadurch, dass die Gerichte von den Akten bzw. den für das Forschungsvorhaben interessanten Teilen der Akten Ablichtungen anfertigen, in denen die Namen und Anschriften sämtlicher darin vorkommender Privatpersonen geschwärzt werden, wäre unproblematisch. Inwieweit eine solche Einschränkung den Erfolg des Forschungsvorhabens beeinträchtigen könnte, ist jeweils im konkreten Einzelfall zu beurteilen.

Die Gewährung von Akteneinsicht ohne vorherige Beseitigung des Personenbezuges, also eine Übermittlung personenbezogener Daten, wäre nur unter Einhaltung der Anforderungen des § 36 Abs. 1 SächsDSG zulässig und setzte danach voraus, dass,

a) die Durchführung des Forschungsvorhabens ohne die Datenübermittlung nicht oder nur mit unverhältnismäßigem Aufwand möglich wäre und
b) ferner das öffentliche, insbesondere das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse der Betroffenen am Unterbleiben der Verarbeitung überwöge.

Eine diesbezügliche Bewertung hängt dabei auch davon ab, ob die zu untersuchenden Verfahren eventuell höchst sensible Belange betreffen (ich denke dabei insbesondere an familiengerichtliche Verfahren) mit der Folge, dass die Betroffenen eher ein schwerwiegendes Interesse am Unterbleiben der Verarbeitung ihrer personenbezogenen Daten haben dürften. Auch dies ist daher einer Entscheidung im jeweiligen Einzelfall vorbehalten.

Bei früheren Justizforschungsvorhaben habe ich mich damit einverstanden erklärt, dass dann, wenn die Anonymisierung einen Aufwand erfordern würde, der, wegen der ohnehin schon bestehenden übermäßigen Arbeitsbelastung gerade der Justiz, von der aktenführenden Stelle nicht geleistet werden kann, diese nicht durch die abgebende Stelle, also das Gericht selbst, sondern durch einen Mitarbeiter des Forschungsinstituts erfolgen darf - aber nur *unter der Voraussetzung*, dass dieser Mitarbeiter nicht an der weiteren Durchführung des Forschungsvorhabens beteiligt ist und vor der Aufnahme seiner Tätigkeit die nach § 6 SächsDSG erforderliche Datengeheimnisverpflichtungserklärung abgibt.

Daran halte ich auch weiterhin fest.

Siehe auch 10.2.21.

14 Technischer und organisatorischer Datenschutz

14.1 Behördeninterne Regelungen für den Einsatz der Informationstechnik, E-Mail und Internet

Es gibt eine Reihe von Konzepten, Dienstvereinbarungen oder Dienstanweisungen, Regelungen zum IT-Betrieb oder andere Festlegungen, die datenschutzrelevant werden können. Es ist festzulegen, wer verantwortlich für die Erstellung, Verabschiedung und Umsetzung der Konzepte ist. Dabei ist zu prüfen, inwiefern die Regelungen durch den Personalrat mitbestimmungspflichtig sind.

Ich habe die Musterdienstvereinbarungen und -anweisungen den aktuellen technischen Entwicklungen angepasst und diese als Beispielvorlage für Kommunen zur weiteren Nutzung im Internet veröffentlicht (http://www.saechsdsb.de/informationen-oeb/arbeitshilfen-oeb).

Folgende Dokumente sind aktualisiert als doc-Dokumente verfügbar:

Musterdienstvereinbarungen
- Dienstvereinbarung über die Nutzung elektronischer Kommunikationssysteme (E-Mail)
- Dienstvereinbarung über die Nutzung des Internets
- Dienstvereinbarung zur Einführung bzw. Anwendung von TK-Anlagen

Musterdienstanweisungen
- Dienstanweisung über die Organisation des Informations- und Datenschutzes
- Dienstanweisung für die Übermittlung vertraulicher Nachrichten mit Hilfe von Telefax-Geräten
- Dienstanweisung für den Einsatz der Informationstechnik

14.1.1 Technische und organisatorische Regelungen

Bei der Prüfung der Dienstanweisungen bzw. Dienstvereinbarungen der Kommunen musste ich mehrfach feststellen, dass die technischen und organisatorischen Regelungen zur Nutzung der Informationstechnik (IT), Internet und E-Mail unzureichend, nicht vollständig oder veraltet waren.

Im Folgenden werde ich auszugsweise auf häufig festgestellte Mängel eingehen.

Soweit dem Benutzer Vorgaben zur datenschutzgerechten Nutzung der IT-Systeme gemacht werden, sollten diese in einer Dienstanweisung oder -vereinbarung zusammengefasst werden. Dabei ist es möglich, zwischen einzelnen Benutzergruppen zu differen-

zieren und jeweils eine Dienstanweisung für Administratoren, für IT-Nutzer oder die Nutzung von Fachverfahren zu erstellen.

14.1.1.1 Grundsätze der E-Mail und Internet-Nutzung

E-Mail sowie Internet werden in vielen Behörden ohne ausreichende Regelung der Verantwortlichkeiten und der Einhaltung des Datenschutzes genutzt. Insbesondere haben die meisten Kommunen keine oder nicht ausreichende Vorgaben für die private Nutzung dieser Dienste.

Der Arbeitgeber ist nicht verpflichtet, die private Nutzung von E-Mail und Internet am Arbeitsplatz zu gestatten. Ob und in welchem Umfang Internet oder E-Mail auch privat genutzt werden kann, muss in der Dienstvereinbarung geregelt werden, um unklare Situationen oder Streitigkeiten zu vermeiden. Derzeit kann für eine Regelung der privaten Nutzung keine Empfehlung abgegeben werden, da umfangreiche rechtliche Aspekte und die damit verbundenen Folgen zu berücksichtigen sind.

Wenn ein Arbeitgeber den Beschäftigten die *private Nutzung* von Internet oder E-Mail erlaubt, gelten die Vorschriften des Telekommunikationsgesetzes, da der Dienstherr in diesem Fall seinen Beschäftigten gegenüber die Funktion eines TK- bzw. Telemediendienste-Anbieters (Providers) wahrnimmt. Dabei dürfen die Verbindungs-, Nutzungs- und Abrechnungsdaten nur verarbeitet und genutzt werden, soweit dies für die Erbringung und Abrechnung der Dienste erforderlich ist. Der Arbeitgeber ist dann gegenüber den Beschäftigten und den Absendern der E-Mail zur Einhaltung des Fernmeldegeheimnisses nach *§ 88 TKG* verpflichtet. Abhängig von der technischen Ausgestaltung kann dies auch Auswirkungen auf die dienstliche Internet- und E-Mailutzung (u. a. bei der Kontrolle) haben. Sofern der Arbeitgeber die private Nutzung duldet, kann dies ebenso zur Folge haben, dass er Anbieter im Sinne des Telekommunikationsgesetzes wird.

Bei der Nutzung von E-Mail und Internetdiensten durch die Beschäftigten sind die eingesetzten Verfahren entsprechend dem Grundsatz der Datenvermeidung und Datensparsamkeit technisch so zu gestalten, dass von vornherein so wenige personenbezogene Daten wie möglich verarbeitet werden. Hierzu sind datenschutzfreundliche Verfahren einzusetzen. Auch die Kontrolle der Nutzung dieser Dienste durch den Arbeitgeber ist so zu gestalten, dass sie zunächst ohne, zumindest aber mit so wenigen personenbezogenen Daten wie möglich durchgeführt wird. Dabei sind präventive Maßnahmen gegen

unbefugte Nutzung, wie z. B. Positivlisten erlaubter Internet-Adressen, nachträglichen Kontrollen vorzuziehen.[1]

14.1.1.2 Verwendung von Passwörtern

Aus gegebenem Anlass weise ich erneut auf die Verwendung aktueller Passwortverfahren hin.

Werden in einem IT-System Passwörter zur Authentisierung verwendet, so ist die Sicherheit der Zugangs- und Zugriffsrechteverwaltung des Systems entscheidend davon abhängig, dass das Passwort korrekt gebraucht wird. Die Zeichenzusammensetzung des Passwortes muss so komplex sein, dass es nicht erraten oder durch einfaches Ausprobieren ermittelt werden kann. Aus heutiger technischer Sicht gelten Passworte als sicher, die aus mindestens acht Zeichen bestehen und dabei drei der vier Zeichengruppen (Großbuchstaben, Kleinbuchstaben, Zahlen, Sonderzeichen) beinhalten. Immer wieder stelle ich fest, dass insbesondere die Passwortlänge von mindesten acht Zeichen in der Praxis oft nicht eingehalten wird.

Es kommt jedoch nicht nur auf die Entscheidung für ein geeignetes Passwort selbst an; wichtig sind ebenso die Umstände seiner Verwendung.

Die auf meiner Internetseite veröffentlichte Musterlösung zur Passwort-Sicherheit, das Merkblatt und Beispiel zur Passwortbildung in der Musterdienstanweisung Informationstechnik sollen dabei helfen, geeignete Verfahren auszuwählen (http://www.saechs-dsb.de/informationen-oeb/kontrollpraxis-oeb/83-passwort-sicherheit).

14.1.1.3 Verschlüsselung von E-Mails

E-Mail-Korrespondenz ist in den meisten Behörden selbstverständlich geworden. Leider ist nicht allen Anwendern bewusst, dass sie mit dem Internet ein offenes Kommunikationsmedium nutzen und die Kommunikation mit erheblichen Gefährdungen des Datenschutzes und der Datensicherheit verbunden ist.

So ist es nicht transparent, welchen Übertragungsweg die Daten nehmen oder über welche Vermittlungsrechner die Daten übertragen werden. Bei der Datenübermittlung über das Internet können die E-Mail-Inhalte durch Dritte gelesen werden. Eine gezielte Manipulation oder unbefugte Verwendung von Informationen kann somit nicht ausgeschlossen werden. Die Vertraulichkeit der Übermittlung entspricht etwa der einer Postkarte. Im Weiteren bestehen Risiken durch falsche Adressierung oder Weiterleitung der E-Mails. Dennoch wird ein Großteil an E-Mails noch unverschlüsselt versendet. Das

[1] Quelle: „Orientierungshilfe zur datenschutzgerechten Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz“ (www.datenschutz.sachsen.de) oder Entschließung der 63. DSK.

Risiko der modernen Kommunikationstechnologie wird oft nicht erkannt und somit die eigene konkrete Gefährdung meist unterschätzt. Dies belegen auch Studien, u. a. durch das BSI[2].

Aus diesem Grund empfehle ich, dass der Einsatz der elektronischen Post ohne zusätzliche Sicherheitsvorkehrungen (z. B. elektronische Signatur oder elektronische Verschlüsselung) nur für Nachrichten zulässig ist, die keine personenbezogenen Daten oder sonstigen schützenswerten Informationen enthalten oder die nicht der Schriftform bedürfen. Sonstige schützenswerte Informationen sind solche, bei denen ein hohes Risiko für deren Missbrauch besteht. Dazu gehören Daten, die z. B. dem Steuergeheimnis, dem Sozialgeheimnis und dem Fernmeldegeheimnis unterliegen. Den Beschäftigten sind zur Einhaltung der Sicherheit und des Datenschutzes mitzuteilen, welche Dokumente oder Daten elektronisch versendet werden dürfen.

Im Weiteren empfehle ich, bei externem Versand von E-Mails alle Dateianhänge (z. B. Word-Dokumente) in das PDF-Format umzuwandeln, sofern sie nicht vom Empfänger weiterzuverarbeiten sind. Vor der Versendung sind alle nicht erforderlichen verborgenen Daten des jeweiligen Dokuments zu entfernen (Autor, Speicherort, Version usw.).

14.1.1.4 Mobile Datenträger

Die Verwendung von USB-Anschlüssen ist mit vielen Risiken, aber auch mit Vorteilen verbunden. Den Risiken muss mit angemessenen Maßnahmen begegnet werden. Praktisch jeder derzeit verkaufte PC ist mit USB-Schnittstellen ausgestattet, über die externe Geräte wie USB-Festplatten, Tastatur, Maus und Arbeitsplatzdrucker angeschlossen werden sowie Netzwerk- oder WLAN-Verbindungen hergestellt werden können. Frei zugängliche mobile Datenträger sind nicht gegen Beschädigung oder Entwendung geschützt. Aufgrund ihrer geringen Größe sind die beweglichen Datenträger (insbesondere USB-Sticks) leicht zu entwenden. Daher sollten folgende Mindestvorgaben für den Umgang mit externen Datenträgern vereinbart werden.

Personenbezogene oder schützenswerte Daten auf elektronischen Datenträgern (z. B. PCs, Notebooks oder mobilen Datenträgern) sind durch geeignete Maßnahmen vor unberechtigten Zugriffen zu schützen, beispielsweise durch Verschlüsselung. IT-Systeme wie Notebooks oder Mobiltelefone und deren Anwendungen sollten durch PINs oder Passwörter geschützt werden. Datenträger (wie z. B. USB-Sticks, Memory-Karten, CDs, DVDs) mit personenbezogenen Daten oder Programmen dürfen nur in den für sie bestimmten Räumen aufbewahrt und nur von Berechtigten befördert und benutzt werden. Datenträger, die vorübergehend nicht verwendet werden, sind einzuschließen,

[2] Schultze-Melling, IT-Sicherheit in der anwaltlichen Beratung, CR 2005, 73. , S. 13; http://www.bsi.bund.de/literat/jahresbericht/jahresbericht_2004/bsi_jahresbericht2004.pdf.

so dass sie vor unbefugtem Zugriff geschützt sind. Werden Datenträger auf Dauer nicht mehr benötigt, sind sie in einem Archiv zu deponieren. Datenträger mit Originaldaten müssen besonders gesichert aufbewahrt werden (z. B. in einem Tresor). Die Daten von mobilen Datenträgern dürfen erst nach Überprüfung auf Virenbefall eingespielt werden.

Außerhalb der Dienststelle sind die Benutzer für den Schutz der ihnen anvertrauten IT verantwortlich. Bei Dienstreisen sind daher besondere Vorsichtsmaßnahmen zu ergreifen. Die IT-Systeme sollten nicht unbeaufsichtigt gelassen werden. Insbesondere sollten sie nicht in Fahrzeugen oder öffentlichen Verkehrsmitteln zurückgelassen werden.

Weitergehende Informationen:
- *Datensicherheit bei USB-Geräten*
  Arbeitskreis „Technische und organisatorische Datenschutzfragen“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Stand: November 2003;
- *Umgang mit USB-Speichermedien*
  Bundesamt für die Sicherheit in der Informationstechnik, IT-Grundschutzhandbuch, (https://ssl.bsi.bund.de/gshb/deutsch/m/m04200.htm)

14.1.1.5 Nutzung von drahtlosen Netzen (WLAN)

Defizite bestehen insbesondere in den Bereichen der Nutzung von drahtlosen Netzwerken (WLAN) in den Behörden. Falls die Notwendigkeit besteht, drahtlose Verbindungen zu externen Netzwerken (z. B. über WLAN) aufzubauen, ergeben sich daraus hohe Risiken für die IT-Sicherheit. Besonders sicherheitskritisch ist, dass in der Praxis für die Übertragung von E-Mails über WLAN-Anschlüsse (z. B. an Bürgermeister) immer noch der bereits veraltete Verschlüsselungsstandard (WEP) angewendet wird. Ferner fehlen in den Behörden Sicherheitskonzepte, Sicherheitshinweise oder Dienstweisungen bzw. -vereinbarungen zur Nutzung dieser drahtlosen Netze.

Eine wesentliche Sicherheitsmaßnahme bei der Nutzung von drahtlosen Netzen ist die Aktivierung der Verbindungsverschlüsselung. Sämtliche nicht verschlüsselte Informationen könnten sonst einfach mitgelesen werden (sniffen). Der Einsatz der Verschlüsselung ist auch eine Maßnahme zum Schutz vor ungesetzlichem Missbrauch des Funknetzes durch Dritte. Als sichere Verschlüsselungsmethode ist derzeit mindestens WPA vorzusehen. Vom Einsatz des WEP-Verschlüsselungsstandards ist grundsätzlich abzuraten. Langfristig soll WPA2 - dieser basiert vollständig auf dem neuen Sicherheitsstandard IEEE 802.11i - verwendet werden. Dieser gilt zurzeit als nicht zu entschlüsseln, solange keine trivialen Passwörter verwendet werden, die über eine Wörterbuch-Attacke gebrochen werden können. Das Passwort muss daher eine ausreichende Länge (maximale Schlüssellänge ausnutzen) und Komplexität (Ziffern, Klein- und Großbuchstaben, auch Sonderzeichen) aufweisen.

Über den WLAN-Zugang darf der Nutzer in keinem Fall eigenständig entscheiden. Damit das geschaffene Sicherheitsniveau nicht unterlaufen werden kann, sind durch die verantwortliche IT-Stelle alle angemessenen technischen Maßnahmen zu ergreifen, um die Einrichtung von Netzwerkverbindungen durch Mitarbeiter zu unterbinden. Diese sind insbesondere die Sperrung aller USB- und WLAN-Anschlüsse am PC sowie die Sperrung administrativer Berechtigungen für Standardnutzer am PC, um zu verhindern, dass Benutzer zusätzliche WLAN-Adapter (z. B. über USB) anschließen können und somit die vorgegebene Konfiguration umgangen wird. Da Verstöße gegen diese Vorgabe das Sicherheitsniveau des gesamten internen Netzwerkes erheblich verschlechtern, sind die Mitarbeiter bei der Eröffnung des Internet-Zugangs darauf in der gebotenen Ausführlichkeit hinzuweisen. Alle technischen und organisatorischen Maßnahmen für den Zugang zum Internet oder zu Netzwerken Dritter sind im IT-Sicherheitskonzept zu dokumentieren.

Die Integrität und die Vertraulichkeit der Kommunikation kann mittels geeigneter technischer Verfahren, wie z. B. WPA2, geschützt werden. Welche konkreten technischen Maßnahmen zur Verschlüsselung, Authentisierung und Konfiguration der Clients, in Abhängigkeit vom Einsatzgebiet, angewendet werden sollten, kann den Publikationen des BSI entnommen werden, z. B. „WLAN-Baustein der IT-Grundschutzkataloge“[3] sowie dem Dokument „Sichere Nutzung von WLAN (ISi-WLAN)“[4].

14.1.1.6 Protokollierung und Mitbestimmungspflicht des Personalrates

Soweit die Nutzung der Informationstechnik, des Internets und E-Mail zur Datenschutzkontrolle, zur Datensicherung oder zum ordnungsgemäßen Betrieb im System protokolliert wird, sind mindestens Art und Umfang der Protokollierung, Zweckbindung, Zugriffsrechte, Auswertung und Löschungsfristen der Protokolldaten festzulegen. Die Durchführung von Kontrollen muss eindeutig geregelt werden. Auf mögliche in Betracht kommende Sanktionen sind die Beschäftigten hinzuweisen.

Bevor ein elektronisches Verfahren eingeführt wird, sind mindestens folgende Festlegungen zur Protokollierung zu treffen:

- Ereignisse, Aktionen, Datenobjekte, welche protokolliert werden sollen,
- Stichproben- oder Vollprotokollierung,
- Speicherort (IT-System/Datenträger),
- Auswertung der Protokolle (wer, wann, wie, Auswertesoftware),
- Fristen zum Löschen,
- Schutz vor unbefugtem Zugriff, Manipulationen,

[3] BSI: IT Grundschutzkataloge, Stand 2008, http://www.bsi.bund.de/gshb/.
[4] BSI: Sichere Nutzung von WLAN (ISi-WLAN) 2009, http://www.bsi.de/fachthem/sinet/dokumente/isi_wlan_leitlinie.pdf.

- Maßnahmen bei Verstößen und
- Information der Mitarbeiter.

Protokolldaten sind personenbezogen, da sie Aufschluss über die Aktivitäten eines Benutzers geben. Sie unterliegen nach dem Datenschutzrecht einer strikten Zweckbindung (§ 13 Abs. 4 SächsDSG) und dürfen nur zum Nachweis der fehlerfreien und ordnungsgemäßen Datenverarbeitung oder zur Aufdeckung von missbräuchlichen Zugriffen oder Zugriffsversuchen, nicht jedoch für Zwecke der Verhaltens- oder Leistungskontrolle der Mitarbeiter verwendet oder ausgewertet werden. Grundsätzlich ist eine pauschale, flächendeckende und „vorbeugende“ Protokollierung aller Aktivitäten der Mitarbeiter am IT-System zur Verhaltens- und Leistungskontrolle nicht erforderlich und damit unzulässig.

Ermöglicht die Auswertung der Protokolldaten eine Verhaltens- und Leistungskontrolle, ist sie mitbestimmungspflichtig. Es empfiehlt sich deshalb, eine Vereinbarung mit dem Personalrat abzuschließen, in der die zulässigen Protokollierungen, ihre Aufbewahrungsdauer sowie die Art ihrer Auswertung und ihrer sonstigen Nutzung genau definiert sind. Da die Protokollierung eine technische Einrichtung zur Überwachung des Verhaltens der Beschäftigten der speichernden Stelle darstellt, hat der Personalrat gemäß § 84 i. V. m. § 80 Abs. 3 Nr. 16 SächsPersVG ein Mitbestimmungsrecht. Durch eine Vereinbarung mit dem Personalrat sollte daher sichergestellt sein, dass das Instrument der Protokollierung nicht zweckentfremdet verwendet wird.

Des Weiteren sind auch die Regelungen, wie z. B. Telearbeit oder E-Mail- und Internetnutzung, mit dem Personalrat abzustimmen und in einer Dienstvereinbarung zu verankern.

Zur Wahrung der o. g. Interessen des Dienstherrn kann eine regelmäßige stichprobenhafte und auch zeitnahe Auswertung der Protokolldaten als erforderlich und verhältnismäßig betrachtet werden.

Die *Aufbewahrungsdauer der Protokolle richtet* sich, da es sich um personenbezogene Daten handelt, nach den allgemeinen Löschungsregeln der Datenschutzgesetze. Maßgeblich ist die „Erforderlichkeit zur Aufgabenerfüllung“. Gibt es keinen zwingenden Grund für das weitere Vorhalten von Protokolldateien, besteht eine Löschungspflicht nach § 20 SächsDSG.

Eine exakte Bestimmung des Aufbewahrungszeitraums für Protokolle, deren Auswertung zeitlich nicht konkretisiert ist (z. B. die Protokolle im Zusammenhang mit der Administration), ist nicht möglich. In der Regel reicht hier eine Aufbewahrung bis zur

tatsächlichen Kontrolle. Erfahrungsgemäß sollte eine Frist von einem halben Jahr nicht überschritten werden.

14.1.1.7 Regelmäßige Überprüfung der Wirksamkeit der Sicherheitsmaßnahmen

Nach größeren Änderungen an den IT-Systemen oder nach spätestens drei Jahren halte ich eine Überprüfung und erneute Bestätigung der Dienstanweisung zur Informationstechnik sowie der Dienstvereinbarungen E-Mail und Internet für erforderlich.

14.1.2 Musterdienstanweisung für die Übermittlung vertraulicher Nachrichten mit Hilfe von Telefax-Geräten

Bei der Übersendung von dienstlichen Regelungen, die die Verarbeitung personenbezogener Zugangsdaten zur jeweiligen Telekommunikationsanlage beinhalten, ist öfters festzustellen, dass die Nutzung von Telefaxgeräten nur unzureichend geregelt wird. Die Einordnung der Fax-Server in das Zugriffs- und Sicherheitskonzept der jeweiligen Daten verarbeitenden Stelle, ist meist nicht geregelt.

Auch werden Beschränkungen bezüglich der Schutzwürdigkeit der zu versendenden personenbezogenen Daten nicht gesetzt. In diesem Zusammenhang verweise ich auf meine *Musterdienstanweisung für die Übermittlung vertraulicher Nachrichten mit Hilfe von Telefax-Geräten* auf meiner Web-Seite: www.datenschutz.sachsen.de unter öffentlicher Bereich-Arbeitshilfen.

Durch die Verwendung moderner digitaler Fax-Geräte sowie durch den Einsatz aktueller Finanzierungsformen (z. B. Leasing) werden diese Geräte nach einer bestimmbaren Zeit der Verfügungsgewalt des jeweiligen Betreibers durch Aussonderung bzw. Rückgabe entzogen. Auf den internen Speichermedien dieser digitalen Faxgeräte (Festplatte, Flash-Speicher) sind jedoch bei Rückgabe noch personenbezogene oder andere schützenswerte Informationen gespeichert. Da diese Daten meist nur durch eine spezielle, gerätebezogene Löschsoftware wirklich gelöscht werden können, ist bereits im Vorfeld der Nutzung moderner Kommunikationsmittel mit dem Lieferanten zu klären, wie nach Ende der Nutzung diese Informationen gelöscht werden können.

In dieser Hinsicht verweise ich erneut auf meine Web-Seite (an gleicher Stelle) auf meine *Orientierungshilfe Sicheres Löschen magnetischer Datenträger*.

14.2 Hilfsmittel - Baustein Datenschutz

Ein weiterer Meilenstein zur Verankerung des Datenschutzes im IT-Grundschutz in Deutschland ist die Erarbeitung des IT-Grundschutz-Bausteines „Datenschutz“ durch

den BfDI gemeinsam mit dem Arbeitskreis Technik der Datenschutzbeauftragten des Bundes und der Länder sowie den Datenschutzaufsichtsbehörden der Länder.

Der Baustein ist sowohl für die privaten als auch für die öffentlichen Anwender für den IT-Grundschutz ausgelegt.

Aufgrund der engen Verflechtung von Datenschutz und IT-Sicherheit werden in diesem IT-Grundschutz-Baustein zum Thema „Datenschutz“ einerseits die Rahmenbedingungen für den Datenschutz praxisgerecht aufbereitet und andererseits die Verbindung zur IT-Sicherheit im IT-Grundschutz aufgezeigt.

Beschreibung:
- rechtliche Rahmenbedingungen bei der Verarbeitung personenbezogener Daten
- Zulässigkeit der Erhebung, Verarbeitung und Nutzung personenbezogener Daten, landesspezifische Besonderheiten
- Datengeheimnis, Verpflichtung auf den Datenschutz, Unterrichtung
- technische und organisatorische Maßnahmen
- besondere Datenarten, Vorabkontrolle, automatisierte Einzelentscheidungen oder Abrufverfahren
- Rechte der Betroffenen
- Ansprechpartner und Kontrollen

Neben dem Formular zur IT-Grundschutzerhebung zu *Baustein B 1.5 Datenschutz* werden auch praktische Arbeitshilfen zum Abruf bereitgehalten, wie z. B. *Kreuzreferenz-Tabellen*, die alle Gefährdungen eines Bausteins und dazugehörige Maßnahmen enthält. Zusätzlich wurde durch den Arbeitskreis eine Tabelle erarbeitet, in der die Maßnahmen der IT-Grundschutz-Kataloge unter Berücksichtigung der Zielsetzungen des Datenschutzes auf ihre Relevanz hin bewertet worden sind.

Der Baustein *B 1.5 Datenschutz* und die zugehörigen Tabellen und Materialien sind in den IT-Grundschutz-Katalogen abzurufen unter www.bsi.bund.de/gshb/baustein-datenschutz.

14.3 Datenschutzgerechte Gestaltung der Protokollierung von IP-Adressen in Webserver-Logfiles

Webserver können je nach Konfiguration sehr komplexe Protokoll-Dateien erzeugen, die unter anderem Angaben darüber enthalten, welche Webseiten abgerufen wurden, welcher Browser und welches Betriebssystem dazu verwendet wurden und - mit welcher Internet-Protokoll (IP)-Adresse ein Nutzer die Seite aufgerufen hat.

§ 15 TMG verbietet jedoch die personenbeziehbare Protokollierung des Nutzungsverhaltens, sofern diese nicht zur Abrechnung erforderlich ist (siehe dazu auch 13/14.2).

Um den Personenbezug zu entfernen, muss der Webserver die IP-Adresse bereits modifiziert im Protokoll ablegen. Dies ist in den gängigen Webserver-Distributionen mit „Bordmitteln“ so nicht möglich, was in der Praxis dazu führte, dass Gesetzesvorgaben entweder nicht beachtet wurden oder auf die Speicherung der IP-Adressen komplett verzichtet wurde. Im letzteren Fall verloren die Protokolldateien für die inhaltsverantwortlichen Stellen aber auch an relevanter Aussagekraft über die Herkunft der Seitenbesucher zu statistischen Zwecken und zur Optimierung von Webangeboten.

Um auf der Grundlage der bestehenden gesetzlichen Regelungen diesen Interessen datenschutzkonform Rechnung zu tragen, habe ich nach einer Machbarkeitsanalyse die Programmierung entsprechender Zusatzmodule für die beiden meistverbreiteten Webserver (Apache und Microsoft IIS) beauftragt.

Bei der Realisierung wird der Ansatz verfolgt, voreingestellt mindestens die letzte Stelle einer vierstelligen IP-Adresse durch eine 0 zu ersetzen. Darüber hinaus ist eine bitweise Maskierung der übrigen 24 Adress-Bits möglich und separat einstellbar, empfohlen wird eine Maskierung von 16 Bit.

Durch diese Verfahrensweise bleibt die IP-Adresse - anonymisiert - im Protokoll erhalten und kann von gängigen Statistik-Programmen zur Auswertung des Webangebotes ohne Personenbezug herangezogen werden.

Die Software kann kostenfrei für die jeweilige Webserverplattform unter http://www.-saechsdsb.de/ipmask heruntergeladen werden.

14.4 Verwaltungsmodernisierung - E-Government

In 13/1.6 berichtete ich über meine Forderung, die E-Government-Aktivitäten der Sächsischen Staatsregierung auf eine gesetzliche Grundlage zu stellen. Mittlerweile hat im Februar 2009 eine Expertenanhörung zu einem entsprechenden von der SK entworfenen Eckwertepapier stattgefunden. In dieser wurde von den geladenen Experten meine Auffassung vollumfänglich bestätigt.

Insbesondere wurde es schon aus staatsorganisationsrechtlichen Gründen als notwendig angesehen, dass sowohl das Betreiben einer E-Government-Plattform als auch das Einrichten eines zentralen IT-Dienstleisters eine gesetzliche Grundlage erhalten.

Auch wird es, anders als von der SK beabsichtigt, nicht möglich sein, eine landesrechtliche Regelung zur Speicherung von IP-Adressen für statistische Zwecke einzuführen. Die Erlaubnis zur Verarbeitung von Nutzungsdaten (wie IP-Adressen) ist nach Ansicht des Gesetzgebers in § 15 TMG abschließend geregelt. Die geladenen Experten wiesen zudem auf die ausschließliche Bundeskompetenz gemäß Art. 73 Abs. 1 Nr. 7 GG hin. Ich habe daher erneut nachdrücklich angeregt, von der in 13/14.1 dargestellten Möglichkeit, statistische Auswertungen mit anonymisierten IP-Adressen vorzunehmen, Gebrauch zu machen.

Die Regelung in § 4 Abs. 5 SächsDSG, wonach eine elektronische Einwilligung nur mit einer qualifizierten elektronischen Signatur erteilt werden kann, dürfte wegen deren mangelnder Verbreitung nach Ansicht der geladenen Experten eine unüberwindbare Hürde für die geplante Speicherung von Profildaten der Nutzer der E-Government-Plattform darstellen.

Es besteht also nach wie vor gesetzgeberischer Handlungsbedarf. Ich bin weiterhin gern bereit, an einem entsprechenden Entwurf beratend mitzuwirken.

15 Vortrags- und Schulungstätigkeit für behördliche Datenschutzbeauftragte

Wie in meinem 13. Tätigkeitsbericht angekündigt, habe ich die Schulungen für die nach § 11 SächsDSG bestellten Datenschutzbeauftragten öffentlicher Stellen fortgesetzt, wenn auch nicht in dem ursprünglich beabsichtigten Umfang. Ich werde mich bemühen, Schulungen künftig häufiger anzubieten. Hilfreich wären in diesem Zusammenhang Anregungen aus dem Kreis der behördlichen Datenschutzbeauftragten hinsichtlich zu behandelnder Themen.

Mittlerweile ist auch das interne Forum unter http://circa.sachsen.de eingerichtet. Hier finden die angemeldeten Nutzer u. a. die Schulungsunterlagen sowie ein Verzeichnis der Erreichbarkeit der Mitarbeiter meiner Behörde. Leider wurde die Möglichkeit, auf diese Weise in einer geschlossenen Benutzergruppe spezielle Fragen und Probleme zum Datenschutz zu diskutieren und Erfahrungen auszutauschen, bisher kaum genutzt. Sowohl für die Anmeldung als auch für Fragen, die sich im Zusammenhang mit der Nutzung des Circa-Servers stellen, können sich die behördlichen Datenschutzbeauftragten unter der Telefonnummer (03578) 33-1717 oder der E-Mail-Adresse circa.nlkm@sid.sachsen.de an den Betreiber des Circa-Servers wenden.

16 Materialien

16.1 Entschließungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder

16.1.1 Entschließung der 75. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 3./4. April 2008 in Berlin: Berliner Erklärung: Herausforderungen für den Datenschutz zu Beginn des 21. Jahrhunderts

Regelungen insbesondere zum großen Lauschangriff, zur Telekommunikationsüberwachung, zur Rasterfahndung, zur Online-Durchsuchung, zur automatischen Auswertung von Kfz-Kennzeichen und zur Vorratsspeicherung von Telekommunikationsdaten haben die verfassungsrechtlich zwingende Balance zwischen Sicherheitsbefugnissen der staatlichen Behörden und persönlicher Freiheit der Bürgerinnen und Bürger missachtet. Das Bundesverfassungsgericht hat mit einer Reihe von grundlegenden Entscheidungen diese Balance wieder hergestellt und damit auch den Forderungen der Datenschutzbeauftragten des Bundes und der Länder größtenteils Rechnung getragen.

Die Herausforderungen für den Datenschutz gehen aber weit über die genannten Bereiche hinaus. Datenverarbeitungssysteme dringen immer stärker in alle Lebensbereiche ein und beeinflussen den Alltag. Das Internet ist zum Massenmedium geworden. Vielfältig sind dabei die Möglichkeiten, das persönliche Verhalten zu registrieren und zu bewerten. Der nächste Quantensprung der Informationstechnik steht unmittelbar bevor: Die Verknüpfung von Informationstechnik mit Körperfunktionen, insbesondere bei der automatisierten Messung medizinischer Parameter und bei der Kompensation organischer Beeinträchtigungen. Die Miniaturisierung von IT-Systemen geht so weit, dass demnächst einzelne Komponenten nicht mehr mit bloßem Auge wahrgenommen werden können (Nanotechnologie).

Das Handeln staatlicher und nicht-öffentlicher Stellen ist verstärkt darauf gerichtet, viele Daten ohne klare Zweckbestimmung zu sammeln, um sie anschließend vielfältig auszuwerten, beispielsweise um versteckte Risiken aufzudecken oder um persönliches Verhalten unbemerkt zu beeinflussen. Geht es der Wirtschaft etwa darum, durch Scoringverfahren die Kundinnen und Kunden vorab einzuschätzen, gewinnt die immer exzessivere Registrierung und automatisierte Beobachtung für staatliche Stellen an Bedeutung. In beiden Bereichen wird ganz normales Verhalten registriert, unabhängig von konkreten Gefahren oder Verdachtsmomenten. Auch diejenigen, die sich nichts haben zu Schulden kommen lassen, werden einem verstärkten Kontroll- und Anpassungsdruck ausgesetzt, der Einschüchterungseffekte zur Folge haben wird.

Der Schutz der Grundrechte, nicht zuletzt des Datenschutzes, dient in einer demokratischen Gesellschaft auch dem Gemeinwohl und ist zunächst Aufgabe jeglicher Staatsgewalt. Darüber hinaus ist er eine gesamtgesellschaftliche Aufgabe. Schließlich ist jede Bürgerin und jeder Bürger auch zur Eigenverantwortung aufgerufen. Hilfen zum informationellen Selbstschutz müssen zur Verfügung gestellt werden, die es den Betroffenen ermöglichen, eine Erfassung ihres Verhaltens zu vermeiden und selbst darüber zu entscheiden, ob und wem gegenüber sie Daten offenbaren. Von zunehmender Bedeutung sind auch Projekte, die das Datenschutzbewusstsein fördern, um vor allem jüngere Menschen von einem fahrlässigen Umgang mit ihren persönlichen Daten abzuhalten.

Alle diese Maßnahmen tragen zur Entwicklung einer neuen Datenschutzkultur bei. Voraussetzung dafür ist auch, dass nicht länger versucht wird, die verfassungsrechtlichen Grenzen und Spielräume auszureizen. Stattdessen muss dem Gebot der Datenvermeidung und -sparsamkeit Rechnung getragen werden.

16.1.2 Entschließung der 75. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 3./4. April 2008 in Berlin: Unzureichender Datenschutz beim deutsch-amerikanischen Abkommen über die Zusammenarbeit der Sicherheitsbehörden

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder beobachtet mit Sorge, dass die Datenschutzrechte der Bürgerinnen und Bürger im Rahmen der internationalen Zusammenarbeit der Sicherheitsbehörden immer häufiger auf der Strecke bleiben. Aktuelles Beispiel ist das am 11. März 2008 paraphierte deutsch-amerikanische Regierungsabkommen über die Vertiefung der Zusammenarbeit bei der Verhinderung und Bekämpfung schwerwiegender Kriminalität. Die Konferenz fordert Bundestag und Bundesrat auf, dem Abkommen solange nicht zuzustimmen, bis ein angemessener Datenschutz gewährleistet ist.

Mit dem Abkommen wurde ein gegenseitiger Online-Zugriff auf Fundstellendatensätze von daktyloskopischen Daten und DNA-Profilen im hit/no-hit-Verfahren nach dem Muster des Prümer Vertrages vereinbart. Zudem wurden dessen Regelungen über den Austausch personenbezogener Daten zur Verhinderung terroristischer Straftaten weitgehend übernommen. Eine Übertragung des als Bedingung für diese umfangreichen Zugriffs- und Übermittlungsbefugnisse im Prümer Vertrag geschaffenen Datenschutzregimes erfolgte jedoch nicht.

Die Voraussetzungen, unter denen ein Datenaustausch erlaubt ist, sind nicht klar definiert. Der Datenaustausch soll allgemein zur Bekämpfung von Terrorismus und schwerer Kriminalität möglich sein. Welche Straftaten darunter konkret zu verstehen sind,

wird nicht definiert. Es erfolgt hier lediglich der Verweis auf das jeweilige nationale Recht. Damit trifft nach dem Abkommen die USA einseitig eine Entscheidung über die Relevanz der abgerufenen Daten.

Bevor in so großem Umfang zusätzliche Datenübermittlungen erlaubt werden, muss zunächst geklärt werden, warum die bisherigen Datenübermittlungsbefugnisse für die internationale Polizeizusammenarbeit mit den USA nicht ausreichen.

Für die weitere Verarbeitung aus Deutschland stammender Daten in den USA bestehen für die Betroffenen praktisch keine Datenschutzrechte. Das Abkommen selbst räumt den Betroffenen keine eigenen Rechte ein, sondern verweist auch hierzu auf die Voraussetzungen im Recht der jeweiligen Vertragspartei. In den USA werden aber Datenschutzrechte, wie sie in der Europäischen Union allen Menschen zustehen, ausschließlich Bürgerinnen und Bürgern der Vereinigten Staaten von Amerika und dort wohnenden Ausländerinnen und Ausländern gewährt. Anderen Personen stehen Rechtsansprüche auf Auskunft über die Verarbeitung der eigenen Daten, Löschung unzulässig erhobener oder nicht mehr erforderlicher Daten oder Berichtigung unrichtiger Daten nicht zu. Außerdem besteht in den USA keine unabhängige Datenschutzkontrolle. Vor diesem Hintergrund sind die im Abkommen enthaltenen weiten Öffnungsklauseln für die weitere Verwendung der ausgetauschten Daten sowie der Verzicht auf Höchstspeicherfristen aus datenschutzrechtlicher Sicht nicht akzeptabel.

16.1.3 Entschließung der 75. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 3./4. April 2008 in Berlin: Mehr Augenmaß bei der Novellierung des BKA-Gesetzes

Der vom Bundesministerium des Innern erarbeitete Referentenentwurf eines Gesetzes zur Abwehr des internationalen Terrorismus durch das Bundeskriminalamt hat zum Ziel, das Bundeskriminalamt mit umfassenden polizeilichen Befugnissen zur Verhütung von terroristischen Straftaten und zur Abwehr von Gefahren für die öffentliche Sicherheit in diesem Zusammenhang auszustatten. Insbesondere sind Befugnisse zur Durchsuchung, Rasterfahndung, Wohnraumüberwachung und Telekommunikationsüberwachung vorgesehen. Außerdem will das Bundesinnenministerium eine Befugnis zum heimlichen Zugriff auf informationstechnische Systeme („Online-Durchsuchung“) in das BKA-Gesetz aufnehmen.

Die Datenschutzbeauftragten des Bundes und der Länder sprechen sich dagegen aus, dass dem Bundeskriminalamt nach dem Gesetzentwurf mehr Befugnisse eingeräumt werden sollen, als einzelnen Landespolizeien zur Erfüllung ihrer eigenen Gefahrenabwehraufgaben zustehen. Sie halten es daher für geboten, im weiteren Gesetzgebungs-

verfahren die Befugnisse des Bundeskriminalamtes auf die zur Aufgabenerfüllung zwingend notwendigen Kompetenzen zu beschränken.

Die bisherige informationelle Gewaltenteilung zwischen den Polizeien der Länder und dem Bundeskriminalamt diente auch dem Datenschutz. Die Konferenz fordert deshalb eine klare, d. h. hinreichend trennscharfe Abgrenzung der spezifischen Befugnisse des Bundeskriminalamts einerseits zu denen der Landespolizeien und Verfassungsschutzbehörden andererseits.

Dem Referentenentwurf zufolge soll die Aufgabenwahrnehmung durch das Bundeskriminalamt die Zuständigkeit der Landespolizeibehörden auf dem Gebiet der Gefahrenabwehr unberührt lassen. Dies führt zu erheblichen datenschutzrechtlichen Problemen, da nach geltendem Recht auch die Länder bei Abwehr einer durch den internationalen Terrorismus begründeten Gefahr parallele Abwehrmaßnahmen ergreifen können. Angesichts der Weite der für das Bundeskriminalamt vorgesehenen und den Landespolizeibehörden bereits eingeräumten Datenerhebungs- und Datenverarbeitungsbefugnisse steht zu befürchten, dass es zu sich überlappenden und in der Summe schwerwiegenderen Eingriffen in das informationelle Selbstbestimmungsrecht Betroffener durch das Bundeskriminalamt und die Landespolizeibehörden kommen wird.

Ebenso stellt sich die grundsätzliche Frage der Abgrenzung von Polizei und Verfassungsschutz. In den vergangenen Jahren sind die Polizeigesetze des Bundes und der Länder zunehmend mit Befugnissen zur verdeckten Datenerhebung (z. B. heimliche Video- und Sprachaufzeichnungen, präventive Telekommunikationsüberwachung) ausgestattet worden. Zudem wurden die Eingriffsbefugnisse immer weiter ins Vorfeld von Straftaten und Gefahren erstreckt. Damit überschneiden sich die polizeilichen Ermittlungsbefugnisse zunehmend mit denen des Verfassungsschutzes.

Das Bundesverfassungsgericht hat in seinem Urteil zur „Online-Durchsuchung“ vom 27. Februar 2008 den Gesetzgeber erneut verpflichtet, den unantastbaren Kernbereich privater Lebensgestaltung zu gewährleisten. Diese Vorgabe des Gerichts gilt nicht nur für eine etwaige gesetzliche Regelung zur „Online-Durchsuchung“, sondern für alle Eingriffsmaßnahmen. Die Datenschutzbeauftragten des Bundes und der Länder fordern den Gesetzgeber deshalb auf, im Rahmen der Novellierung des BKA-Gesetzes den Schutz des Kernbereichs privater Lebensgestaltung für alle Eingriffsmaßnahmen zu regeln.

16.1.4 Entschließung der 75. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 3./4. April 2008 in Berlin: Keine Vorratsspeicherung von Flugpassagierdaten

Die EU-Kommission hat den Entwurf eines Rahmenbeschlusses des Rates zur Speicherung von Flugpassagierdaten und zu deren Weitergabe an Drittstaaten vorgelegt. Künftig sollen die Fluggesellschaften bei Flügen aus der EU und in die EU zu jedem Fluggast insgesamt 19 Datenelemente, bei unbegleiteten Minderjährigen sechs weitere Datenelemente, an eine von dem jeweiligen Mitgliedstaat bestimmte „Zentralstelle“ übermitteln. Die Daten sollen bei den Zentralstellen anlass- und verdachtsunabhängig insgesamt 13 Jahre lang personenbezogen gespeichert werden und zur Durchführung von Risikoanalysen dienen. Unter im Einzelnen noch unklaren Voraussetzungen sollen die Daten an Strafverfolgungsbehörden von Nicht-EU-Staaten (z. B. die USA), übermittelt werden dürfen. Neben Grunddaten zur Person, über Reiseverlauf, Buchungs- oder Zahlungsmodalitäten und Sitzplatzinformationen sollen auch andere persönliche Angaben gespeichert werden. Unklar ist, welche Daten unter „allgemeine Hinweise“ gespeichert werden dürfen. Denkbar wäre, dass beispielsweise besondere Essenswünsche erfasst werden.

Mit der beabsichtigten Vorratsspeicherung und der Datenübermittlung wird die EU es auswärtigen Staaten ermöglichen, Bewegungsbilder auch von EU-Bürgerinnen und -Bürgern zu erstellen. In Zukunft besteht die Gefahr, dass Menschen Angst haben werden, durch ihre Reisegewohnheiten aufzufallen.

Die in dem Rahmenbeschluss vorgesehene Vorratsdatenspeicherung von Daten sämtlicher Fluggäste, die EU-Grenzen überschreiten, verstößt nicht nur gegen Art. 8 der Europäischen Menschenrechtskonvention und die Europaratskonvention 108, sondern ist auch mit dem im Grundgesetz verankerten Recht auf informationelle Selbstbestimmung nicht vereinbar. Grundrechtseingriffe „ins Blaue hinein“, also Maßnahmen ohne Nähe zu einer abzuwehrenden Gefahr sind unzulässig.

Der Vorschlag für den Rahmenbeschluss erfolgte, ohne den Nutzen der erst jüngst in nationales Recht umgesetzten Richtlinie 2004/82/EG[5], die bereits alle Beförderungsunternehmen verpflichtet, die Daten von Reisenden an die Grenzkontrollbehörden zu übermitteln, auszuwerten. Hinzu kommt, dass der Vorschlag kaum datenschutzrechtliche Sicherungen enthält. Er bezieht sich nur auf eine bisher nicht bestehende und im Entwurf mit Mängeln behaftete EU-Datenschutzregelung. Diese Mängel wirken sich dadurch besonders schwerwiegend aus, dass in den Drittstaaten ein angemessenes

[5] RL 2004/82 EG vom 29. April 2004 (Amtsbl. L 261 (2004), S. 24 ff.), Richtlinie über die Verpflichtung von Beförderungsunternehmen, Angaben über die Beförderten zu übermitteln.

Datenschutzniveau nicht immer gewährleistet ist und eine Änderung dieser Situation auch in Zukunft nicht zu erwarten ist.

Die EU-Kommission hat nicht dargelegt, dass vergleichbare Maßnahmen in den USA, in Kanada oder in Großbritannien einen realen, ernst zu nehmenden Beitrag zur Erhöhung der Sicherheit geleistet hätten. Sie hat die kritischen Stellungnahmen der nationalen und des Europäischen Datenschutzbeauftragten sowie der Art. 29-Datenschutzgruppe nicht berücksichtigt.

Die Konferenz fordert die Bundesregierung auf, den Entwurf abzulehnen. Sie teilt die vom Bundesrat geäußerten Bedenken an der verfassungsrechtlichen Zulässigkeit der Speicherung der Passagierdaten.

16.1.5 Entschließung der 75. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 3./4. April 2008 in Berlin: Keine Daten der Sicherheitsbehörden an Arbeitgeber zur Überprüfung von Arbeitnehmerinnen und Arbeitnehmern

Die Datenschutzbeauftragten des Bundes und der Länder wenden sich entschieden gegen die Übermittlung polizeilicher und nachrichtendienstlicher Erkenntnisse an Arbeitgeber zur Überprüfung von Bewerberinnen und Bewerbern, Beschäftigten und Fremdpersonal (z. B. Reinigungskräfte) außerhalb gesetzlicher Grundlagen. In zunehmendem Maß bitten Arbeitgeber die Betroffenen, in eine Anfrage des Arbeitgebers bei der Polizei oder dem Verfassungsschutz zu etwaigen dort vorliegenden Erkenntnissen zu ihrer Person einzuwilligen. In anderen Fällen sollen die Betroffenen eine solche Auskunft („fremdbestimmte Selbstauskunft“) selbst einholen und ihrem Arbeitgeber vorlegen. Eine solche „Einwilligung des Betroffenen“ ist regelmäßig keine wirksame Einwilligung. Die Betroffenen sehen sich oftmals dem faktischen Druck des Wohlverhaltens zum Zwecke des Erhalts und der Sicherung des Arbeitsplatzes ausgesetzt.

Die gesetzliche Grundentscheidung, in einem „Führungszeugnis“ dem Arbeitgeber nur ganz bestimmte justizielle Informationen zu einer Person verfügbar zu machen, wird dadurch unterlaufen. Es stellt einen Dammbruch dar, wenn jeder Arbeitgeber durch weitere Informationen direkt oder indirekt an dem Wissen der Sicherheitsbehörden und Nachrichtendienste teilhaben kann. Die Übermittlung dieser Informationen an Arbeitgeber kann auch den vom Bundesarbeitsgericht zum „Fragerecht des Arbeitgebers“ getroffenen Wertentscheidungen widersprechen. Danach darf der Arbeitgeber die Arbeitnehmerinnen und Arbeitnehmer bei der Einstellung nach Vorstrafen und laufenden Ermittlungsverfahren fragen, wenn und soweit die Art des zu besetzenden Arbeitsplatzes dies erfordert.

Polizei und Nachrichtendienste speichern - neben den in ein „Führungszeugnis“ aufzunehmenden Daten - auch personenbezogene Daten, die in das Bundeszentralregister gar nicht erst eingetragen werden oder Arbeitgebern in einem „Führungszeugnis“ nicht übermittelt werden dürfen. Es stellt eine grundsätzlich unzulässige Durchbrechung des Zweckbindungsgrundsatzes dar, wenn ein Arbeitgeber diese Daten - über den Umweg über die Polizei oder einen Nachrichtendienst - für Zwecke der Personalverwaltung erhält. Dabei ist besonders zu beachten, dass polizeiliche oder nachrichtendienstliche Daten nicht zwingend gesicherte Erkenntnisse sein müssen, sondern oftmals lediglich Verdachtsmomente sind. Die Folgen von Missdeutungen liegen auf der Hand.

16.1.6 Entschließung der 75. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 3./4. April 2008 in Berlin: Vorgaben des Bundesverfassungsgerichts bei der Online-Durchsuchung beachten

1. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt, dass das Bundesverfassungsgericht die Regelung zur Online-Durchsuchung im Verfassungsschutzgesetz Nordrhein-Westfalen für nichtig erklärt hat. Hervorzuheben ist die Feststellung des Gerichts, dass das allgemeine Persönlichkeitsrecht auch das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme umfasst. 25 Jahre nach dem Volkszählungsurteil hat das Bundesverfassungsgericht damit den Datenschutz verfassungsrechtlich weiter gestärkt und ihn an die Herausforderungen des elektronischen Zeitalters angepasst.

2. Ein solches Grundrecht nimmt auch den Staat in die Verantwortung, sich aktiv für die Vertraulichkeit und Integrität informationstechnischer Systeme einzusetzen. Das Bundesverfassungsgericht verpflichtet den Staat, im Zeitalter der elektronischen Kommunikation Vertraulichkeit zu gewährleisten. Nunmehr ist der Gesetzgeber gehalten, diesen Auftrag konsequent umzusetzen. Dazu müssen die Regelungen, welche die Bürgerinnen und Bürger vor einer „elektronischen Ausforschung“ schützen sollen, gemäß den Vorgaben des Gerichts insbesondere im Hinblick auf technische Entwicklungen verbessert werden. Hiermit würde auch ein wesentlicher Beitrag geleistet, Vertrauen in die Sicherheit von E-Government- und E-Commerce-Verfahren herzustellen.

3. Die Konferenz unterstützt die Aussagen des Gerichts zum technischen Selbstschutz der Betroffenen. Ihre Möglichkeiten, sich gegen einen unzulässigen Datenzugriff zu schützen, etwa durch den Einsatz von Verschlüsselungsprogrammen, dürfen nicht unterlaufen oder eingeschränkt werden.

4. Die Konferenz begrüßt außerdem, dass das Bundesverfassungsgericht das neue Datenschutzgrundrecht mit besonders hohen verfassungsrechtlichen Hürden vor staatlichen Eingriffen schützt. Sie fordert die Gesetzgeber in Bund und Ländern auf, diese Eingriffsvoraussetzungen zu respektieren. Die Konferenz spricht sich in diesem Zusammenhang gegen Online-Durchsuchungen durch die Nachrichtendienste aus.

5. Das Bundesverfassungsgericht hat den Gesetzgeber erneut verpflichtet, den unantastbaren Kernbereich privater Lebensgestaltung auch bei Eingriffen in informationstechnische Systeme zu gewährleisten. Unvermeidbar erhobene kernbereichsrelevante Inhalte sind unverzüglich zu löschen. Eine Weitergabe oder Verwertung dieser Inhalte ist auszuschließen.

6. Auch wenn Online-Durchsuchungen innerhalb der durch das Bundesverfassungsgericht festgelegten Grenzen verfassungsgemäß sind, fordert die Konferenz die Gesetzgeber auf, die Erforderlichkeit von Online-Durchsuchungsbefugnissen kritisch zu hinterfragen. Sie müssen sich die Frage stellen, ob sie den Sicherheitsbehörden entsprechende Möglichkeiten an die Hand geben wollen. Die Konferenz bezweifelt, dass dieser weiteren Einbuße an Freiheit ein adäquater Gewinn an Sicherheit gegenüber steht.

7. Sollten gleichwohl Online-Durchsuchungen gesetzlich zugelassen werden, sind nicht nur die vom Bundesverfassungsgericht aufgestellten verfassungsrechtlichen Hürden zu beachten. Die Konferenz hält für diesen Fall zusätzliche gesetzliche Regelungen für erforderlich. Zu ihnen gehören vor allem folgende Punkte:

   - Soweit mit der Vorbereitung und Durchführung von Online-Durchsuchungen der Schutzbereich von Art. 13 GG (Unverletzlichkeit der Wohnung) betroffen ist, bedarf es dafür jedenfalls einer besonderen Rechtsgrundlage.

   - Der vom Bundesverfassungsgericht geforderte Richtervorbehalt ist bei Online-Durchsuchungen mindestens so auszugestalten wie bei der akustischen Wohnraumüberwachung. Ergänzend zu einer richterlichen Vorabkontrolle ist eine begleitende Kontrolle durch eine unabhängige Einrichtung vorzuschreiben.

   - Gesetzliche Regelungen, welche Online-Durchsuchungen zulassen, sollten befristet werden und eine wissenschaftliche Evaluation der dabei gewonnenen Erkenntnisse und Erfahrungen anordnen.

   - Informationstechnische Systeme, die von zeugnisverweigerungsberechtigten Berufsgruppen genutzt werden, sind von heimlichen Online-Durchsuchungen auszunehmen.

- Für die Durchführung von „Quellen-Telekommunikationsüberwachungen“, die mit der Infiltration von IT-Systemen einhergehen, sind die gleichen Schutzvorkehrungen zu treffen wie für die Online-Durchsuchung selbst.

8. Schließlich sind die Gesetzgeber in Bund und Ländern aufgrund der Ausstrahlungswirkung der Entscheidung des Bundesverfassungsgerichts gehalten, die sicherheitsbehördlichen Eingriffsbefugnisse in Bezug auf informationstechnische Systeme, z. B. bei der Überwachung der Telekommunikation im Internet sowie der Beschlagnahme und Durchsuchung von Speichermedien, grundrechtskonform einzuschränken.

16.1.7 Entschließung der 75. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 3./4. April 2008 in Berlin: Medienkompetenz und Datenschutzbewusstsein in der jungen „online-Generation“

1. Die Nutzung moderner Informationssysteme ist auch mit Risiken verbunden. Diese begründen ein besonderes Schutzbedürfnis der Bürgerinnen und Bürger. Dieses verlangt aber nicht nur rechtliche Vorkehrungen und Sicherungen, sondern auch Aufklärung und Information darüber, mit welchen Risiken die Nutzung dieser Informationssysteme verbunden sind. Dies gilt vor allem für die junge „online-Generation“, die in der Altersgruppe der 14- bis 19-Jährigen zu 96 % regelmäßig das Internet nutzt und zwar im Durchschnitt länger als zweieinhalb Stunden täglich.

2. Die Datenschutzbeauftragten des Bundes und der Länder sehen es daher als wichtige Aufgabe an, Kinder und Jugendliche für einen sorgsamen und verantwortungsbewussten Umgang mit den eigenen Daten und den Daten anderer zu sensibilisieren. Diese Aufgabe obliegt gesellschaftlichen Einrichtungen ebenso wie staatlichen Organen.

   Die Erfahrungen, die anlässlich des 2. Europäischen Datenschutztages am 28. Januar 2008 gemacht wurden, stützen dies. Zu dem Motto "Datenschutz macht Schule" wurde von den Datenschutzbeauftragten des Bundes und der Länder eine Vielzahl von Veranstaltungen und Schulbesuchen organisiert. Eltern, Lehrkräfte, Schülerinnen und Schüler, aber auch Studierende hatten dabei die Möglichkeit, sich z. B. bei Podiumsdiskussionen, Rollenspielen und Workshops über datenschutzrelevante Fragen bei der Nutzung moderner Medien zu informieren. Die dabei gewonnenen Erfahrungen lassen nicht nur einen enormen Informationsbedarf, sondern auch ein großes Informationsinteresse erkennen, und zwar bei allen Beteiligten, bei den Jugendlichen ebenso wie bei ihren Eltern und den Lehrkräften.

   Bei den Informationsangeboten, die derzeit den Schulen angeboten werden, um die Medienkompetenz junger Menschen zu verbessern, spielt das Thema „Datenschutz“

aber nur eine untergeordnete Rolle. Es beschränkt sich überwiegend auf Fragen der Datensicherheit und wird zudem häufig von Fragen des Jugendmedienschutzes und des Verbraucherschutzes überlagert.

3. Die Datenschutzbeauftragten des Bundes und der Länder halten es daher für notwendig, dass die für die schulische Bildung zuständigen Ministerinnen und Minister der Landesregierungen bei der Förderung der Medienkompetenz von Kindern und Jugendlichen - schon im Grundschulalter - deren Datenschutzbewusstsein stärken. Der Datenschutz muss bei den Angeboten und Projekten zur Förderung der Medienkompetenz eine größere Rolle spielen. Die bisherigen Ansätze reichen bei weitem nicht aus. Gerade bei jungen Menschen muss das Bewusstsein über den Datenschutz als Bürgerrecht und Bestandteil unserer demokratischen Ordnung stärker gefördert werden.

16.1.8 Entschließung der 75. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 3./4. April 2008 in Berlin: Datenschutzförderndes Identitätsmanagement statt Personenkennzeichen

Elektronische Identitäten sind der Schlüssel zur Teilnahme an der digitalen Welt. Die Möglichkeiten der pseudonymen Nutzung, die Gewährleistung von Datensparsamkeit und -sicherheit und der Schutz vor Identitätsdiebstahl und Profilbildung sind wichtige Grundpfeiler moderner Informations- und Kommunikationstechnologien. Darauf hat die Bundesregierung zu Recht anlässlich des Zweiten Nationalen IT-Gipfels im Dezember 2007 (Hannoversche Erklärung) hingewiesen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist darauf hin, dass der gesetzliche Rahmen für die anonyme oder pseudonyme Nutzung elektronischer Verfahren bereits seit langem vorhanden ist. Beispielsweise hat jeder Diensteanbieter die Nutzung von Telemedien und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist (§ 13 Abs. 6 Telemediengesetz).

Bisher werden jedoch anonyme oder pseudonyme Nutzungsmöglichkeiten nur sehr selten angeboten. Vielmehr speichern Wirtschaft und Verwaltung immer mehr digitale Daten mit direktem Personenbezug. Erschlossen werden diese Datenbestände in der Regel über einheitliche Identifizierungsnummern. Mit der lebenslang geltenden, bundeseinheitlichen Steuer-Identifikationsnummer (Steuer-ID) oder der mit der Planung der Gesundheitskarte zusammenhängenden, ebenfalls lebenslang geltenden Krankenversichertennummer werden derzeit solche Merkmale eingeführt. Auch mit der flächendeckenden Einführung des ePersonalausweises wird jeder Bürgerin und jedem Bürger

eine elektronische Identität zugewiesen, mit der sie bzw. er sich künftig auch gegenüber eGovernment-Portalen der Verwaltung oder eCommerce-Angeboten der Wirtschaft identifizieren soll.

Einheitliche Personenkennzeichen bergen erhebliche Risiken für das Recht auf informationelle Selbstbestimmung. So könnte sich aus der Steuer-ID ein Personenkennzeichen entwickeln, über das alle möglichen Datenbestände personenbezogen verknüpft und umfassende Persönlichkeitsprofile erstellt werden. Angesichts der stetig verbesserten technischen Möglichkeiten, zunächst verteilt gespeicherte Daten anwendungsübergreifend zu verknüpfen, wachsen entsprechende Begehrlichkeiten.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist darauf hin, dass die effektive Nutzung von Informationstechnik und hohe Datenschutzstandards keinen Widerspruch bilden. Ein datenschutzförderndes Identitätsmanagement kann den Einzelnen vor unangemessener Überwachung und Verknüpfung seiner Daten schützen und zugleich eine moderne und effektive Datenverarbeitung ermöglichen. Entsprechende EU-Projekte wie PRIME (Privacy and Identity Management for Europe) und FIDIS (Future of Identity in the Information Society) werden im Rahmen des 6. Europäischen Forschungsprogramms „Technologien für die Informationsgesellschaft“ gefördert.

Identitätsmanagement sollte auf der anonymen oder pseudonymen Nutzung von elektronischen Verfahren und der dezentralen Haltung von Identifikationsdaten unter möglichst weitgehender Kontrolle der betroffenen Bürgerinnen und Bürger basieren. Datenschutzfördernde Identitätsmanagementsysteme schließen Verknüpfungen nicht aus, wenn die Nutzenden es wünschen oder wenn dies gesetzlich vorgesehen ist. Sie verhindern jedoch, dass unkontrolliert der Bezug zwischen einer elektronischen Identität und einer Person hergestellt werden kann. Unter bestimmten, klar definierten Bedingungen kann mit Hilfe von Identitätsmanagementsystemen sichergestellt werden, dass ein Pseudonym bei Bedarf bezogen auf einen bestimmten Zweck (z. B. Besteuerung) einer Person zugeordnet werden kann.

Identitätsmanagementsysteme werden nur dann die Akzeptanz der Nutzerinnen und Nutzer finden, wenn sie einfach bedienbar sind, ihre Funktionsweise für alle Beteiligten transparent ist, möglichst alle Komponenten standardisiert sind und die Technik von unabhängigen Dritten jederzeit vollständig nachprüfbar ist.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Bundesregierung daher auf, den Absichtserklärungen des IT-Gipfels Taten folgen zu lassen und den Einsatz datenschutzfördernder Identitätsmanagementsysteme voranzu-

treiben. Sowohl die öffentliche Verwaltung als auch die Wirtschaft sollte die Einführung solcher datenschutzfördernder Systeme unterstützen.

16.1.9 Entschließung zwischen der 75. und 76 Konferenz der Datenschutzbeauftragen des Bundes und der Länder vom 16. September 2008: Entschlossenes Handeln ist das Gebot der Stunde

Nie haben sich in der jüngeren Geschichte die Skandale um den Missbrauch privater Daten in der Wirtschaft so gehäuft wie heute und damit deutlich gemacht, dass nicht nur im Verhältnis Bürger-Staat das Grundrecht auf informationelle Selbstbestimmung bedroht ist. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat wiederholt - zuletzt in ihrer Berliner Erklärung vom 4. April dieses Jahres - auf diese Gefahren hingewiesen, die von massenhaften Datensammlungen privater Unternehmen und ihrer unkontrollierten Nutzung ausgehen. Sie hat auch deshalb den Gesetzgeber zu einer grundlegenden Modernisierung und Verbesserung des Datenschutzrechts aufgefordert und eine neue Datenschutzkultur angemahnt.

Dass jetzt endlich im politischen und gesellschaftlichen Raum die Problematik erkannt und diskutiert wird, ist zu begrüßen. Dabei kann und darf es aber nicht bleiben, nur entschlossenes Handeln kann die Bürgerinnen und Bürger vor weiterem Missbrauch ihrer persönlichen Daten schützen und das verlorene Vertrauen wiederherstellen.

Das vom Grundgesetz garantierte Recht eines Jeden, selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten zu entscheiden, muss endlich die ihm gebührende Beachtung finden. Die Weitergabe von persönlichen Angaben zu Werbezwecken darf nur mit ausdrücklicher Einwilligung der Betroffenen zulässig sein. Daten sind mit einem Vermerk über ihre Quelle zu kennzeichnen. Der Abschluss von Verträgen darf nicht von der Einwilligung in die Datenübermittlung zu Werbezwecken abhängig gemacht werden. Verstöße gegen den Datenschutz dürfen nicht ohne Konsequenzen bleiben, sondern müssen strikt geahndet werden. Deshalb müssen die bestehenden Lücken in den Bußgeld- und Strafbestimmungen geschlossen und der Bußgeld- und Strafrahmen für Datenschutzverstöße deutlich erhöht werden. Diese Sofortmaßnahmen, die bereits Gegenstand des Spitzentreffens im Bundesministerium des Innern am 4. September 2008 waren, können vom Deutschen Bundestag noch in den bereits vorliegenden Gesetzentwurf zur Änderung des Bundesdatenschutzgesetzes aufgenommen werden.

Gesetzgeberische Maßnahmen allein helfen aber nicht weiter, wenn ihre Einhaltung nicht ausreichend kontrolliert und Verstöße nicht sanktioniert werden können. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert deswegen,

die Datenschutzaufsichtsbehörden endlich organisatorisch, personell und finanziell in die Lage zu versetzen, ihren Beratungs- und Kontrollaufgaben flächendeckend, unabhängig und wirkungsvoll nachkommen zu können, und entsprechend der EU-Datenschutzrichtlinie mit wirksamen Einwirkungsbefugnissen auszustatten, die sie bisher nicht haben.

Außerdem müssen Konzepte zur grundlegenden Modernisierung des Datenschutzes entwickelt und umgesetzt werden. Wichtige Themen sollten dabei noch in dieser Legislaturperiode angegangen werden:

- Verbesserung der Protokollierung des Datenzugriffs in automatisierten Verfahren
- Stärkung der datenschutzrechtlichen Auskunftsrechte
- Pflicht zur Information der betroffenen Personen und der Aufsichtsbehörden bei Datenpannen und missbräuchlicher Datennutzung
- Gewinnabschöpfung aus unbefugtem Datenhandel
- Einführung eines gesetzlich geregelten Datenschutzaudits, mit dem unabhängig und qualifiziert die Datenschutzkonformität von Verfahren und Produkten bestätigt wird
- Stärkung der betrieblichen Datenschutzbeauftragten als Organ der Selbstkontrolle
- Spezialisierung der Strafverfolgungsbehörden
- Anerkennung von Datenschutzbestimmungen als verbraucherschützende Normen

Nur wenn jetzt den Ankündigungen Taten folgen und entschlossen gehandelt wird, können die Bürgerinnen und Bürger künftig vor Datenmissbrauch und Verletzung ihres Grundrechts auf informationelle Selbstbestimmung besser als in der Vergangenheit geschützt werden.

16.1.10 Entschließung der 76. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 6./7. November 2008 in Bonn: Adress- und Datenhandel nur mit Einwilligung der Betroffenen

Der auf dem „Datenschutzgipfel“ im September 2008 gefundene Konsens, den Adress- und Datenhandel zukünftig nur auf der Grundlage einer Einwilligung zuzulassen, ist in Politik und Gesellschaft auf breite Zustimmung gestoßen. Nur eine solche Lösung respektiert das informationelle Selbstbestimmungsrecht und damit die Wahlfreiheit der Verbraucherinnen und Verbraucher. Wer davon jetzt abrücken will, verkennt die auf Grund der jüngsten Datenskandale ans Licht gekommenen Missstände, deren Ursache nicht nur in der kriminellen Energie Einzelner zu suchen ist. Um die Daten der Betroffenen tatsächlich wirksam schützen zu können, muss die Wahlmöglichkeit der Menschen von Maßnahmen flankiert werden, die die Herkunft der Daten jederzeit nachvollziehbar machten.

Die von der Werbewirtschaft gegen die Einwilligungslösung ins Feld geführten Argumente sind nicht überzeugend. Die behaupteten negativen Folgen für den Wirtschaftsstandort sind nicht zu belegen. Unabhängig davon gilt: Es gibt keine schutzwürdigen Interessen für die Beibehaltung von Geschäftsmodellen, die darauf beruhen, hinter dem Rücken und ohne Information der Betroffenen mit deren Daten Handel zu treiben. Die Einführung des Einwilligungsprinzips würde im Gegenteil zielgenaueres und wirksameres Direktmarketing erlauben. Die Bundesregierung sollte sich deshalb nicht von ihrer Absicht abbringen lassen, die beim „Datenschutzgipfel“ gegebenen Zusagen zur schnellen Verbesserung des Datenschutzes einzulösen. Sie würde es sonst versäumen, die notwendigen Lehren aus den jüngsten Skandalen zu ziehen. Der Referentenentwurf des Bundesinnenministeriums zur Änderung des Bundesdatenschutzgesetzes im Bereich des Adress- und Datenhandels (Stand: 22. Oktober 2008) zieht mit der Einwilligungslösung - bei aller Verbesserungswürdigkeit im Detail - die einzig richtige und notwendige Konsequenz aus den zahlreichen Datenskandalen und darf nicht verwässert werden.

16.1.11 Entschließung der 76. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 6./7. November 2008 in Bonn: Abfrage von Telekommunikationsverkehrsdaten einschränken: Gesetzgeber und Praxis müssen aus wissenschaftlichen Erkenntnissen Konsequenzen ziehen

Das Max-Planck-Institut für ausländisches und internationales Strafrecht in Freiburg hat im Auftrag des Bundesministeriums der Justiz die Nutzung von Telekommunikationsverkehrsdaten für Zwecke der Strafverfolgung (§§ 100g, 100h StPO alte Fassung) evaluiert. Die Studie geht zu Recht davon aus, dass Verkehrsdaten ein hohes Überwachungspotential in sich tragen und besser als andere Daten dazu geeignet sind, soziale Netzwerke nachzuweisen, Beziehungen zu identifizieren und Informationen über Individuen zu generieren. Der Studie zufolge ist die Zahl der Verkehrsdatenabfragen erheblich und kontinuierlich von 10.200 (2002) auf 40.000 Abfragen (2005) angestiegen. Zudem erfasst die Maßnahme regelmäßig auch eine Vielzahl unbescholtener Bürgerinnen und Bürger.

Das Bundesministerium der Justiz hat die Studie erst im Februar dieses Jahres und somit nach der Neuregelung der Telekommunikationsüberwachung und Einführung der Vorratsdatenspeicherung veröffentlicht. Das Gutachten liefert Erkenntnisse, deren Berücksichtigung im Gesetz vom 21. Dezember 2007 erforderlich gewesen wäre. Die Datenschutzbeauftragten des Bundes und der Länder sehen sich durch die Studie in ihrer schon früher geäußerten Kritik (vgl. ihre Entschließung vom 8./9. März 2007) be-

stätigt. Sie fordern den Gesetzgeber auf, die gesetzliche Regelung unter folgenden Aspekten nun zügig nachzubessern:

- Die Straftatenschwelle für Verkehrsdatenabfragen sollte insbesondere im Hinblick auf die inzwischen eingeführte Vorratsdatenspeicherung auf schwere Straftaten angehoben werden. Ein bedeutsamer Anteil der überprüften Verfahren war allenfalls der mittleren Kriminalität zuzuordnen.

- Die gesetzliche Höchstdauer der Maßnahme sollte von drei auf zwei Monate reduziert werden. Das Gutachten hat gezeigt, dass die praktischen Bedürfnisse, wie sie sich in den Aktendaten und Befragungsergebnissen äußern, dadurch vollständig abgedeckt würden.

- Für die Verkehrsdatenabfrage sollten (nach dem Vorbild der Regelungen für die akustische Wohnraumüberwachung) qualifizierte Begründungspflichten in der StPO vorgesehen werden. Dabei sollten auch die Rechtsfolgen für erhebliche Verstöße gegen die Begründungsanforderungen gesetzlich geregelt werden (z. B. Beweisverwertungsverbote). Wesentliche Kritikpunkte der Studie waren insbesondere die lediglich formelhafte Wiedergabe des Gesetzestextes sowie die häufig wörtliche Übernahme der staatsanwaltschaftlichen Anträge in den Begründungen.

- Zur Vermeidung von Rechtsunsicherheit und zur Stärkung des Richtervorbehalts sollte in den Fällen staatsanwaltschaftlicher Eilanordnung die Verwertbarkeit der erlangten Daten davon abhängig gemacht werden, dass ein Gericht rückwirkend die formelle und materielle Rechtmäßigkeit der Maßnahme feststellt. Dem Gutachten zufolge besteht insbesondere bei den Telekommunikationsunternehmen Unsicherheit, inwieweit sie zur Herausgabe der Verkehrsdaten verpflichtet sind, wenn eine staatsanwaltschaftliche Eilanordnung nicht innerhalb der gesetzlichen Frist richterlich bestätigt wird.

- Der tatsächliche Nutzen der Vorratsdatenspeicherung für die Strafverfolgung und damit die Erforderlichkeit der Maßnahme müssen in Frage gestellt werden. Bereits bei der früheren Höchstspeicherdauer von 3 Monaten waren nach der Studie 98 % der Abfragen erfolgreich.

Auch in der praktischen Anwendung der Regelungen zur Verkehrsdatenabfrage hat die Studie Defizite deutlich gemacht. Die Datenschutzbeauftragten des Bundes und der Länder appellieren daher auch an die Strafverfolgungsbehörden und Gerichte, aus dem Gutachten Konsequenzen zu ziehen. Besonderes Augenmerk ist vor allem auf die Prüfung der Angemessenheit der Maßnahme zu richten. Dies muss auch in substantiierten Begründungen zum Ausdruck kommen. Die gesetzlich festgeschriebenen, dem Grund-

rechtsschutz dienenden Benachrichtigungs-, Löschungs- und Dokumentationspflichten müssen - trotz hoher Belastungen in der Praxis - unbedingt eingehalten werden. Der Richtervorbehalt muss seine grundrechtssichernde Funktion effizient erfüllen können. Die Justizverwaltungen sind in der Verantwortung, hierfür ausreichende personelle Ressourcen zur Verfügung zu stellen.

Eine Fortführung der wissenschaftlichen Evaluation der Verkehrsdatenabfrage ist – unter den neuen rechtlichen Rahmenbedingungen und aufgrund der Weiterentwicklung der Technik - unerlässlich. Insbesondere sollten dabei Notwendigkeit und Nutzen der Verkehrsdatenabfrage - auch im Vergleich zu anderen möglichen Maßnahmen - mit Blick auf den Verhältnismäßigkeitsgrundsatz auf den Prüfstand gestellt werden.

16.1.12 Entschließung der 76. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 6./7. November 2008 in Bonn: Gegen Blankettbefugnisse für die Software-Industrie

Gegenwärtig wird auf europäischer Ebene über Änderungen der Richtlinie zum Datenschutz in der elektronischen Kommunikation (2002/58/EG) beraten. Dabei geht es auch um die Frage, ob in Zukunft einzelfallunabhängig Verkehrsdaten zur Gewährleistung der Netz- und Informationssicherheit, also etwa zur Verfolgung von Hackerangriffen, verarbeitet werden dürfen.

Bereits auf der Grundlage der geltenden Richtlinie erlaubt § 100 Telekommunikationsgesetz den Telekommunikationsdiensteanbietern eine zielgerichtete, einzelfallbezogene Datenverarbeitung zur Fehlerbeseitigung und Missbrauchsbekämpfung. Diese Regelung hat sich in der Praxis bewährt. Es ist daher nicht erforderlich, zur Gewährleistung der Netz- und Informationssicherheit einzelfallunabhängig personenbezogene Verkehrsdaten zu speichern. Die Anbieter von Telekommunikationsdiensten sind aufgefordert, ihre Systeme so sicher zu gestalten, dass Angriffe von vornherein erfolglos bleiben.

Obwohl die Europäische Kommission eine Änderung der bisherigen Rechtslage nicht für erforderlich hält, schlagen mehrere Mitgliedstaaten bei den gegenwärtigen Beratungen im Rat vor, entsprechend den Vorstellungen der Software-Industrie (Business Software Alliance) eine generelle Ermächtigung in die Richtlinie aufzunehmen, wonach „*jede natürliche oder juristische Person mit einem berechtigten Interesse*“ berechtigt sein soll, Verkehrsdaten zu verarbeiten, um „technische Maßnahmen zur Gewährleistung der Sicherheit eines öffentlichen Telekommunikationsdienstes, eines öffentlichen oder privaten Telekommunikationsnetzes, eines Dienstes der Informationsgesellschaft oder von Endgeräten zu deren Nutzung“ zu ergreifen. Damit wäre nicht nur der jeweilige Diensteanbieter, der Maßnahmen zum Schutz des eigenen Angebots treffen

will, zur einzelfallunabhängigen Speicherung von Verkehrsdaten berechtigt, sondern praktisch jeder mit einem wirtschaftlichen Verarbeitungsinteresse, insbesondere auch die Hersteller von Sicherheitssoftware.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder lehnt eine solche zeitlich unbegrenzte und inhaltlich unbestimmte Blankett-Ermächtigung als inakzeptabel ab. Der Hinweis auf die „Informationssicherheit“ rechtfertigt es nicht, dass Verkehrsdaten nahezu uferlos auch von Dritten verarbeitet werden. Die Bundesregierung wird aufgefordert, einer derartigen Aufweichung des Telekommunikationsgeheimnisses im Rat ihre Zustimmung zu verweigern.

16.1.13 Entschließung der 76. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 6./7. November 2008 in Bonn: Weiterhin verfassungsrechtliche Zweifel am ELENA-Verfahren

Die Bundesregierung hat am 25. Juni 2008 den Gesetzentwurf über das Verfahren des elektronischen Entgeltnachweises (ELENA-Verfahrensgesetz) beschlossen (BT-Drs. 16/10492). Danach haben Beschäftigte die monatliche Übermittlung ihrer Einkommensdaten an die Zentrale Speicherstelle zu dulden, obwohl zurzeit nicht verlässlich abgeschätzt werden kann, in welchem Umfang die Speicherung der Daten tatsächlich erforderlich ist. Ein großer Anteil der Betroffenen wird die dem Anwendungsbereich des ELENA-Verfahrens unterfallenden Sozialleistungen niemals oder erst zu einem erheblich späteren Zeitpunkt geltend machen. Es steht somit bereits jetzt zu vermuten, dass eine große Zahl der übermittelten Daten von der Zentralen Speicherstelle wieder zu löschen sein wird, ohne jemals für irgendein Verfahren genutzt worden zu sein.

Die Datenschutzbeauftragten des Bundes und der Länder haben deshalb wiederholt verfassungsrechtliche Bedenken unter dem Gesichtspunkt der Verhältnismäßigkeit und speziell der Erforderlichkeit geltend gemacht und eine substantiierte Begründung gefordert. Diese ist nicht erfolgt. Bisher bestehen lediglich höchst vage Erwartungen auf langfristige Effizienzsteigerungen insbesondere der Arbeitsverwaltung. Angesichts dieser Unklarheiten verbleiben erhebliche Zweifel an der Verfassungsmäßigkeit des Gesetzes. Hinzu kommt, dass derartige umfangreiche Datensammlungen Begehrlichkeiten wecken, die Daten für andere Zwecke zu verwenden.

Für den Fall, dass diese verfassungsrechtlichen Bedenken ausgeräumt werden können, sind unter dem Gesichtspunkt des technisch-organisatorischen Datenschutzes noch folgende Verbesserungen durch den Gesetz- bzw. Verordnungsgeber erforderlich:

- Es muss sichergestellt werden, (z. B. durch die Einrichtung eines Verwaltungsausschusses der Zentralen Speicherstelle), dass unter Mitwirkung von Datenschutzbeauf-

tragten gemeinsame Grundsätze zur Wahrung des Datenschutzes und der technischen Sicherheit berücksichtigt werden.

- Für die Zentrale Speicherstelle muss ein Datenschutzbeauftragter eingesetzt werden, der dazu verpflichtet ist, regelmäßig an den Verwaltungsausschuss zu berichten.

- Schlüssel zur Ver- und Entschlüsselung der bei der Zentralen Speicherstelle gespeicherten Daten dürfen nicht in der Verfügungsgewalt der Zentralen Speicherstelle liegen. Die Ver- und Entschlüsselungskomponente muss von einer unabhängigen Treuhänderstelle verantwortet werden.

- Mittelfristig ist ein Verfahren anzustreben, das die technische Verfügungsmöglichkeit über die individuellen Daten den Betroffenen überträgt.

- Das im Rahmen der ELENA-Modellvorhaben erarbeitete differenzierte Löschungskonzept muss weiterentwickelt und umgesetzt werden.

- Für abrufende Stellen sind starke Authentisierungsverfahren vorzuschreiben, die dem Stand der Technik entsprechen und den Forderungen der Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 11. Oktober 2006 zur sachgemäßen Nutzung von Authentisierungs- und Signaturverfahren genügen.

- Für die technischen Komponenten muss eine Zertifizierung durch eine unabhängige Prüfung vorgeschrieben werden.

16.1.14 Entschließung der 76. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 6./7. November 2008 in Bonn: Datenschutzgerechter Zugang zu Geoinformationen

Die Einführung einer einheitlichen Geodateninfrastruktur und die Veröffentlichung der staatlichen Daten eröffnen ein großes Potential an volkswirtschaftlichem Nutzen und ist geeignet, vielen E-Government- und E-Commerce-Anwendungen die erforderliche Infrastruktur zur Verfügung zu stellen. Als einen ersten Schritt regelt das europäische Recht mit der so genannten INSPIRE-Richtlinie, die bis Mai 2009 in nationales Recht umgesetzt werden muss, die Bereitstellung von amtlichen Geodaten nach einheitlichen Standards für europaweite behördliche, kommerzielle und private Nutzungen.

Durch diese neue Infrastruktur werden georeferenzierbare Angaben auf Grund der Erschließungsmöglichkeit über Wohnanschriften oder Eigentümer- bzw. Standortdaten als personenbezogene Daten zur Verfügung gestellt. Diesem Umstand müssen die ge-

setzlichen Regelungen gerecht werden und angemessene Datenschutzregelungen enthalten.

Bei der Bereitstellung amtlicher Geodaten ist sowohl nach der europäischen Richtlinie als auch nach deutschem Verfassungsrecht der Schutz personenbezogener Daten angemessen zu gewährleisten. Der Entwurf der Bundesregierung zur Umsetzung dieser Richtlinie in einem Geodatenzugangsgesetz (BT-Drs. 16/10530) sieht eine entsprechende Anwendung der Schutzvorschriften des Umweltinformationsgesetzes vor. Im Gegensatz zum einzelfallbezogenen Zugang nach den Umweltinformationsgesetzen birgt der im Entwurf eines Geodatenzugangsgesetzes vorgesehene massenhafte Abruf solcher Daten aber ein höheres datenschutzrechtliches Gefährdungspotenzial. Der Verweis auf das Umweltinformationsgesetz ist nach Ansicht der Konferenzen der Datenschutz- und der Informationsfreiheitsbeauftragten des Bundes und der Länder deshalb nicht interessengerecht. Ein Geodatenzugangsgesetz muss einen differenzierenden Ausgleich zwischen Informations- und Schutzinteressen für die spezielle Problematik der Geobasis- und der Geofachdaten vornehmen. Es ist insbesondere zu berücksichtigen, dass nach der INSPIRE-Richtlinie die Zugangsmöglichkeit eingeschränkt werden soll, wenn der Zugang nachteilige Auswirkungen auf die Vertraulichkeit personenbezogener Daten haben kann.

16.1.15 Entschließung der 76. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 6./7. November 200 in Bonn: Mehr Transparenz durch Informationspflichten bei Datenschutzpannen

In den letzten Monaten hat eine Reihe von gravierenden Datenschutzverstößen die Aufmerksamkeit der Öffentlichkeit und der Medien gefunden. In vielen dieser Fälle lag der Verlust oder Missbrauch personenbezogener Daten längere Zeit zurück und war der verantwortlichen Stelle bekannt, ohne dass die Betroffenen oder die zuständige Datenschutzaufsichtsbehörde hierüber informiert worden wären. Dadurch wurde ihnen die Möglichkeit genommen, Sicherheitsmaßnahmen zu ergreifen und mögliche Schäden zu begrenzen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bekräftigt deswegen die Forderung, alle verantwortlichen Stellen - grundsätzlich auch alle öffentlichen Stellen - gesetzlich zu verpflichten, bei Verlust, Diebstahl oder Missbrauch personenbezogener Daten unverzüglich die hiervon betroffenen Bürgerinnen und Bürger und die zuständigen Aufsichts- oder Kontrollbehörden sowie gegebenenfalls auch die Öffentlichkeit zu unterrichten. Dies entspricht ihrer datenschutzrechtlichen Verantwortung und ermöglicht es den Betroffenen, negative Konsequenzen solcher Datenschutzpannen abzuwenden oder einzugrenzen. Hinter diesem Interesse hat der Wunsch der

entsprechenden Stellen zurückzustehen, solche Vorkommnisse geheim zu halten, um keinen Imageschaden oder keine wirtschaftlichen Nachteile zu erleiden.

Etliche Staaten haben bereits entsprechende Regelungen. Eine solche Informationspflicht würde die Transparenz erhöhen und das Vertrauen der Betroffenen in eine korrekte Datenverarbeitung stärken. Darüber hinaus würde sie einen wichtigen Anstoß geben, mehr für Datenschutz und Datensicherheit zu tun.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert deswegen, entsprechende umfassende Informationspflichten für Unternehmen und öffentliche Stellen im Bundesdatenschutzgesetz und den Landesdatenschutzgesetzen zu schaffen. Die übrigen aus Anlass der Datenschutzskandale in einer Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 16. September 2008 erläuterten Forderungen zur Novellierung des Bundesdatenschutzgesetzes werden bekräftigt.

16.1.16 Entschließung der 76. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 6./7. November 2008 in Bonn: Steuerungsprogramme der gesetzlichen Krankenkassen datenschutzkonform gestalten

Mit der Gesundheitsreform soll über die Einführung von Wettbewerbsmechanismen die Qualität und Effizienz der gesetzlichen Krankenkassen verbessert werden. Die Kassen sind daher bemüht und auch vom Gesetzgeber gehalten, Versicherten ein Versorgungsmanagement anzubieten. Von zentraler Bedeutung sind dabei Patientenschulungsmaßnahmen und strukturierte Behandlungsprogramme für chronisch kranke Versicherte, die jedoch lediglich Angebotscharakter haben dürfen. Ihre Teilnahme soll nach dem Willen des Gesetzgebers freiwillig sein und eine eingehende Unterrichtung voraussetzen. Diese Vorgaben werden von einzelnen Krankenkassen nicht beachtet, wenn sie versuchen, die Versicherten in ihrem Gesundheitsverhalten zu steuern und sie in bestimmte Maßnahmen und Programme zu drängen.

Um Teilnehmerinnen und Teilnehmer zu gewinnen und um Maßnahmen durchzuführen, bedienen sich die Kassen vielfach privater Dienstleister und offenbaren diesen teils höchst sensible Gesundheitsdaten ihrer Versicherten. Dies ist datenschutzrechtlich nach dem Sozialgesetzbuch unzulässig, wenn die Übermittlung ohne Kenntnis und vorherige Einwilligung der jeweiligen Versicherten erfolgt.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hält die Einhaltung insbesondere der folgenden Eckpunkte bei gesundheitlichen Steuerungsprogrammen der Krankenkassen für unerlässlich:

- Die Krankenkassen dürfen Versichertendaten nur dann zur Auswahl von Personen für besondere Gesundheitsmaßnahmen verwenden, wenn dies gesetzlich ausdrücklich vorgesehen ist. Es muss sich um valide und erforderliche Daten handeln. Mit der Auswahl darf kein privater Dienstleister beauftragt werden.

- Die erstmalige Kontaktaufnahme mit potenziell für eine Gesundheitsmaßnahme in Betracht kommenden Versicherten muss durch die Krankenkasse selbst erfolgen, auch wenn ein privater Dienstleister mit der späteren Durchführung der Gesundheitsmaßnahme beauftragt worden ist.

- Die Versicherten sind vor Übermittlung ihrer Daten umfassend zu informieren. Die Information muss auch den Umstand umfassen, dass ein privates Unternehmen mit der Durchführung betraut werden soll. Soweit die Versicherten ausdrücklich in die Teilnahme eingewilligt haben, dürfen die für die Durchführung der Maßnahme erforderlichen Daten an den Dienstleister übermittelt werden.

- Wenn Versicherte - zu welchem Zeitpunkt auch immer - eindeutig zum Ausdruck bringen, nicht an einer Maßnahme teilnehmen zu wollen oder nicht an weitergehenden Informationen, einer konkreten Anwerbung oder einer fortgesetzten Betreuung interessiert zu sein, ist dies zu respektieren. Weitere Maßnahmen (auch telefonische Überredungsversuche) sind zu unterlassen.

16.1.17 Entschließung der 76. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 6./7. November 2008 in Bonn: Angemessener Datenschutz bei der polizeilichen und justiziellen Zusammenarbeit in der EU dringend erforderlich

Auf europäischer Ebene ist eine Vielzahl von Vorhaben beschlossen bzw. initiiert worden, die in ihrer Gesamtheit zu erheblichen Eingriffen in die Persönlichkeitsrechte führt:

- Die Telekommunikationsunternehmen in den Mitgliedstaaten der EU sind verpflichtet, die bei der Nutzung öffentlich zugänglicher Telekommunikationsdienste anfallenden Verkehrsdaten über das Kommunikationsverhalten der Einzelnen für die Sicherheitsbehörden ohne konkreten Anlass auf Vorrat zu speichern.

- Die Pässe der Bürgerinnen und Bürger der EU-Mitgliedstaaten werden mit biometrischen Merkmalen ausgestattet.

- Fluggastdaten (PNR) werden in die USA übermittelt, um sie den dortigen Behörden zur Verfügung zu stellen. Die Nutzung von Fluggastdaten zu Strafverfolgungszwecken wird auch in der Europäischen Union vorbereitet.

- Der Vertrag von Prüm, der in den Rechtsrahmen der Union überführt wird, ermöglicht den Polizei- und Strafverfolgungsbehörden der Mitgliedstaaten einen gegenseitigen Zugriff auf Fingerabdruck-, DANN- und Kfz-Daten.

- Es soll ein Europäisches Strafregisterinformationssystem geschaffen werden, mit dem Informationen über strafrechtliche Verurteilungen zwischen den Mitgliedstaaten ausgetauscht werden können.

- Das Schengener Informationssystem wird weiter ausgebaut, u. a. durch die Speicherung von biometrischen Merkmalen. Zudem wird der Kreis der Nutzer erweitert um das Europäische Polizeiamt EUROPOL und die Einheit für justizielle Zusammenarbeit in der EU (EUROJUST).

- Ein Europäisches Visa-Informationssystem (VIS) wird eingeführt, um den Austausch von Visa-Daten zwischen den Mitgliedstaaten zu erleichtern. Auch für EUROPOL, die Sicherheitsbehörden und die Nachrichtendienste soll dieser Datenbestand zugänglich sein.

- Das europäische Verfahren EURODAC, in dem die Fingerabdrücke von Asylbewerberinnen und Asylbewerbern gespeichert sind, soll auch von der Polizei und den Strafverfolgungsbehörden genutzt werden können.

- Der Aufgabenbereich von EUROPOL soll über die Bekämpfung der Organisierten Kriminalität hinaus auch auf andere Formen der schweren Kriminalität erweitert werden. Außerdem soll EUROPOL erstmals die Befugnis erhalten, Daten auch von privaten Stellen entgegenzunehmen und Zugriff auf alle polizeilich relevanten Datenbanken in der EU bekommen.

- Der Informationsaustausch zwischen den Strafverfolgungsbehörden der EU wird entsprechend dem Rahmenbeschluss des Rates vom 18. Dezember 2006 („Schwedische Initiative“) ausgebaut. Danach soll der Austausch verfügbarer Daten innerhalb der EU zu den gleichen Bedingungen erfolgen wie nach nationalem Recht.

Neben diesen Vorhaben gibt es zudem Abkommen auf bilateraler Ebene zwischen EU-Mitgliedstaaten und Drittstaaten, wie z. B. das Abkommen der Bundesrepublik Deutschland mit den Vereinigten Staaten für einen erweiterten Informationsaustausch zwischen den Sicherheitsbehörden.

Der Aufbau zentraler Datenbestände und der Ausbau der grenzüberschreitenden Datenübermittlung greifen erheblich in das Grundrecht auf informationelle Selbstbestimmung ein und führen dadurch zu Gefahren für jede Einzelne und jeden Einzelnen. Diese werden noch gesteigert durch die angestrebte Verknüpfbarkeit der bestehenden und geplanten Datenbanken.

Umso wichtiger ist deshalb ein hoher und gleichwertiger Datenschutz bei der polizeilichen und justiziellen Zusammenarbeit in Europa. Dies wurde von den Datenschutzbeauftragten auf nationaler und europäischer Ebene mehrfach angemahnt. Der hierzu im Oktober 2005 vorgelegte Rahmenbeschluss-Vorschlag genügt diesen Anforderungen nicht (siehe dazu die Entschließung der 71. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 16./17. März 2006 „Mehr Datenschutz bei der polizeilichen und justiziellen Zusammenarbeit in Strafsachen“). Zur Wahrung des erforderlichen Gleichgewichts zwischen Freiheit und Sicherheit sollten die Parlamente und Regierungen ihre Einflussmöglichkeiten bei europäischen Vorhaben stärker nutzen und dabei auch datenschutzrechtliche Aspekte einbringen. Wie notwendig ein angemessener Datenschutz ist, hat sich beim Verfahren der Aufnahme Verdächtiger in die so genannte EU-Terrorliste gezeigt, das durch den Europäischen Gerichtshof für rechtswidrig erklärt wurde.

Die Datenschutzbeauftragten fordern deshalb:

- Bei jeder neuen Initiative ist das Verhältnismäßigkeitsprinzip zu wahren und deren Auswirkung auf das bestehende System von Eingriffsmaßnahmen zu berücksichtigen.

- Im Hinblick auf den Kumulationseffekt sind die verschiedenen europäischen Initiativen zudem grundrechtskonform aufeinander abzustimmen. Redundanzen und Überschneidungen müssen verhindert werden.

- Ein Rechtsakt muss unverzüglich beschlossen werden, der über den Rahmenbeschlussvorschlag hinaus einen hohen und gleichwertigen Datenschutzstandard bei der Verarbeitung personenbezogener Daten im Rahmen der polizeilichen und justiziellen Zusammenarbeit verbindlich vorschreibt. Die gesamte nationale und grenzüberschreitende Informationsverarbeitung in diesem Bereich muss davon erfasst sein, um ein einheitliches Datenschutzniveau in den EU-Mitgliedstaaten zu gewährleisten.

- Ein unabhängiges, beratendes Datenschutzgremium sowie eine unabhängige und umfassende datenschutzrechtliche Kontrolle müssen für die polizeiliche und justizielle Zusammenarbeit eingerichtet bzw. gewährleistet werden.

16.1.18 Entschließung der 76. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 6./7. November 2008 in Bonn: Besserer Datenschutz bei der Umsetzung der „Schwedischen Initiative“ zur Vereinfachung des polizeilichen Datenaustausches zwischen den EU-Mitgliedstaaten geboten

Der Rahmenbeschluss des Rates zur Vereinfachung des Informationsaustausches zwischen den Strafverfolgungsbehörden der EU-Mitgliedstaaten (sog. „Schwedische Initiative“) vom 18. Dezember 2006 verpflichtet diese, an die grenzüberschreitende Übermittlung personenbezogener Daten innerhalb der EU keine höheren Anforderungen zu stellen, als auf nationaler Ebene für den Datenaustausch zwischen Polizei- und Strafverfolgungsbehörden gelten. Seine Umsetzung wird zu einem deutlichen Anstieg und zur Beschleunigung des Informationsaustausches und damit zu einer weiteren Intensivierung der polizeilichen und justiziellen Zusammenarbeit in Strafsachen auf EU-Ebene führen. Das erstrebte Ziel, nämlich die Schaffung eines Raumes der Freiheit, der Sicherheit und des Rechts setzt aber auch voraus, dass in den Mitgliedstaaten ein möglichst gleichwertiger Datenschutz auf hohem Niveau besteht. Dies ist bislang nicht erfüllt. Es besteht nach wie vor der aus datenschutzrechtlicher Sicht unhaltbare Zustand, dass die auf EU-Ebene ausgetauschten polizeilichen Informationen in den jeweiligen EU-Mitgliedstaaten unterschiedlichen Datenschutzregelungen hinsichtlich ihrer Verwendung unterworfen sind. Zudem gelten keine einheitlichen Rechte auf Auskunft, Berichtigung und Löschung der Datenverarbeitung für die Betroffenen in den Empfängerstaaten.

Vor diesem Hintergrund fordern die Datenschutzbeauftragten des Bundes und der Länder den Gesetzgeber auf, den bei der innerstaatlichen Umsetzung der „Schwedischen Initiative“ verbleibenden Spielraum zu nutzen und die Befugnisse zum Informationsaustausch mit den Strafverfolgungsbehörden der EU-Mitgliedstaaten für die nationalen Polizei- und Strafverfolgungsbehörden normenklar und unter Beachtung des Grundsatzes der Verhältnismäßigkeit gesetzlich zu regeln. Dazu zählen insbesondere:

- Ausschluss der gesonderten Erhebung der angefragten Daten durch die Strafverfolgungsbehörden allein um diese zu übermitteln.

- Eindeutige inhaltliche Anforderungen, die an ein Ersuchen um Datenübermittlung zu stellen sind, um Überschussinformationen zu vermeiden,

- Regelung enger Voraussetzungen für sog. Spontanübermittlungen, um für den Empfänger nutzlose und damit nicht erforderliche Übermittlungen auszuschließen,

- Nutzung des Spielraums bei der Ausgestaltung der Verweigerungsgründe, um unverhältnismäßige Datenübermittlungen zu verhindern,

- normenklare Abgrenzung der Befugnis zur Übermittlung von Daten zu präventiven Zwecken gegenüber der justiziellen Rechtshilfe,

- vollständige Umsetzung der Datenschutzbestimmungen in Art. 8 des Rahmenbeschlusses und begrenzende Regelungen zur Weiterübermittlung an Drittstaaten,

- normenklare Bestimmung welche Behörden als zuständige Strafverfolgungsbehörden im Sinne des Rahmenbeschlusses gelten und welche Informationen nur durch Ergreifen von Zwangsmaßnahmen im Sinne des Rahmenbeschlusses verfügbar sind,

- normenklare Bestimmung, welche Informationen nicht vom Rahmenbeschluss erfasst werden, weil sie für die Strafverfolgungsbehörden nur durch das Ergreifen von Zwangsmaßnahmen verfügbar sind.

16.1.19 Entschließung der 76. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 6./7. November 2008 in Bonn: Elektronische Steuererklärung sicher und datenschutzgerecht gestalten

Mit dem Steuerbürokratieabbaugesetz (BR-DS 547/08) sollen u. a. verfahrenstechnische Regelungen für die elektronische Übermittlung von Steuererklärungen durch Steuerpflichtige festgelegt werden. Zu diesem Zweck soll § 150 Abgabenordnung (AO) durch Abs. 7 Satz 1 dahingehend ergänzt werden, dass bei Einführung einer Verpflichtung zur elektronischen Abgabe die übermittelten Steuerdaten mit einer qualifizierten Signatur nach dem Signaturgesetz zu versehen sind.

Die Konferenz sieht es kritisch, dass § 150 Abs. 7 Satz 2 Nrn. 6 und 7 AO auch vorsieht, zur Erleichterung und Vereinfachung des automatisierten Besteuerungsverfahrens *anstelle* der qualifizierten elektronischen Signatur ein so genanntes anderes sicheres Verfahren im Benehmen mit dem Bundesinnenministerium zuzulassen oder sogar auf beide Verfahren vollständig zu verzichten. In der Gesetzesbegründung wird darauf verwiesen, dass neben der qualifizierten elektronischen Signatur künftig auch eine Übermittlung der Daten unter Nutzung der Möglichkeiten des neuen elektronischen Personalausweises möglich sein soll.

Bereits in ihrer Entschließung zur sachgemäßen Nutzung von Authentisierungs- und Signaturverfahren vom 11. Oktober 2006 hat die Konferenz gefordert, Nutzenden die Möglichkeit zu eröffnen, die elektronische Kommunikation mit der Verwaltung durch eine qualifizierte elektronische Signatur abzusichern. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt daher die vorgesehene Regelung in der AO zur Nutzung der qualifizierten elektronischen Signatur, da dieses Verfahren ge-

eignet ist, die Authentizität und Integrität eines elektronisch übermittelten Dokuments sicherzustellen, und somit die handschriftliche Unterschrift ersetzen kann.

Die Datenschutzbeauftragten des Bundes und der Länder erklären hierzu:

1. Das Verfahren der qualifizierten elektronischen Signatur nach dem Signaturgesetz ist im Hinblick auf die Authentizität und Integrität elektronisch übermittelter Dokumente derzeit alternativlos.

2. Für die Bewertung anderer Verfahren sollte unmittelbar auf die Fachkenntnis unabhängiger Gutachter abgestellt werden. Als Gutachter für die Beurteilung der technischen Sicherheit kämen etwa die Bundesnetzagentur oder das BSI in Frage.

3. Steuerpflichtige müssen auch im elektronischen Besteuerungsverfahren die Möglichkeit haben, die elektronische Kommunikation mit der Finanzverwaltung durch das hierfür geeignete Verfahren der qualifizierten elektronischen Signatur abzusichern.

16.1.20 Entschließung der 77. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 26./27. März 2009 in Berlin: Auskunftsanspruch der Steuerpflichtigen im Besteuerungsverfahren gewährleisten!

Das Bundesministerium der Finanzen (BMF) hat mit einer einfachen Verwaltungsanweisung den Auskunftsanspruch der Bürgerinnen und Bürger im Besteuerungsverfahren weitgehend eingeschränkt. Es macht die Auskunftserteilung von einem „berechtigten Interesse“ abhängig, was zu einer Einschränkung des Auskunftsrechts führt.

Die Vorgehensweise des BMF steht im krassen Widerspruch zum Beschluss des Bundesverfassungsgerichts vom 10. März 2008 (1 BvR 2388/03). Danach sind auch von der Finanzverwaltung die Grundrechte auf informationelle Selbstbestimmung und auf effektiven Rechtsschutz zu gewährleisten. Der in § 19 Bundesdatenschutzgesetz (BDSG) verankerte umfassende Auskunftsanspruch findet auch im Besteuerungsverfahren unmittelbare Anwendung.

Es ist inakzeptabel, dass verfassungsrechtlich garantierte Auskunftsrechte der Steuerpflichtigen ausgehebelt werden. Auch die Finanzverwaltung ist an Recht und Gesetz gebunden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert, dass das BMF die Verwaltungsanweisung vom 17. Dezember 2008 unverzüglich aufhebt. Die Finanzbehörden des Bundes und der Länder sind zu verpflichten, entsprechend der Rechtslage den Auskunftsanspruch zu erfüllen. Die Datenschutzbeauftragten des Bun-

des und der Länder appellieren zudem an den Bundesgesetzgeber, den Auskunftsanspruch der Steuerpflichtigen durch eine eindeutige Regelung in der Abgabenordnung klarzustellen, die dem § 19 BDSG entspricht.

16.1.21 Entschließung der 77. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 26./27. März 2009 in Berlin: Die polizeiliche Datenverarbeitung in INPOL hat keine Rechtsgrundlage

Die Speicherung von Daten im polizeilichen Informationssystem INPOL durch die Polizeien des Bundes und der Länder ist nur dann rechtmäßig, wenn eine Rechtsverordnung gemäß § 7 Abs. 6 Bundeskriminalamtsgesetz das Nähere über die Art der Daten bestimmt, die in dieser Datei gespeichert werden dürfen. Eine solche Rechtsverordnung existiert nicht. Mit Urteil vom 16. Dezember 2008 (Az. 11 LC 229/08) hat das Niedersächsische Oberverwaltungsgericht dies in Bezug auf die Verbunddatei „Gewalttäter Sport“ bekräftigt. Das Urteil ist nicht nur für die Rechtmäßigkeit der Hooligan-Datei bedeutsam, sondern hat Auswirkung auf alle im Rahmen von INPOL geführten Verbunddateien.

Mit der Entscheidung des Gerichts wird die Auffassung der Datenschutzbeauftragten des Bundes und der Länder bestätigt. Die vom Bundesministerium des Innern bisher vertretene Auffassung, wonach die Rechtsverordnung keine Zulässigkeitsvoraussetzung für die Datenverarbeitung in den Verbunddateien sei, wird durch die einschlägigen Regelungen nicht gestützt.

Ohne eine derartige Rechtsverordnung ist die Gesamtheit der in Verbunddateien stattfindenden polizeilichen Datenverarbeitungen rechtswidrig. Die Datenschutzbeauftragten von Bund und Länder fordern das Bundesministerium des Innern und die Landesregierungen auf, unverzüglich daraus Konsequenzen zu ziehen und die polizeiliche Datenverarbeitung auf den Prüfstand zu stellen.

16.1.22 Entschließung der 77. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 26./27. März 2009 in Berlin: Defizite beim Datenschutz jetzt beseitigen!

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Gesetzgeber in Deutschland auf, endlich die nötigen Konsequenzen aus den nicht mehr abreißenden Datenskandalen zu ziehen. Dazu sind mindestens folgende Schritte geboten:

1. Der Deutsche Bundestag wird aufgefordert, noch in dieser Legislaturperiode die von der Bundesregierung vorgelegten Gesetzentwürfe für erste notwendige Korrekturen

des Bundesdatenschutzgesetzes im Bereich der Auskunfteien und des Adresshandels zu verabschieden. Ansonsten verlieren die Bürgerinnen und Bürger das Vertrauen in die Zusagen der Bundesregierung nach den Skandalen des Jahres 2008. Insbesondere mit Adressen darf nur noch mit ausdrücklicher Einwilligung der Betroffenen Handel getrieben werden. Der Entwurf für ein Datenschutzauditgesetz muss gründlich überarbeitet werden, damit dieser notwendige Schritt hin zu einem modernen Datenschutzrecht von der Praxis auch umgesetzt werden kann.

2. Mit Beginn der nächsten Legislaturperiode muss endlich eine grundlegende Modernisierung des Datenschutzrechts in Angriff genommen werden, die bereits zu lange aufgeschoben wurde. Nur so kann das Datenschutzrecht den Herausforderungen der Informationsgesellschaft zu Beginn des 21. Jahrhunderts gerecht werden.

3. Der Einsatz datenschutzfreundlicher Technik muss vorangetrieben und rechtlich verpflichtend vorgeschrieben werden. Darin liegt auch eine Chance für den Wirtschaftsstandort Deutschland in Zeiten der Krise.

16.1.23 Entschließung der 77. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 26./27. März 2009 in Berlin: Eckpunkte für ein Gesetz zum Beschäftigtendatenschutz

Datenskandale der letzten Zeit haben deutlich gemacht, dass bei der Verarbeitung von Beschäftigtendaten weder Transparenz noch Rechtssicherheit besteht. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Bundesregierung auf, nach jahrelanger Untätigkeit jetzt unverzüglich einen entsprechenden Gesetzentwurf vorzulegen.

Ziel des neuen Beschäftigtendatenschutzgesetzes muss sein, Rechtssicherheit herzustellen, Regelungslücken zu schließen und bereits vorhandene Regelungsaspekte sowie Vorgaben der Rechtsprechung in einem Spezialgesetz zusammenzufassen. Die Konferenz der Datenschutzbeauftragten hält deshalb vor allem folgende Eckpunkte für unverzichtbar:

- Die Regelungen des Beschäftigtendatenschutzgesetzes müssen sowohl für die Beschäftigten der Privatwirtschaft als auch für die Beschäftigten im öffentlichen Dienst gelten.

- Es muss klar geregelt werden, welche Daten Unternehmen und öffentliche Stellen im Rahmen des Einstellungsverfahrens und im weiteren Verlauf des Arbeitslebens über ihre Beschäftigten erheben dürfen, wie sie damit verfahren müssen und wozu sie die Daten nutzen dürfen. Es bedarf besonderer Festlegungen im Hinblick auf Gesund-

heitsdaten (u. a. zur Frage der Zulässigkeit von Drogen-Screening, psychologischen Testverfahren, ärztlichen Untersuchungen, etc.)

- Einen umfassenden anlass- und verdachtslosen Datenabgleich darf es nicht geben. Der Zugriff von Kontrollinstanzen wie z. B. der Innenrevision auf erhobene Personaldaten bedarf enger gesetzlicher Vorgaben.

- Moderne Informations- und Kommunikationstechnologien dürfen nicht zu lückenlosen Verhaltens- und Leistungskontrollen eingesetzt werden. Da die Nutzung von Telefon, Internet und E-Mail-Diensten nicht mehr aus dem Arbeitsleben wegzudenken ist, sind auch die Voraussetzungen für eine beschäftigtenbezogene Auswertung dieser Kommunikationsmittel eindeutig und restriktiv festzulegen. Dabei ist auch zu regeln, welcher Personenkreis solche Auswertungen durchführen darf und ab welchem Verfahrensstand ggf. Dritte (z. B. Mitarbeitervertretungen oder Datenschutzbeauftragte) hinzugezogen werden müssen. Auswertungen von Datenbeständen der Zugangs- und Personalinformationssysteme sind strikt zu begrenzen.

- Der Einsatz von Überwachungssystemen, wie z. B. Videokameras und Ortungssystemen, ist auf das unbedingt notwendige Maß zu beschränken und unter Wahrung der Beteiligungsrechte der Mitarbeitervertretungen zulässig. Die Verwendung biometrischer Verfahren bedarf besonders enger Vorgaben.

- Es bedarf der Festlegung der Rechte der Beschäftigten, z. B. im Hinblick auf Auskunfts-, Einsichts-, Widerrufs-, Berichtigungs-, Löschungs- und Schadensersatzansprüche.

- Der Schutz von Persönlichkeitsrechten der in Deutschland tätigen Beschäftigten weltweit agierender Unternehmen oder Konzerne ist sicherzustellen.

- Eine effektive Kontrolle durch die zuständigen Datenschutzbehörden muss gewährleistet werden. Die betrieblichen und behördlichen Datenschutzbeauftragten sind bei allen personaldatenschutzrechtlich relevanten Verfahren und Entscheidungen frühzeitig einzubinden und umfassend zu beteiligen. Ihre Rechte und Befugnisse gegenüber den Mitarbeitervertretungen sind gesetzlich festzulegen.

- Verstöße gegen die Bestimmungen des Beschäftigtendatenschutzgesetzes müssen ein gesetzliches Verwertungsverbot der dadurch gewonnenen Daten nach sich ziehen. Zur Abschreckung bedarf es wirksamer Sanktionen.

16.1.24 Entschließung zwischen der 77. und 78. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 16. April 2009: Datenschutz beim vorgesehenen Bürgerportal unzureichend

Der Gesetzentwurf zur Regelung von Bürgerportalen (BR-DS 174/09) soll rechtliche Rahmenbedingungen für eine sichere und vertrauenswürdige elektronische Kommunikation zwischen Bürgerinnen und Bürgern und der Wirtschaft und Verwaltung im Internet schaffen. Private Anbieter sollen die Portale betreiben, über die der sichere E-Mail-Verkehr De-Mail, eine sichere Dokumentenablage De-Safe und ein Identitätsbescheinigungsdienst abgewickelt werden sollen. Eine solche Infrastruktur stellt hohe Anforderungen an die IT-Sicherheit und den Datenschutz.

Der Gesetzentwurf wird diesen Anforderungen noch nicht gerecht und ist zumindest in folgenden Punkten zu korrigieren:

- Der Entwurf sieht vor, dass nur akkreditierte Anbieter Portale betreiben dürfen. Voraussetzung für die Akkreditierung darf nicht allein der Nachweis der technischen und administrativen Sicherheit, sondern muss auch die tatsächliche Einhaltung datenschutzrechtlicher Standards sein. Die dabei zu erfüllenden Mindestanforderungen müssen verbindlich im Gesetz vorgegeben werden. Portalbetreiber sollten zudem erst dann die Akkreditierung erhalten, wenn die Umsetzung dieser Anforderungen durch unabhängige Prüfstellen bescheinigt wurde.

- Die Sicherung der Vertraulichkeit, Integrität und Authentizität von Nachrichteninhalten soll lediglich durch eine Verschlüsselung auf dem Transport zwischen den Diensteanbietern und durch die Sicherung des Zugangs zu den Bürgerportalen erfolgen. Es muss jedoch sichergestellt werden, dass Nachrichten auch bei den Portalbetreibern nicht durch Dritte gelesen oder verändert werden können. Deshalb muss die Kommunikation standardmäßig durch eine Ende-zu-Ende-Verschlüsselung zwischen Absendenden und Empfangenden nach dem Stand der Technik gesichert und nicht nur als Option angeboten werden.

- Das Bürgerportal soll gerade zwischen Bürgerinnen und Bürgern und Verwaltung eine rechtlich gesicherte Kommunikation ermöglichen. Insbesondere sind über das Bürgerportal förmliche Zustellungen mit den entsprechenden Rechtsfolgen beabsichtigt. Dies darf nur auf Basis einer sicheren Anmeldung erfolgen. Die nach der Gesetzesbegründung ebenfalls mögliche unsichere Anmeldung mit Passwort wird abgelehnt.

- Der Nachweis der Absenderin oder des Absenders soll lediglich durch Anmeldung am Bürgerportal erfolgen. Das ermöglicht Angriffe durch Schadsoftware auf dem Rechner der Nutzenden. So könnten Zugangsdaten beschafft und widerrechtlich dazu verwen-

det werden, De-Mails zu versenden, empfangene De-Mails zu unterdrücken, zu verzögern und zu verändern oder unberechtigt auf Daten im De-Safe zuzugreifen. Deshalb sind zusätzliche Sicherungsmaßnahmen vorzusehen.

- Die Möglichkeit, eine pseudonyme Bürgerportaladresse zu nutzen, muss - entgegen der Stellungnahme des Bundesrates vom 3. April 2009 - erhalten bleiben. Denn die pseudonyme Nutzung ermöglicht gerade einen sinnvollen Kompromiss zwischen hinreichender Identifizierbarkeit im Rechtsverkehr und Datenschutz für die Nutzerinnen und Nutzer.

- Die Nutzerinnen und Nutzer müssen bei der Eröffnung des Bürgerportalkontos auf mögliche Rechtsfolgen - etwa zur verbindlichen Kommunikation mit staatlichen Stellen - hingewiesen werden. Die Aufklärungs- und Informationspflichten müssen im Gesetzestext klarer als bislang geschehen gefasst werden. Gleiches gilt für die Feststellung von Identitätsdaten und der Aufdeckung von Pseudonymen.

- Eine Benachteiligung von Bürgerinnen und Bürgern, die über kein Bürgerportalkonto verfügen, muss ausgeschlossen werden. Auch dürfen Bürgerportale nicht dazu führen, dass staatliche Stellen dazu übergehen, bei jeder Inanspruchnahme einer E-Government-Anwendung eine persönliche Identifizierung zu verlangen, selbst wenn dies für die konkrete Dienstleistung nicht erforderlich ist.

- Der Entwurf sieht vor, dass grundsätzliche Fragen der technischen Ausgestaltung der Bürgerportale und der darüber angebotenen Dienste in einer Rechtsverordnung geregelt werden sollen. Dies widerspricht der Rahmenkonzeption des Art. 80 GG und dient auch sonst nicht der Normenklarheit des Gesetzes. Zumindest die grundsätzlichen technisch-organisatorischen Anforderungen an die Eröffnung des Kontos, den Postfach- und Versanddienst, den Speicherplatz, den Identitätsbescheinigungsdienst und das Akkreditierungsverfahren sollten in das Gesetz selbst aufgenommen werden.

- Der Entwurf des Bürgerportalgesetzes sieht jetzt auch vor, dass nicht nur die Datenerhebung, sondern auch die Verarbeitung und Nutzung der erhobenen Daten durch den akkreditierten Dienstanbieter an eine enge Zweckbestimmung gebunden ist. Allerdings ist der pauschale Verweis auf die Regelungen des Bundesdatenschutzgesetzes, des Telemediengesetzes und des Telekommunikationsgesetzes in diesem Zusammenhang zu weitgehend, da so für die Diensteanbieter die Möglichkeit eröffnet wird, die personenbezogenen Daten für Werbung oder Marktforschungszwecke zu nutzen. Die Bürgerinnen und Bürger müssen jedoch sicher sein können, dass ihre Daten ausschließlich zur Teilnahme am Bürgerportal genutzt werden.

16.2 Sonstiges

16.2.1 Schreiben an die Jugendämter zur VwV ISIS

Empfehlung des Sächsischen Datenschutzbeauftragten gemäß § 30 Abs. 4 SächsDSG im Hinblick auf die

Gemeinsame Verwaltungsvorschrift des SMI, des SMJus und des SMS zur Einrichtung eines Informationssystems zur Intensivüberwachung besonders rückfallgefährdeter Sexualstraftäter (VwV ISIS) vom 27. Juni 2008 (SächsABl. 2008 Nr. 33 S. 1058)
hier: Datenübermittlung durch die Jugendämter gemäß Abschnitt V 8 der VwV

Sehr geehrte Damen und Herren,

am 1. September 2008 ist die oben genannte, vor allem vom Sächsischen Staatsministerium der Justiz erarbeitete Verwaltungsvorschrift in Kraft getreten. Sie enthält in Abschnitt V 8 eine an die Jugendämter gerichtete Anweisung zur Übermittlung personenbezogener Daten, die den Eindruck erweckt, dass die Jugendämter unter den von der Vorschrift genannten Voraussetzungen in größerem oder zumindest nicht unbeträchtlichem Ausmaß zu der betreffenden Datenübermittlung befugt seien.

Da ich mit meinen diesbezüglichen Einwänden gegenüber dem Sächsischen Staatsministerium der Justiz und den beiden anderen beteiligten Ministerien nicht durchgedrungen bin, mache ich gemäß § 30 Abs. 4 SächsDSG beratend und empfehlend auf diese mögliche irreführende Wirkung aufmerksam, den dieser Abschnitt der VwV auf die Jugendämter haben kann - damit die VwV nicht insoweit unrechtmäßigen Datenübermittlungen Vorschub leistet.

Zu dieser Unterrichtung über meine Rechtsauffassung besteht um so mehr Anlass, als es bereits vor dem Erlass der Verwaltungsvorschrift in ähnlich gelagerten Fällen im Hinblick auf an sächsische Jugendämter gerichtete Übermittlungsanforderungen seitens Strafverfolgungsbehörden oder Strafgerichten erhebliche datenschutzrechtliche Probleme gegeben hat.

Auch ist zu besorgen, dass die dem Staatsministerium der Justiz unterstehenden Strafvollstreckungsbehörden dessen Rechtsstandpunkt den Jugendämtern gegenüber geltend machen werden.

Die betreffende Regelung in der VwV lautet wie folgt:

„***V.***
Informationsübermittlung
……..
8.
Ist ein Proband in das Informationssystem ISIS aufgenommen, informieren das Jugendamt und der soziale Dienst der Justiz die Strafvollstreckungsbehörde insbesondere über Erkenntnisse betreffend das soziale und familiäre Umfeld des Probanden, soweit dies gesetzlich zulässig ist.“

Das Sächsische Staatsministerium der Justiz hat zuletzt die dem Jugendamt für die Befolgung dieser Anweisung zu Gebote stehende Übermittlungserlaubnis vor allem in § 463a Abs. 1 Satz 1 StPO gesehen, es hat aber außerdem auch zu bedenken gegeben, ob nicht zusätzlich § 8a Abs. 4 Satz 2 SGB VIII eine ausreichende Ermächtigungsgrundlage darstelle. Beides trifft meines Erachtens nicht zu.

Im Falle des **§ 463a Abs. 1 Satz 1 StPO** ist dies unschwer erkennbar:

Gemäß § 35 Abs. 2 SGB I ist eine Verarbeitung (i. w. S.) von Sozialdaten *ausschließlich* aufgrund einer im SGB X vorgesehenen Erlaubnis zulässig, die gemäß § 67d Abs. 1 SGB X auch in einem anderen Buch des Sozialgesetzbuches, nicht jedoch in einer außerhalb des Sozialgesetzbuches stehenden Rechtsvorschrift begründet sein kann. § 71 Abs. 1 Satz 1, vor Nr. 1, SGB X, mit seiner ausdrücklichen Erlaubnis, Sozialdaten zum Zweck der Erfüllung außerhalb des SGB begründeter gesetzlicher Mitteilungspflichten zu übermitteln, macht diese Rechtslage mehr als deutlich.

§ 71 SGB X verweist in seinem *abschließenden* Aufzählungskatalog (so ausdrücklich auch die Begründung zu § 68 [= § 71 n. F.], siehe BT- Drucksache 8/4022 Seite 85) indes *nicht* auf die entsprechende Strafprozessvorschrift. Mit anderen Worten: Angesichts von § 67d Abs. 1 SGB X ist es unzweifelhaft, dass der Katalog des § 71 Abs. 1 Satz 1 zwingend einen Umkehrschluss begründet: Dort nicht aufgeführte Mitteilungspflichten aus anderen Gesetzen begründen keine Übermittlungsbefugnis für unter § 35 Abs. 1 Satz 1 SGB I fallende Stellen wie etwa die Jugendämter. Eine gegenteilige Rechtsauffassung ist nicht vertretbar.

Damit scheidet § 463a Abs. 1 Satz 1 StPO als Übermittlungserlaubnis für das Jugendamt im Anwendungsbereich des Abschnittes V 8 der VwV vollständig aus.

§ 8a Abs. 4 Satz 2 SGB VIII ist hingegen auf den ersten Blick gut geeignet, den gegenteiligen Eindruck zu erwecken, also denjenigen, als eine Übermittlungsbefugnis für die Jugendämter in Frage zu kommen, die Abschnitt V 8 der VwV voraussetzt.

Bei näherem Hinsehen stellt sich heraus, dass das Gegenteil der Fall ist. Denn:

§ 8a Abs. 4 Satz 2 SGB VIII erlaubt die Datenweitergabe durch das Jugendamt (ausschließlich) an *die anderen zur Abwendung der Gefährdung zuständigen Stellen*. Diese Wendung bezieht sich auf Satz 1 der Vorschrift, in dem als *zur Abwendung der Gefährdung* möglicherweise einzuschaltende zuständige Stellen ausschließlich *sonstige (SGB-)Leistungsträger* (also neben dem Jugendamt), *die Einrichtungen der Gesundheitshilfe und die Polizei* genannt werden.

Daraus folgt, dass in Satz 2 wegen des „*die anderen*“ nur solche Stellen als Datenempfänger (Empfänger einer Information über die Gefahr) in Betracht kommen, die in Satz 1 als (für die Abwehr der Gefahr neben dem Jugendamt) zuständig genannt sind, also nicht die Staatsanwaltschaft und nicht die Strafverfolgungsbehörde.

Anders ausgedrückt: Der Anwendungsbereich des § 8a Absatz 4 Satz 2 SGB VIII geht, was die Frage der Übermittlungsbefugnis der Jugendämter an Dritte betrifft, nicht über die in § 8a Absatz 4 Satz 1 SGB VIII explizit genannten Stellen hinaus. § 8a Absatz 4 Satz 2 SGB VIII berechtigt das Jugendamt unter den dort genannten Voraussetzungen (namentlich dass die dort genannten Personen nicht selbst tätig werden) im Unterschied zu § 8a Absatz 4 Satz 1 SGB VIII nur zusätzlich, die betreffenden Stellen eigenständig, das heißt *selbst einzuschalten* - und nicht nur wie in den Fällen des § 8a Absatz 4 Satz 1 SGB VIII auf deren Einschaltung *hinzuwirken*. Ich halte den Wortlaut des § 8a Absatz 4 SGB VIII für insoweit eindeutig. Zudem weist übrigens auch die Gesetzesbegründung zu § 8a Absatz 4 SGB VIII die Polizei als geeignete Institutionen zur Abwehr einer Gefährdung aus, die Staatsanwaltschaft wird hingegen nicht erwähnt (BR- Drucksache 586/04 Seite 53, 54).

Der Wortlaut der Vorschrift ist unter dem Gesichtspunkt der Beschränkung auf das zur Gefahrenabwehr Tunliche auch sehr sinnvoll. Allerdings erschließt sich dieser Sinn der Vorschrift nur bei genauem Hinsehen.

Die einzige im Anwendungsbereich des Abschnitte V 8 der VwV für die Jugendämter in Frage kommende Befugnis zu einer unter V 8 der VwV fallenden Übermittlung an die Strafvollstreckungsbehörde ist **§ 71 Abs. 1 Satz 1 Nr. 1 SGB X i. V. m § 138 Abs. 1 StGB**. Allerdings kommt neben oder statt der Polizei die Strafvollstreckungsbehörde als Übermittlungsempfänger nur in Frage, wenn die Ausführung des „Vorhabens“ noch nicht nah bevorsteht. Hinzu kommt, das § 138 Abs. 1 StGB keine Sexualdelikte als solche erfasst, sondern in dem hier einschlägigen Bereich nur Mord, Totschlag, Menschenhandel und Menschenraub, und dass es sich um die Kenntnis von einem

„Vorhaben“ handeln muss, so dass die Kenntnis einer allgemeinen Rückfallneigung des Probanden nicht für die Erlaubtheit der Übermittlung ausreicht.

Meiner aus dieser Rechtslage, also der nur in extrem seltenen Fällen bestehenden Befugnis der Jugendämter zur Übermittlung an die Strafvollstreckungsbehörde, gefolgerte Empfehlung, die diesbezügliche Übermittlungs-Anweisung in Abschnitt V 8 der VwV wegzulassen oder jedenfalls die Jugendämter ausdrücklich auf § 71 Absatz 1 Satz 1 Nr. 1 SGB X i. V. m. § 138 StGB als die allein in Betracht kommende Übermittlungserlaubnis hinzuweisen, ist man nicht gefolgt.

Bitte teilen Sie mir mit, wenn Sie beabsichtigen, entsprechend meiner Empfehlung zu verfahren, andernfalls bitte ich mir Ihre rechtlichen Einwände dagegen darzulegen.

16.2.2 Datenschutzrechtliche Grundlagen bei Auftragsdatenverarbeitung / Outsourcing in der öffentlichen Verwaltung

Arbeitspapier des Arbeitskreises Grundsatzfragen der Verwaltungsmodernisierung (AK GdV) der Konferenz der Datenschutzbeauftragten des Bundes und der Länder (Stand 8./9. Oktober 2008)

Spezielle Landesregelungen sind zu berücksichtigen.

I. Problemaufriss

Kostendruck, Rationalisierung der Arbeitsabläufe, Effizienzsteigerung und Nutzung moderner Technologien haben zur Konsequenz, dass immer mehr Verwaltungen dazu übergehen, einen Teil der bislang von ihnen durchgeführten Tätigkeiten nicht mehr selbst vorzunehmen, sondern auf Dritte (andere öffentliche Stellen oder private Anbieter) zu übertragen. Dies wird häufig mit dem etwas schillernden Begriff „Outsourcing“ umschrieben. Vergleichbare Effekte treten ein, wenn mehrere öffentliche Stellen gemeinsam Projekte betreiben, etwa kommunale Servicebüros. Auch eGovernment-Projekte erfordern vielfach entsprechende Aufgabenübertragungen.

Dabei stellt sich die Frage, wie der damit verbundene Austausch personenbezogener Daten rechtlich eingeordnet werden kann.

In der Regel wird auf § 11 BDSG bzw. vergleichbare Vorschriften in den Landesdatenschutzgesetzen verwiesen und der jeweilige Vorgang als Datenverarbeitung im Auftrag qualifiziert. Dies hat den Vorteil, dass nach den Begriffsdefinitionen des BDSG keine datenschutzrechtlich relevante Übermittlung der entsprechenden personenbezogenen Daten vorliegt, da Übermittlung i. S. d. § 3 Abs. 4 Nr. 3 BDSG die Bekanntgabe personenbezogener Daten an einen Dritten voraussetzt und der Auftragnehmer nach § 3

Abs. 8 Satz 3 BDSG nicht Dritter ist. Die gesetzlichen Voraussetzungen für eine Datenübermittlung brauchen deswegen nicht eingehalten zu werden und es gibt für die uneingeschränkte Datenweitergabe scheinbar keine rechtlichen Hindernisse. Deswegen ist eine ausufernde Anwendung des § 11 BDSG und entsprechender Vorschriften im Landesrecht festzustellen. Um die Anwendung einzugrenzen, ist in der Kommentarliteratur zu § 11 BDSG der Begriff der „Funktionsübertragung“ entwickelt worden. Liegt eine solche vor, soll die Anwendung des § 11 BDSG ausgeschlossen sein, so dass in diesen Fällen eine Datenweitergabe nur im Rahmen der gesetzlichen Übermittlungsvorschriften möglich ist.

Allerdings lässt sich nicht eindeutig definieren, wann von einer Funktionsübertragung in diesem Sinne auszugehen ist. Deswegen bleibt die Abgrenzung zur Datenverarbeitung im Auftrag unscharf und eröffnet unverändert weite Interpretationsspielräume, die je nach Interessenlage auch entsprechend genutzt werden.

In diesem Zusammenhang spielt auch die Schutzfunktion der gesetzlichen Regelungen zur Auftragsdatenverarbeitung eine Rolle. § 11 BDSG und die entsprechenden Vorschriften im Landesrecht sollen sicherstellen, dass den Betroffenen gegenüber die Stelle in der datenschutzrechtlichen Verantwortung bleibt, die ihre personenbezogenen Daten ursprünglich erhoben, verarbeitet oder genutzt oder dies zumindest veranlasst hat. Die verantwortliche Stelle soll sich ihrer Verantwortung nicht dadurch entledigen können, dass sie die Datenverarbeitung auslagert. Nur wenn sie diese weiterhin den Betroffenen gegenüber rechtlich verantworten muss, wird sie ihrerseits bei Auswahl, rechtlicher Ausgestaltung des Auftragsverhältnisses und bei der Kontrolle die erforderliche Sorgfalt walten lassen, um für die Betroffenen den größtmöglichen Datenschutz zu gewährleisten. In den Fällen, in denen nach den bisherigen Definitionen § 11 BDSG nicht zur Anwendung kommt, kann damit eine Verschlechterung der datenschutzrechtlichen Position der Betroffenen verbunden sein. Eine weite Auslegung des § 11 BDSG bzw. der entsprechenden Landesregelungen könnte deswegen im Einzelfall durchaus auch im Interesse der Betroffenen liegen, etwa weil so in Fällen, die nach den gängigen Interpretationen eindeutig als Funktionsübertragung zu werten wären, die datenschutzrechtliche Verantwortung beim Auftraggeber verbliebe.

Ausgehend vom Gesetzestext, seiner Entstehungsgeschichte und von den vom Gesetzgeber verfolgten Zwecken wird im Folgenden deswegen ein neuer Ansatz für die datenschutzrechtliche Bewertung von Auftragsdatenverarbeitung und Outsourcing entwickelt.

II. Regelungsinhalt des § 11 BDSG (und entsprechender Landesregelungen)

Grundsätzlich ist im deutschen Datenschutzrecht die Zulässigkeit der Datenverarbeitung durch öffentliche Stellen mit der Erfüllung der zugrunde liegenden Aufgabe verbunden (vgl. z. B. § 13 Abs. 1, § 14 Abs. 1 BDSG). Personenbezogene Daten dürfen von diesen erhoben, gespeichert, verändert oder genutzt werden, wenn deren Kenntnis und Verarbeitung zur Erfüllung der in der Zuständigkeit der verantwortlichen Stelle liegenden Aufgaben erforderlich ist. Insoweit liegen inhaltliche Verantwortung für die Aufgabenerfüllung und Verantwortung für die damit verbundene Datenverarbeitung in der gleichen Hand.

§ 11 BDSG (vergleichbares gilt für die entsprechenden Landesregelungen) bezieht sich nach seinem Wortlaut, insbesondere aber auch nach seiner Entstehungsgeschichte auf die Fälle, in denen die Abwicklung der Datenverarbeitung auf einen Dritten (Auftragnehmer) übertragen wird, während die inhaltliche Verantwortung für die Aufgabenerfüllung beim Auftraggeber verbleibt. Dieser hat nach § 11 Abs. 1 BDSG auch weiterhin die Verantwortung für die Einhaltung des Datenschutzes zu tragen.

Mit dieser Regelung, die ursprünglich als Datenverarbeitung für fremde Zwecke betrachtet wurde, sollte sichergestellt werden, dass die datenschutzrechtliche Verantwortung und die inhaltliche Verantwortung nicht auseinander fallen, sondern in einer Hand beim Auftraggeber verbleiben. Niemand sollte sich durch die Auslagerung des Datenverarbeitungsprozesses seiner datenschutzrechtlichen Verpflichtungen entledigen können. Obwohl danach der Anwendungsbereich des § 11 BDSG eigentlich relativ eng abgegrenzt war, ist eine ständig wachsende Tendenz festzustellen, ihn sehr weit auszulegen. Dies geschieht vor allem dadurch, dass das Auftragsverhältnis, das der Anwendung des § 11 BDSG zugrunde liegt, nicht nur auf die Datenverarbeitung im engen, technischen Sinn bezogen wird, sondern stillschweigend auch auf eine inhaltliche Aufgabenübertragung. Danach soll es genügen, einem Dritten den Auftrag zu erteilen, bestimmte Aufgaben auch inhaltlich wahrzunehmen, um von einer rechtmäßigen Auftragsdatenverarbeitung i. S. d. § 11 BDSG ausgehen zu können. Diese Norm mutiert so zu einer allgemeinen Rechtsgrundlage für Outsourcing und Aufgabenübertragung auf Dritte, obwohl sie von Wortlaut und Zweck her eine ganz andere Fallgestaltung regeln soll. Dadurch entstehen auch die unübersehbaren Abgrenzungsschwierigkeiten zwischen Auftragsdatenverarbeitung und „Funktionsübertragung“. Deswegen erscheint es erforderlich, § 11 BDSG auf seinen ursprünglichen Regelungsgehalt zurückzuführen und ausschließlich als Rechtsgrundlage für Aufträge zur Datenverarbeitung zu verstehen. Für eine inhaltliche Aufgabenverlagerung kann § 11 BDSG danach niemals eine rechtliche Grundlage sein.

III. Aufgabenübertragung / Outsourcing

Für die unterschiedlichen Formen der Zusammenarbeit zwischen unterschiedlichen Verwaltungen oder zwischen Verwaltung und nicht-öffentlichen Stellen lassen sich danach datenschutzrechtlich folgende Fallgruppen unterscheiden:

1. Übermittlung

Erfolgt die Übertragung personenbezogener Daten zwischen zwei Stellen im Rahmen und zur Erfüllung ihrer eigenen Aufgaben, handelt es sich datenschutzrechtlich um eine typische Übermittlung, deren Voraussetzungen z. B. für öffentliche Stellen u. a. in den §§ 15 und 16 BDSG geregelt sind. Diese Fälle werden im Folgenden nicht weiter behandelt.

Beispiele:
- Datenübermittlung der Meldebehörden an den Suchdienst des Deutschen Roten Kreuzes
- Datenübermittlung der Katasterämter an Banken
- Datenaustausch zwischen Ausländerzentralregister und Ausländerbehörden

2. Auslagerung der Datenverarbeitung

Bedient sich eine öffentliche Stelle einer anderen öffentlichen oder nicht-öffentlichen Stelle zur rein technischen Abwicklung der für ihre Aufgabenerfüllung erforderlichen Datenverarbeitung, ist dies der typische Fall der Datenverarbeitung im Auftrag, wie sie z. B. in § 11 BDSG geregelt ist (s. o. unter II.). Gemeint sind hier die Fälle, in denen sich der erteilte Auftrag nur auf die Durchführung der eigentlichen technischen Abwicklung der Datenverarbeitung nach einem vorgegebenen Algorithmus bezieht. Nicht hierunter fällt hingegen die Übertragung solcher Aufgaben oder Teilaufgaben, bei denen nicht alle vorzunehmenden Verarbeitungsschritte von vornherein festgelegt sind, z. B. wenn die Bearbeitung eines Antrages der Auslegung unbestimmter Rechtsbegriffe bedarf und eine algorithmische Lösung auf der Ebene der reinen technischen Abwicklung nicht gegeben ist. Auch die Weisungen des Auftraggebers im Sinne des § 11 Abs. 3 BDSG (oder vergleichbarer Landesregelungen) beziehen sich auf die Datenverarbeitung selbst und nicht etwa auf eine inhaltliche Aufgabenerledigung.

Beispiele:
- Nutzung externer Rechenzentren oder externer Speicherkapazität, sofern ausschließlich rechentechnische Vorgänge nach vorgegebenem Algorithmus ausgelagert werden
- Fernwartung (u. U. aber abweichende Länderregelungen)
- Entsorgung von Datenträgern
- Virtuelle Poststelle (soweit nur die Technik ausgelagert ist)

3. Auslagerung von Aufgaben

Immer häufiger sind aber die Fälle, in denen durch Outsourcing, Schaffung gemeinsamer Institutionen verschiedener verantwortlicher Stellen, eGovernment-Projekte etc. Aufgaben oder auch nur Teilbereiche der Aufgabenerfüllung inhaltlich auf eine andere öffentliche oder nicht-öffentliche Stelle übertragen werden und die damit verbundene elektronische Erhebung, Verarbeitung oder Nutzung personenbezogener Daten nur Annex zur eigentlichen Aufgabenverlagerung ist. Dabei wird der Begriff der „Aufgabe", an den die datenschutzrechtlichen Bestimmungen anknüpfen, soweit ersichtlich nirgendwo weiter definiert oder näher erläutert. Für die folgenden Ausführungen wird als „Aufgabe" jede nach allgemeiner Auffassung eine Einheit bildende funktionale Tätigkeit der Verwaltung verstanden, die von anderen Tätigkeitsbereichen abgrenzbar und für die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten erforderlich ist, wie z. B. Festsetzung und Einzug von Gebühren, Eingabenbearbeitung, Führung von öffentlichen Registern etc. Angesichts der verfassungsrechtlich geforderten Bindung der Verwaltung an Recht und Gesetz (Art. 20 Abs. 3 GG) kann eine funktionale Tätigkeit nur durch den Gesetz- und Verordnungsgeber (bzw. durch ein nach Landesrecht befugtes Organ oder das Vertretungsorgan einer juristischen Person des öffentlichen Rechts, z. B. einer Gemeinde oder einer Hochschule) zu einer Aufgabe gemacht werden, wobei damit gleichzeitig der Umfang der funktionalen Tätigkeit begrenzt und die zuständige Stelle bestimmt wird.

Soll die inhaltliche Wahrnehmung von Aufgaben in diesem Sinne vollständig oder in Teilbereichen auf andere Stellen übertragen werden, scheiden als rechtliche Grundlage hierfür § 11 BDSG oder die vergleichbaren Landesregelungen aus, auch wenn der Auftragnehmer keinen eigenen Entscheidungsspielraum hat und bei der inhaltlichen Auftragserfüllung vollständig von Weisungen des Auftraggebers abhängig ist. Da - wie oben dargelegt - die Zuständigkeit für die Aufgabenerledigung durch Rechtsvorschrift in der Regel eindeutig definiert ist, kann die auf die bloße Datenverarbeitung als Hilfsfunktion zur Aufgabenerfüllung gerichtete Vorschrift des § 11 BDSG diese Festlegung nicht ändern. Voraussetzung ist vielmehr, dass eine solche Aufgabenverlagerung auf anderer rechtlicher Grundlage zulässig oder rechtlich möglich ist. Dies können u. a. gesetzliche Regelungen, Satzungen, Verwaltungsvereinbarungen oder vertragliche Regelungen sein, soweit diese ihrerseits die Grenzen beachten, die sich aus dem Grundgesetz, der Staatsorganisation oder anderen gesetzlichen Vorschriften ergeben. Dies ist keine datenschutzrechtliche Frage, die datenschutzrechtliche Norm des § 11 BDSG (und vergleichbarer Länderregelungen) kann aber ihrerseits nicht Grundlage für staatsorganisationsrechtliche Entscheidungen sein.

Im Einzelnen sind folgende Fallgestaltungen denkbar:

a. Wird eine Aufgabe vollständig von einer Stelle in die Zuständigkeit einer anderen Stelle übergeleitet, gehen sowohl die inhaltliche wie die datenschutzrechtliche Verantwortung auf die neue Stelle über. Als Rechtsgrundlage für eine solche Aufgabenübertragung kommen im öffentlichen Bereich entweder gesetzliche Regelungen oder Organisationserlasse der jeweils zuständigen obersten Behörden in Betracht. Datenschutzrechtlich ist dies in der Regel kein Problem, da grundsätzlich die Zulässigkeit der Datenverarbeitung mit der Erfüllung der zugrunde liegenden Aufgabe verbunden ist. Kommt es zu einer Zuständigkeitsverlagerung bei der Aufgabe, verliert die bisherige Stelle ihre Berechtigung zur entsprechenden Datenverarbeitung und die neue Stelle erwirbt sie zusammen mit der Zuständigkeit für die Aufgabe. Die entsprechenden Datenbestände bei der bisherigen Stelle sind, soweit für die künftige Aufgabenerfüllung erforderlich, nach den einschlägigen Vorschriften an die neue Stelle zu übermitteln und im Übrigen zu löschen. Dies ist kein Anwendungsfall des § 11 BDSG oder von vergleichbaren Landesregelungen.

   Beispiele:
   - Zentrale Bearbeitung von Reisekostenabrechnungen für mehrere Dienststellen
   - Zentralisierte Festsetzung von Dienstbezügen für die Beschäftigten mehrerer Dienststellen
   - Privatisierung von Staatsaufgaben auf gesetzlicher Grundlage

b. Bleibt die öffentliche Stelle grundsätzlich Träger der Aufgabe und benutzt sie zu ihrer Erfüllung Dritte, so ist hierin zunächst zu prüfen, ob und in welchem Umfang dies zulässig ist. Dabei ist zum einen zu berücksichtigen, ob es sich um eine andere öffentliche Stelle oder um einen privaten Anbieter handelt, und zum anderen, ob es um hoheitliche Tätigkeit, öffentliche Aufgaben nicht-hoheitlicher Art oder rein fiskalisches Handeln geht.

   aa. Hoheitliche Tätigkeiten können ohne gesetzliche Regelung (Beleihung) nicht von privaten Stellen ausgeübt werden. Eine öffentliche Stelle kann auch nicht von sich aus einen Teil ihrer hoheitlichen Aufgaben von einer anderen öffentlichen Stelle wahrnehmen lassen. Im Bereich der Hoheitsverwaltung bedarf es dazu immer eines formalen Aktes auf gesetzlicher Grundlage.

      Beispiele:
      - Bearbeitung von Beihilfeangelegenheiten (vgl. OVG NRW, Urteil vom 21. April 2005 - 1 A 265/04)
      - Privatisierung des Maßregelvollzuges
      - Parkraumbewirtschaftung (hinsichtlich einer vollständigen Verlagerung, der Feststellung von Ordnungswidrigkeiten oder der Gebührenfestsetzung)

bb. Öffentliche Aufgaben nicht-hoheitlicher Art können grundsätzlich ganz oder teilweise auch von privaten oder anderen öffentlichen Stellen durchgeführt werden, etwa auf gesetzlicher oder vertraglicher Grundlage oder - bei unselbständigen Hilfstätigkeiten - auch durch Verwaltungshelfer. Aber auch hier bedarf es einer klaren rechtlichen Basis.

Beispiele:
- Callcenter mit bloßer Weiterleitungsfunktion
- Virtuelle Poststelle (inhaltliche Bearbeitung)
- Betriebsführungsgesellschaften von Zweckverbänden (ohne Übertragung hoheitlicher Befugnisse)
- Parkraumbewirtschaftung (nur Abrechnung)

cc. Bei rein fiskalischem Handeln können durch einfachen Vertrag Dritte mit bestimmten Aufgaben betraut werden.

Beispiele:
- Verwaltung von Liegenschaften
- Betreiben einer Stadtgärtnerei

Sind von einer verantwortlichen Stelle nach alledem im Rahmen ihrer Aufgaben, deren Trägerin sie bleibt, einzelne Tätigkeiten oder Teilaufgaben zulässigerweise und in rechtlich einwandfreier Form auf andere öffentliche oder private Stellen zur Erfüllung übertragen worden, kann die damit verbundene Datenverarbeitung parallel dazu nach § 11 BDSG (oder vergleichbaren Landesregelungen) übertragen und abgewickelt werden, selbst wenn der Auftragnehmer im Rahmen seines Auftrages auch inhaltlich eigenverantwortlich tätig wird. Dabei muss selbstverständlich eindeutig festgelegt sein, welche Stelle für welche Tätigkeit inhaltlich verantwortlich ist, um eine Verwischung der Verantwortlichkeiten in jedem Falle zu vermeiden. Damit bleibt auch in diesen Fällen der gesetzlich gewollte Schutz der Betroffenen erhalten, die sich hinsichtlich des Datenschutzes und ihrer Betroffenenrechte weiterhin ausschließlich an die verantwortliche Stelle wenden können, die ihrerseits für die Einhaltung des Datenschutzes verantwortlich bleibt. Eine solche Konstruktion wahrt auf der einen Seite für die Betroffenen die datenschutzrechtlichen Vorteile, die mit der Anwendung des § 11 BDSG und der vergleichbaren Landesregelungen verbunden sind, verhindert aber zugleich, dass die rein datenschutzrechtlichen Regelungen der Auftragsdatenverarbeitung als allgemeine Rechtsgrundlage für Aufgabenübertragung und Outsourcing in der öffentlichen Verwaltung herangezogen werden.

IV. Sonderfälle

1. Sozialdaten
Für Sozialdaten gelten grundsätzlich die gleichen Prinzipien, allerdings sind die Sonderregelungen des § 80 SGB X zu beachten.

2. Besondere Arten von Daten
Soweit besondere Arten von personenbezogenen Daten (§ 3 Abs. 9 BDSG) in zulässiger Weise erhoben, verarbeitet oder genutzt werden, können sie auch Gegenstand einer Auftragsdatenverarbeitung nach § 11 BDSG sein, wenn die Voraussetzungen im Übrigen erfüllt sind.

3. Berufsgeheimnisse / Besondere Amtsgeheimnisse
Personenbezogene Daten, bei denen es sich um Berufs- oder besondere Amtsgeheimnisse handelt, unterliegen insoweit den hierfür geltenden Spezialvorschriften. Dem ist bei der Prüfung, ob eine inhaltliche Übertragung von Aufgaben oder Teilaufgaben zulässig ist, Rechnung zu tragen. Eine Offenbarung etwa von Informationen, die dem Patientengeheimnis unterliegen, ist durch § 11 BDSG nicht gedeckt.

4. Aufgabenverlagerung ins Ausland
Sofern es sich um eine Aufgabenverlagerung in Mitgliedsstaaten der Europäischen Union oder Vertragsstaaten im Europäischen Wirtschaftsraum (EWR) sowie der Organe der EU handelt, gelten grundsätzlich keine Besonderheiten hinsichtlich einer Auftragsdatenverarbeitung nach § 11 BDSG, da insoweit gem. § 3 Abs. 8 Satz 3 BDSG vor dem Hintergrund der EU-Datenschutzrichtlinie 95/46/EG eine ausdrückliche Gleichstellung erfolgt. Hinsichtlich einer Übertragung inhaltlicher (Teil-)Aufgaben auf Grundlage eines Rechtsaktes sind allerdings (ebenso wie zwischen Bund und Ländern im Inland) die jeweiligen Hoheitsgrenzen zu beachten. So ist es dem nationalen Gesetzgeber mangels Zuständigkeit nicht ohne Weiteres möglich, eine Stelle in einem anderen Mitgliedsstaat der EU mit der inhaltlichen Wahrnehmung öffentlicher Aufgaben zu betrauen. Soll eine Stelle außerhalb von EU/EWR beauftragt werden, ist diese in jedem Falle als Dritter zu bezeichnen; eine Datenverarbeitung im Auftrag kommt daher von vornherein nicht in Betracht. Deshalb kommen zu den Einschränkungen bei der Verlagerung der inhaltlichen Aufgabenerledigung ins Ausland auch noch erhebliche Beschränkungen bei der Verlagerung der rein technischen Datenverarbeitung hinzu: Mangels Anwendbarkeit von § 11 BDSG bedarf es einer Übermittlungsbefugnis nach den §§ 4b, 4c BDSG.

V. Ergebnis

Die Auslegung des § 11 BDSG (bzw. vergleichbarer Landesregelungen) ergibt, dass dieser ausschließlich die Übertragung der Datenverarbeitung im technischen Sinne (s. o. III.2) auf einen Dritten regelt und nicht Rechtsgrundlage für eine inhaltliche Aufgaben-

übertragung sein kann. Soweit inhaltlich eine Zuständigkeitsverlagerung (ganz oder teilweise) auf private oder öffentliche Stellen außerhalb der zuständigen Stelle erfolgt, richtet sich deren Zulässigkeit nach den verfassungs- und verwaltungsrechtlichen Vorgaben des Verwaltungsorganisationsrechts.

Ist danach eine inhaltliche Verlagerung von Tätigkeiten zulässig und in der jeweils rechtlich gebotenen Form vorgenommen worden, können für die damit verbundene Datenverarbeitung § 11 BDSG (oder vergleichbare Landesregelungen) als Grundlage herangezogen und so die Schutzwirkungen dieser Norm für die Betroffenen erhalten werden. Die zuständige Datenschutzaufsicht hat in diesen Fällen nicht nur zu prüfen, ob die Voraussetzungen des § 11 BDSG erfüllt sind, sondern auch, ob die inhaltliche Aufgabenübertragung zulässig ist, da dies Voraussetzung für die Anwendung des § 11 BDSG ist.

Stichwortverzeichnis